МІНІСТЕРСТВО ОСВІТИ І НАУКИ
МОЛОДІ ТА СПОРТУ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

В. А. Фільштінський, А. В. Бережний

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

КОНСПЕКТ ЛЕКЦІЙ

Суми
Сумський державний університет
2011

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

Конспект лекцій

для студентів спеціальностей
7.080202 „Прикладна математика”,
денної форми навчання

Затверджено
на засіданні кафедри
прикладної та обчислювальної
математики
як конспект лекцій
з дисципліни „Вища математика”.
Протокол № 05 від 28.12.2010 р.

.

Суми
Сумський державний університет
2011

Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.

Кафедра прикладної та обчислювальної математики

Невеликий курс криптографії присвячений питанням математичних основ криптографії. У ньому розглядаються необхідні розділи теорії чисел (оглядово), деякі блокові й потокові шифри. Основна увага приділяється криптосистемам з відкритим ключем і першочерговими задачами, які розв'язуються із залученням таких криптографічних алгоритмів, як шифрування даних, цифрові підписи, схеми ідентифікації, обмін сеансовими ключами та ін. Розглядаються деякі питання криптоаналізу, криптографічних протоколів.

Виклад проілюстрований прикладами.

Предмет орієнтований на студентів-математиків і майбутніх фахівців з інформаційної безпеки.

ВСТУП

Як вступні слова наведемо кілька цитат із книги [19].

«Без сумніву, немає ніякої можливості зрозуміти напрями розвитку людського суспільства окремо від його палкого прагнення до таємниць. Політики й військові, священики й торгівці, письменники й учені, шарлатани й аферисти тисячами років розвивали науку про секрети, доводячи їхнє творіння до досконалості, служили таємницям, насичували свої потреби в них. Без таємниць не може бути не тільки держави, але навіть малої спільноти людей без них не можна виграти битву або вигідно продати товар, здолати своїх політичних супротивників у жорстокій боротьбі за владу або зберегти першість у технології. Таємниці становлять основу науки, техніки й політики будь-якої людської формації, будучи цементом державності.

Історія зберігає так багато секретів, що просто дивно, як людям вони необхідні. Служба безпеки намагається поділяти їх на ряд класів: від «для службового користування» до «абсолютно секретно» і «сугубо довірчо». Американський фізик Річард Фейнман жартома казав, що при роботі над створенням атомної бомби йому разом із документами, що мають позначку «ingest after reading», тобто буквально «знищити після прочитання», попадалися іноді папери й зі штампом «знищити до прочитання».

Уряди всіх країн світу прагнуть позбавити людей інтимного життя: листи читаються, телефони прослуховуються, багаж і носильні речі додивляються, за людьми спостерігають. Разом із тим усе більше наші приватні повідомлення йдуть по електронних каналах.

Спочатку були телефони, потім з’явилися факси й, нарешті, щосили запрацювала електронна пошта. Повідомлення електронної пошти особливо легко перехоплювати або сканувати по ключових словах, що широко застосовується, як урядовими органами, так хакерами й просто зацікавленими.

Міжнародні перекази всі без винятку читаються державними службами.

Крім цієї проблеми, існує й не менш важлива зараз, нехай не для особистості, але для країни конфіденційність даних досліджень, розробок і стратегічної керуючої інформації в комп'ютерних системах. Від цього безпосередньо залежить безпека суспільства.

Наприклад, злочинне порушення роботи програм керування ядерних реакторів Ігналінської АЕС у 1992 році за серйозністю можливих наслідків прирівнюється до Чорнобильської катастрофи.

Основна небезпека «дияволів комп'ютерної злочинності» полягає у тому, що їм, як правило, успішно вдається приховати своє існування і сліди діяльності. Чи можна почуватися у безпеці, якщо ЕОМ перебуває вдома, а доступ до неї обмежений паролем? Однак відомий випадок, коли копіювання даних з такого комп'ютера зробила дитина, яка не підозрювала нічого поганого й розраховувала, запустивши дану йому іншою людиною дискету, пограти в нову дуже цікаву гру.

Статистика економічних злочинів демонструє їхнє переміщення в область електронної обробки даних. При цьому лідируюче положення займають махінації в банках, які зводяться до зміни даних з метою одержання фінансової вигоди. Новизна комп'ютерних злочинів полягає в тому, що інформація, що представляє активи фірм, тепер зберігається не на папері у видимому й легко доступному для людському сприйняттю вигляді, а в незрозумілій й зчитувальній тільки машинами формі на електронних пристроях зберігання. Розкривається лише мала кількість комп'ютерних злочинів, тому що фінансові компанії воліють про неї умовчувати, щоб не втратити іміджу.

Посилення залежності ділових і наукових кіл від ЕОМ поряд із стурбованістю громадськості, що обробка інформації зачіпає особисті інтереси громадян, привела до зростання уваги проблем захисту конфіденційних даних у комп'ютерах від незаконного доступу.

Хоча традиційно криптографія застосовувалася винятково

збройними силами й дипломатичними службами, але зараз вона дозволяє виконувати ділові операції шляхом передачі інформації по мережам зв'язку з використанням методів ідентифікації й аутентифікації (ідентифікація й аутентифікація доказ авторства і достовірності повідомлення), цифрового підпису, видачі дозволів на транзакції з реєстрацією і їхнім нотаріальним завіренням, оцінки дати, часу доби й багато чого іншого. Ці нові додатки перетворюють криптографію в техніку подвійного використання для військових і цивільних цілей. Шифрування в цивільному секторі ведеться для проведення міжнародних банківських операцій, електронного обміну інформацією, обміну електронною поштою й комерційними справами по мережах зв'язку.

В основі такого розмежування застосувань полягає поділ сфер використання криптографії для збереження таємності інформації й для її аутентифікації. Це розмежування явно виражене в новітніх криптографічних системах з відкритим ключем. Криптографія необхідна приватному комерційному сектору економіки для прогресивного розвитку. Це стосується і використання криптографічних алгоритмів, їхніх прикладних застосувань, загальних методів керування ключами і їхнього розподілу.

1 ЗАГАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Небезпека даних

Крім надання конфіденційності, криптографія часто використовується для інших функцій.

Перевірка достовірності. Одержувач повідомлення може перевірити його джерело, зловмисник не зможе замаскуватися під іншу особу.

Цілісність. Одержувач повідомлення може перевірити, чи не було повідомлення, змінене в процесі доставки, зловмисник не зможе підмінити правильне повідомлення хибним.

Незаперечення авторства. Відправник не зможе неправдиво заперечувати відправлення повідомлення.

Розглянемо види втрат, що виникають від розкриття інформації.

Звичайно, дані про людей найбільш важливі для них самих, але, як би це не описували в шпигунських фільмах, мало що значать для викрадачів. Іноді особисті дані можуть використовуватися для компрометації не тільки окремих людей, але цілих організацій, Наприклад, розкриття стратегічної інформації.

Підміни інформації становлять істотну небезпеку. У багатьох організаціях життєво важливі дані зберігаються у файлах: інвентарні описи, графіки робіт, списки замовлень. Якщо такі дані будуть підмінені або стерті, то робота надовго паралізується. Найбільшу небезпеку в цьому складає те, що в примітивних криптографічних системах необхідні дані для цих підмін можуть бути зроблені й без знання ключа. Тому серйозні шифри повинні гарантувати не тільки стійкість їхнього розкриття, але й неможливість непомітної модифікації одинарного біта. Володіння ключем відкриває повний доступ до даних – отже, можна скомпрометувати бухгалтерську або конструкторську систему, ледве підмінивши десяток-інший чисел, або видалити відомості про реальний рух товару, щоб рахунок за нього не був виставлений. Схоже, що найбільш

уразлива для підміни інформація економічного характеру, де втрати можуть бути надзвичайно великі. Таким чином, критичні дані обов'язково повинні зберігатися в шифрованому вигляді або хоча б підтверджуватися цифровим підписом, щоб уникнути підміни.

1.2 Рівні захисту даних

Найважливіший рівень захисту криптографічний. У нашому контексті він являє собою шифрування даних з метою приховати їхній зміст. Доти, поки користувач не ідентифікований по ключу, зміст даних йому недоступний. Дані в цьому випадку розглядаються як повідомлення, і для захисту їхнього змісту використовується класична техніка шифрування. Криптографія припускає наявність трьох компонентів: даних, ключа й криптографічного перетворення. При шифруванні вхідними даними будуть повідомлення, а результуючими - шифрування. При розшифруванні вони міняються місцями. Вважається, що криптографічне перетворення відоме всім, але, не знаючи ключа, за допомогою якого користувач закрив зміст повідомлення від третіх осіб, потрібно витратити неймовірно багато зусиль на відновлення тексту повідомлення. (Варто підкреслити, що немає абсолютно стійкого від розкриття шифрування. Якість шифру визначається лише грошима, які потрібно викласти для його розкриття від $10 і до $1000000.) Така вимога задовольняється рядом сучасних криптографічних систем, наприклад, створених за «Стандартом шифрування даних Національного бюро стандартів США» DES і ДЕРЖСТАНДАРТ 28147-89 (Росія). Оскільки ряд даних критичний до деяких їхніх перетворень, які не можна виявити з контексту, то звичайно використовуються лише такі способи шифрування, які чутливі до перетворень будь-якого символу. Вони гарантують не тільки високу таємність, але й ефективне виявлення будь-яких підмін або помилок. Раніше, достатньо було взяти пари затисків і навушники, помістити їх на необхідні контакти й слухати бесіду абонентів. Зараз цифрова передача сигналу робить цю задачу дуже важкою бесіди перетворюються в незв'язний потік цифр і

складаються разом знову у звуки на іншому кінці лінії. (Широко поширена в колишні роки й справедлива на той час думка, що багато телефонних розмов прослуховуються, зараз невірна. Тепер це складно й дорого зробити. Клацання в трубці, підключення сторонніх абонентів та інші перешкоди зазвичай викликаються просто збоями апаратури АТС).

Тепер розглянемо апаратні засоби захисту. Вони досить дорогі й мало поширені. Апаратура, що використовує ключі у вигляді магнітних та електронних карток, не так давно почала широко розповсюджуватися. Вони зберігають інформацію на інтегрованій мікросхемі або мікропроцесорі. Електронні картки мають масу застосувань:

- у вигляді грошей, коли картка використовується як дебетна або кредитна;
- як посвідчення особи при розрахунках по банківському рахунку для зберігання даних клієнта й установлення процедур аутентифікації;
- як ключ шифрування або криптографічний процесор; як електронний документ пропуск на підприємство, водійське посвідчення, медична карта, накладна для вантажів;
- як електронний ключ для систем охоронної сигналізації доступу в приміщення й до обладнання.

Інформація в пам’яті карток зберігається в зашифрованому вигляді, для якої, як правило, використовується DES алгоритм, але зустрічається й RSA, що дає більше можливостей.

Базою для обчислення пароля береться унікальний серійний номер картки. Повторні спроби несанкціонованого доступу до інформації на карті звичайно приводять до стирання її коду. Прикладом найпоширенішої картки для ідентифікації доступу до комп’ютера є IBM Personal Security Card із пристроєм зчитування й ідентифікації підпису IBM-4754. Крім того, що цей пристрій зчитує карти, він ще вимагає підписи її власника, реєструючи не тільки контур підпису, але й особливості натиску пера. Це робить процедуру ідентифікації настільки надійною, що вона була прийнята швейцарськими банками. Незважаючи

на всі свої переваги, звичайні ключі, картки й паролі для завантаження системи надзвичайно мало ефективні.

Криптографічний захист представляється найбільш дешевим й ефективним із всіх розглянутих. Секретний диск, підкріплений засобами криптографії, являється досить надійним від проникнення в нього пристроєм. Хоча перед уведенням пароля варто переконатися, що маєте справу з оригінальною програмою. На жаль, всі відомі нам криптографічні програмні засоби передбачають тільки уведення пароля, а не обмін паролями між користувачем і системою так зване «рукостискання». Військові давно вже створили правило рукостискання й у відповідь на пароль вимагали відклик, щоб переконатися, що вартовий справжній, а не диверсант, що намагається лише вивідати пароль. Криптографічне перетворення файлів є єдиним засобом, що гарантує абсолютний захист від розкриття його змісту при умовах, які будуть описані пізніше. Крім криптографічних програм часто використовуються спеціальні програми для знищення з дисків і файлів інформації, яка повинна бути знищена. Знищення диска й файлів означає перезапис їхнього змісту якоюсь несекретною інформацією, наприклад, нулями, для того, щоб дані, що містяться в них, зникли фізично. Адже звичайне видалення файлів знищує дані тільки логічно, і, якщо на їхнє місце не була записана інша інформація, то дані можна відновити. Подібний результат дає запис у файл іншого файла, більшого за розміром, а потім стирання його, хоча ця операція менш надійна й дані іноді все-таки можуть бути відновлені спеціальними програмами. Особливо зручне знищення незайнятих областей диска по закінченні роботи над даними, які були закодовані. Однак ця операція може зайняти кілька хвилин, що іноді дратує повільністю.

З усього сказаного можна зрозуміти центральне місце криптографії в захисті даних на ЕОМ, яка, не вимагаючи великих витрат, забезпечує абсолютний їхній захист. Разом з тим потрібно враховувати, що лише адміністративні міри можуть захистити саму криптографію, її ключі й людей від

можливого обману або погроз застосуванню фізичної сили. Звичайно є небезпека перестаратися в реалізації мір захисту. Але труднощі захисту полягають у тому, що не тільки джерела потенційної погрози погано відомі, але й переважна більшість комп'ютерних злочинів залишаються невідомими для потерпілих. На жаль, безпеку даних не можна ні довести, ні, тим більше, прийняти на віру.

2 ПРЕДМЕТ КРИПТОЛОГІЇ

2.1 Коди та їхнє призначення

До шифрів не відносяться коди системи умовних позначень або назв, які застосовуються при передачі інформації в дипломатії, комерції й військовій справі. Кодування часто застосовується для підвищення якості передачі. Добре відомі й широко використовуються коди, що виправляють помилки при передачі повідомлень за каналами зв'язку або зберіганні даних у пам'яті ЕОМ. Так, код Хемінга добре зарекомендував в апаратурі оперативної пам'яті ЕОМ СМ-4. Інший численний клас кодів представлений засобами упаковки даних, на зразок програм архівації ARC, ARJ, ICE, ZIP і упаковки дисків на IBM-PC. Застосування цих кодів викликано не таємністю, а прагненням заощадити на вартості передачі або зберіганні повідомлення. Файли текстів, зображень і програм містять інформацію із властивостями, які сильно відрізняються, і програми їхнього кодування повинні бути різними. Якщо архіватор добре стискає текст, це зовсім не означає, що він так само оптимальний для упаковки зображень або інших даних.

Для текстових файлів частіше інших уживається кодування Хаффмана, яке полягає в тому, що символи тексту заміняються послідовностями біт різної довжини. Чим частіше символ, тим коротша відповідна послідовність. Розглянемо приклад кодування Хаффмана [6, 8] слова «МАТЕМАТИКА» з такою таблицею кодування:

Символ	Кількість у тексті	Код
А	3	1
М	4	01
Т	4	001
Е	1	0001
И	1	00001
К	1	00000

Одержимо повідомлення: 01100100010110010000100000 1.

Легко тепер підрахувати, що оскільки вихідне слово складається з 10 символів, то при кодуванні в ASCII він займає 80 біт, у той час як кодоване по Хаффману лише 27 біт.

2.2 Криптографія

Дипломатичні, військові й промислові секрети, як правило, передаються або зберігаються не у початковому вигляді, а після шифрування. На відміну від тайнопису, що приховує сам факт наявності повідомлення, шифрування передаються відкрито, а закривається тільки зміст. Отже, криптографія забезпечує збереження змісту повідомлення за допомогою шифрування й відкриття його розшифровуванням, які виконуються по спеціальних криптографічних алгоритмах за допомогою ключів у відправника й одержувача. Розглянемо класичну схему передачі секретних повідомлень криптографічним перетворенням, де зазначені етапи й учасники цього процесу.

	Шифрування	**Передача**	**Розшифрування**
ТЕКСТ	листок	→	листок
КЛЮЧ	конверт	→	конверт
	Відправник	Канал зв’язку	Одержувач

Зі схеми можна побачити такі особливості й відмінності від звичайних комунікаційних каналів. Відправником шифрується повідомлення за допомогою ключа, і отримане шифрування передається по звичайному відкритому каналу зв’язку

одержувачеві, у той час як ключ відправляється йому по закритому каналу, що гарантує таємність. Маючи ключ і шифрування, одержувач виконує розшифровування й відновлює вихідне повідомлення. Залежно від цілей засекречування ця схема може дещо видозмінюватися. Так, у комп'ютерній криптографії відомі випадки, коли відправник і одержувач одна й та сама особа. Наприклад, можна зашифрувати дані, закривши їх від стороннього доступу при зберіганні, а потім розшифрувати, коли це буде необхідно. У цьому випадку найчастіше роль закритого каналу зв'язку відіграє пам'ять. Проте, у наявності всі елементи цієї схеми.

Криптографічні перетворення використовуються для досягнення двох цілей щодо захисту інформації. По-перше, вони забезпечують неприступність її для осіб, що не мають ключа й, по-друге, підтримують із необхідною надійністю виявлення несанкціонованих підмін.

До необхідних аксесуарів криптографічної техніки крім алгоритмів шифрування й розшифрування належать секретні ключі. Їхня роль така сама, як і в ключів від сейфа.

3 ІСТОРІЯ КРИПТОЛОГІЇ

3.1 Поява шифрів

Ряд систем шифрування дійшов до нас із глибокої стародавності. Швидше за все вони з'явилися одночасно з писемністю в 4 тисячолітті до нашої ери. Методи секретної переписки були винайдені незалежно в багатьох древніх суспільствах таких, як Єгипет, Шумер і Китай. Навіть у Біблії можна знайти приклади шифрувань, хоча мало хто на це звертає увагу. У книзі пророка Єремії (25, 26) читаємо: «...а цар Сессаха вип'є після них». Такого царя або царства не було - невже помилка переписувача? Ні, просто часом священні іудейські тексти зашифровувалися простою заміною. Замість першої букви алфавіту писалася остання, замість другої - передостання й так далі. Цей давній метод шифрування називався атбаш.

Читаючи по ньому слово «сессах», мовою оригіналу одержуємо слово «вавілон», і зміст біблійного тексту може бути прийнятий, навіть, якщо не вірити сліпо в істинність писання.

Багатьом, напевно, відомий шифр заміни, пов'язаний з ім'ям Юлія Цезаря. Щоб розібрати й прочитати лист Цезаря, потрібно читати щораз четверту букву замість першої, наприклад, D замість A і так далі. Це означає, що кожна літера шифрування замінялася четвертою по порядку від неї в алфавіті: $A \to B \to C \to D$, або D замість A. Послання сенату VENI VIDI VICI, тобто ПРИЙШОВ ПОБАЧИВ ПЕРЕМІГ, зроблене Цезарем після одноденної війни з понтійским царем Фарнаком, виглядало б шифровкою SBKF SFAF SFZF.

Не потрібно глузувати над простотою і наївністю перших шифрів - досвід піонерів завжди незграбний. Однак зовсім не до сміху, коли, намагаючись захистити свою працю, сучасні програмісти відтворюють помилки Гаю Юлія - це свідчить про глибокі пробіли у нашій освіті.

Тому дивно було познайомитися з використанням згаданого шифру Цезаря в комп'ютерному довіднику, що містить десятки тисяч адрес організацій і підприємств. При перевірці стійкості шифру, розкриття декількох мегабайт даних, що збиралися по крупинках протягом років, інформації зайняло менше години й від покупки довідника довелося відмовитися. Поміркуйте самі: недосвідчені користувачі на зразок бухгалтерів і фінансистів стали б думати, начебто занесена ними в довідник інформація надійно захищена, у той час як вона легко доступна будь-якому хакеру (і авторам довідника).

Принципово інший шифр, більш давній, пов'язаний з перестановкою літер повідомлення за певним, відомим відправнику й одержувачу правилом. Якийсь хитрун зі спартанців виявив, що якщо смужку пергаменту намотати спіраллю на паличку й написати на ньому уздовж палички текст повідомлення, то, після зняття смужки букви на ній розташуються хаотично. Це так само, якщо б букви писати не підряд, а через домовлене число по порядку доти, поки весь текст не буде вичерпаний.

3.2 Становлення науки криптології

Грецький письменник і історик Полібій винайшов за два століття до нашої ери так званий полібіанский квадрат розміром 5×5, заповнений алфавітом у довільному порядку. Для шифрування на квадраті знаходили букву тексту й вставляли в шифровку нижню від неї в тому самому стовпчику. Якщо буква була в нижньому рядку, то брали верхню з того самого стовпчика. Такого роду квадрати широко використовувалися в пізніших криптографічних системах.

У якості підручних шифрів того часу часто використовувалися таблиці, які дають прості шифрувальні процедури перестановки літер у повідомленні. Ключем у них являються розмір таблиці, фраза, що задає перестановку або спеціальну особливість таблиць. Проста перестановка без ключа - один з найпростіших методів шифрування. Наприклад, повідомлення КРИПТОГРАФІЯ Є НЕБЕЗПЕЧНЕ МИСТЕЦТВО записується в таблицю по стовпцях. Для таблиці з 4 рядків і 8 стовпців це виглядає так:

К	Р	И	П	Т	О	Г	Р
А	Ф	І	Я	Є	Н	Е	Б
Е	З	П	Е	Ч	Н	Е	М
И	С	Т	Е	Ц	Т	В	О

Після того, як відкритий текст записаний рядками, для утворення шифрування він зчитується по стовпцях. Якщо його записувати групами по 4 літери, то вийде: КАЕИ РФЗС ИІПТ ПЯЕЕ ТЄЧЦ ОННТ ГЕЕВ РБМО. Для використання цього шифру відправникові й одержувачеві потрібно домовитися про загальний ключ у вигляді розміру таблиці. Об'єднання літер у групи не входить у ключ шифру й використовується лише для зручності запису тексту без смислу.

Більш практичний метод шифрування [18, 19, 20], названий одиночною перестановкою по ключу, дуже схожий на попередній. Він відрізняється лише тим, що стовпчики таблиці переставляються по ключовому слову, фразі або набору чисел

довжиною із рядок таблиці. Використавши у вигляді ключа слово ЛЮТЕРАНИ, отримаємо таку таблицю:

Л	Ю	Т	Е	Р	А	Н	И
4	8	7	2	6	1	5	3
К	Р	И	П	Т	О	Г	Р
А	Ф	І	Я	Є	Н	Е	Б
Е	З	П	Е	Ч	Н	Е	М
И	С	Т	Е	Ц	Т	В	О

до перестановки,

А	Е	И	Л	Н	Р	Т	Ю
1	2	3	4	5	6	7	8
О	П	Р	К	Г	Т	И	Р
Н	Я	Б	А	Е	Є	І	Ф
Н	Е	М	Е	Е	Ч	П	З
Т	Е	О	И	В	Ц	Т	С

після перестановки.

У верхньому рядку її записаний ключ, а номери під ключем визначені за звичайним порядком відповідних букв ключа в алфавіті. Якщо в ключі зустрілися б однакові букви, вони б нумерувалися зліва направо. Виходить шифротекст: ОПРКГТИР НЯБАЕЄІФ НЕМЕЕЧПЗ ТЕОИВЦТС. Для додаткової безпеки можна повторно зашифрувати повідомлення, що вже було зашифровано. Цей спосіб відомий за назвою подвійна перестановка. Для цього розмір другої таблиці підбирають так, щоб довжини її рядків і стовпців були відмінні від першої таблиці. Найкраще, якщо вони будуть взаємно простими. Крім того, у першій таблиці можна переставляти стовпці, а в другій рядки. Нарешті, можна заповнювати таблицю зиґзаґом, змійкою, по спіралі або іншим способом. Такі способи заповнення таблиці якщо й не підсилюють стійкість шифру, то роблять процес шифрування більш цікавим.

Які ж шифри застосовувалися ще середньовічними вченими? Шифр, що зазвичай називають шифром Гронсфельда

[18], полягає в модифікації шифру Цезаря числовим ключем. Для цього під повідомленням пишуть ключ. Якщо ключ коротший повідомлення, то його повторюють циклічно. Шифрування одержують за аналогією шифру Цезаря, але відраховуючи не третю букву за алфавітом, а ту, яка здвинута на відповідну цифру ключа. Так, застосовуючи як ключ групу із трьох початкових цифр числа π, а саме 314, одержуємо шифровку:

Повідомлення	Ц	І	Л	К	О	М	Т	А	Є	М	Н	О
Ключ	3	1	4	3	1	4	3	1	4	3	1	4
Шифротекст	Щ	Ї	П	Н	П	Р	Х	Б	І	П	О	Т

Щоб зашифрувати першу букву повідомлення «Ц» використовуючи першу цифру ключа 3, відраховується третя по порядку від «Ц» у алфавіті буква «Щ» і виходить буква шифрування «Щ». Шифр Гронсфельда має масу модифікацій, що претендують на його поліпшення, від курйозних, на зразок запису тексту шифрування буквами іншого алфавіту, до неіронічних, як подвійне шифрування різними ключами.

Ще один спосіб шифрування можна описати таблицею шифрування, іноді згадуваною як таблиця Віженера, за ім'ям Блеза Віженера, дипломата XVI століття, що розвивав і вдосконалював криптографічні системи:

	А	Б	В	…	Ю	Я
А	А	Б	В	…	Ю	Я
Б	Я	А	Б	…	Ь	Ю
В	Ю	Я	А	…	Щ	Ь
…	…	…	…	…	…	…
Ю	В	Г	Ґ	…	А	Б
Я	Б	В	Г	…	Я	А

Кожний рядок у цій таблиці відповідає одному шифру заміни подібно шифру Юлія Цезаря для алфавіту. При шифруванні повідомлення його виписують у рядок, а під ним

ключ. Якщо ключ виявився коротший повідомлення, то його циклічно повторюють. Шифрування одержують, знаходячи символ у колонці таблиці по букві тексту й рядку, що відповідає букві ключа. Цей дуже поширений вид шифру зберігся до наших днів. Наприклад, використовуючи ключ АГАВА, з повідомлення ДЕРЖАВНИЙ КОШТ одержуємо таку шифровку:

Повідомлення	Д	Е	Р	Ж	А	В	Н	И	Й		К	О	Ш	Т
Ключ	А	Г	А	В	А	А	Г	А	В		А	А	Г	А
Шифротекст	Д	З	Р	И	А	В	Р	И	Л		К	О	Ю	Т

У комп'ютері така операція відповідає додаванню кодів ASCII символів повідомлення й ключа за деяким модулем. Здається, що якщо таблиця буде більш складною, ніж циклічний зсув рядків, то шифр стане надійніший. Це дійсно так, якщо її міняти частіше, наприклад, від слова до слова. Але створення таких таблиць, що представляють собою латинські квадрати, де будь-яка буква зустрічається в рядку або стовпчику один раз, складне і його варто робити лише на ЕОМ. Для ручного ж поліалфавітного шифру покладаються лише на довжину й складність ключа, використовуючи наведену таблицю, яку можна не тримати в таємниці, а це спрощує шифрування й розшифровування.

Книга архітектора Альберті «Трактат про шифр», написана в 1466 році, являла собою першу у світі наукову працю з криптології, якщо не брати до уваги арабських рукописів, з якими Європа в цей час навряд була добре знайома.

Такі табличні шифри називаються монограмними, тому що шифрування ведеться за однією буквою. Трисемус першим помітив, що можна шифрувати по дві букви за раз. Такі шифри були названі біграмними. Найбільш відомий шифр біграмами називається Playfair. Він застосовувався Великобританією в Першу світову війну.

Шифрування біграмами, запропоноване абатом Трисемусом у його праці «Поліграфія», одразу підсилило стійкість шифрів до розкриття. Зважаючи на те, що «Поліграфія» була досить

доступною друкованою книгою, описані в ній ідеї отримали визнання лише трьома століттями пізніше. Є думка, що все це викликано невисокою популярністю серед криптографів Трисемуса, який був богословом, бібліофілом і засновником архівної справи.

Але згодом, криптологія стала давати плоди. Розгром Великої Армади в 1588 році в значній мірі був обумовлений міццю англійської криптографічної школи, яка легко проводила аналіз іспанських шифрів й, яка інформувала про всі пересування ворожих судів.

До XVIII століття криптографія остаточно склалася у вигляді самостійної науки. Однак незважаючи на наявність професійних криптологів, що перебувають на державній службі, і постійного використання шифрів у дипломатії й військовій справі, криптологія ще не вийшла з дитячого віку й нею могли займатися лише обрані, обдаровані одинаки.

3.3 Шифр Хілла

Починаємо з вибору m- буквеного алфавіту й кодуємо кожну букву одним числом із множини $\{0,1,2,...,m-1\}$. Нехай алфавіт містить звичайні 33 літери алфавіту української мови (тобто $m=33$):

А	Б	В	…	Ю	Я
0	1	2	…	31	32

Тепер будемо ставити у відповідність кожній біграмі (α, β) таке число $P=33\alpha+\beta\in\{0,1,...,33^2-1\}$.

Наприклад, біграмі «НІ» є відповідним ціле натуральне число $P=33\cdot17+11=572$. Далі, зручно мати прості правила або функції шифрування й розшифрування. Ці функції повинні здійснювати ін'єктивне відображення:

$P\xrightarrow{f}C\xrightarrow{f^{-1}}P$,

де P - множина відкритих повідомлень (у цьому випадку біграм), але вже у формі чисел із множини $Z/33^2Z=\{0,1,...,33^2-1\}$. Функція шифрування повинна здійснювати перестановку на множині $Z/33^2Z$. Вибір відображення f, що шифрує, найпростіше взяти у вигляді афінного перетворення:

$$C=aP+b\left(\mathrm{mod}\,N^2\right).$$

Тут a, b - цілі числа, $N=33$.

Для того, щоб існувало обернене відображення f^{-1}, необхідно вимагати, щоб $(a,N^2)=1$. Тобто, a і N^2 – взаємно прості. У цьому випадку:

$$P=f^{-1}(C)=a^{-1}C-a^{-1}b\left(\mathrm{mod}\,N^2\right).$$

Приклад 3.1

Якщо використовувати кодування над заданим алфавітом, то модуль $N=33$. Будемо шифрувати біграму «НІ», код якої дорівнює $P=33\cdot17+11=572$. Нехай функція шифрування має вид:

$$f(P)=5P+6\left(\mathrm{mod}\,33^2\right).$$

Така функція припустима, тому що числа 5 і 33 взаємно прості. Отже,

$$f(P)=5\cdot572+6\equiv688\left(\mathrm{mod}\,33^2\right),$$

$$688=33\cdot20+28.$$

Коду $(20,28)$ відповідає біграма «РШ». Отже, відкритий текст «НІ» переходить у шифрований текст «РШ».

Функція розшифрування

$$f^{-1}(C)=a^{-1}C-a^{-1}b\left(\mathrm{mod}\,33^2\right).$$

Дійсно,

$$f^{-1}(C)=a^{-1}(aP+b)-a^{-1}b=$$

$$=a^{-1}aP+a^{-1}b-a^{-1}b=P\left(\mathrm{mod}\,33^2\right).$$

У нашому прикладі

$$f^{-1}(C) = 5^{-1} \cdot 688 - 5^{-1} \cdot 6 \left(\mathrm{mod}\, 33^2\right),$$

але

$$5^{-1} \equiv 218 \left(\mathrm{mod}\, 33^2\right),$$

і тому

$$f^{-1}(C) = f^{-1}(688) = 218 \cdot 688 - 218 \cdot 6 \equiv 572 \left(\mathrm{mod}\, 33^2\right),$$

$$572 = 33 \cdot 17 + 11,$$

що є закодованим значенням біграми «HI».

Для розкриття шифрованого тексту можна застосувати частотний аналіз. У довгій послідовності шифрованого тексту виділяємо найбільш часто уживані біграми й зіставляємо їх з відомими частотами біграм українського тексту. Ця інформація часто дозволяє визначити a й b функції шифрування.

Приклад 3.2

Нехай відомо, що супротивник використовує криптосистему з 27-буквеним алфавітом, у якій літери $A - Z$ мають числові еквіваленти $[0..25]$ і пробіл - 26. Кожній біграмі відповідає числовий еквівалент – ціле число між 0 і $728 = 27^2 - 1$, обумовлене за правилом $27x + y$, де x й y - числові еквіваленти літер біграми. Нехай аналіз великої послідовності шифрованого тексту показав, що найчастіше в ньому зустрічаються біграми «*ZA*», «*IA*», «*IW*» (у зазначеному порядку). Припустимо, що найчастішими біграмами в англійській мові (у 27 – буквеному алфавіті) є «*E*» і пробіл, «*S*» і пробіл, пробіл і «*T*». Ми знаємо, що криптосистема використовує афінне відображення, яке шифрує по $27^2 = 729$ модулю. Знайдемо ключі шифрування й дешифрування і прочитаємо шифроване повідомлення «NDXBHO». Ми знаємо, що відкритий текст зашифровується за правилом $C = aP + b \left(\mathrm{mod}\, 729\right)$, і що шифрований текст може бути розшифрований за правилом $P = a'C + b' \left(\mathrm{mod}\, 729\right)$, де a і b

утворюють ключ шифрування, а a' і b' - ключ дешифрування. Знайдемо спочатку a' і b'. Нам відомо, як розшифровуються три біграми. Замінивши ці біграми їхніми числовими еквівалентами:

$ZA = 27 \cdot 25 + 0 = 675$,

$IA = 27 \cdot 8 + 0 = 216$,

$IW = 27 \cdot 8 + 22 = 238$,

одержимо три рівності:

$$675a' + b' \equiv 134 \pmod{729},$$

$$216a' + b' \equiv 512 \pmod{729},$$

$$238a' + b' \equiv 721 \pmod{729}.$$

З перших двох рівностей можна одержати:

$$459a' \equiv 351 \pmod{729},$$

$$b' = 134 - 675 \cdot 374 \equiv 647 \pmod{729},$$

що не дає однозначного розв'язку, тому що НСД $(459, 27) > 1$. З першої і третьої рівностей можна одержати:

$$437a' \equiv 142 \pmod{729}.$$

Отже,

$$a' = 362 \cdot 142 \equiv 374 \pmod{729},$$

$$b' = 134 - 675 \cdot 374 \equiv 647 \pmod{729}.$$

Тепер застосуємо перетворення дешифрування до біграм «*ND*», «*XB*» і «*HO*» нашого повідомлення (їм відповідають цілі числа 354, 622 і 203 відповідно) і одержимо числа 365, 724 і 24. Записавши $365 = 13 \cdot 27 + 14$, $724 = 26 \cdot 27 + 22$, $24 = 0 \cdot 27 + 24$, ми з'єднаємо біграми відкритого тексту у повідомлення «NO WAY». Нарешті, для знаходження ключа шифрування ми обчислюємо:

$$a \equiv a'^{-1} \equiv 374^{-1} \equiv 614 \pmod{729},$$

$$b \equiv -a'^{-1}b' \equiv -614 \cdot 647 \equiv 47 \pmod{729}.$$

3.4 Матриці, що шифрують

Нехай є N - буквений алфавіт і нам необхідно передавати біграми як елементи повідомлення. Кожній біграмі відповідає ціле число за модулем N^2. Інший спосіб складається у зіставленні у відповідність біграмі деякого двовимірного вектора (x, y) з x і y узятими за модулем N. Наприклад, якщо є 29-буквений алфавіт із числовими еквівалентами $[0..28]$ відповідно, то біграмі «NO» відповідає вектор $(13,14)$. Далі, беремо у якості ключа 2×2 матрицю A за модулем $N = 29$, яка має обернену, з елементами із множини $[0..28]$. Варто сказати, що всі обчислення з матрицями проводяться за модулем $N = 29$ (у цьому прикладі), і що існує обернена матриця A^{-1} тоді й тільки тоді, коли $\det A \neq 0 (\mathrm{mod}\, 29)$.

Далі, кожний символ вихідного тексту замінюється відповідним кодом. Якщо довжина отриманого вектора v більше n, то розбиваємо вектор v на вектори v_j з n координатами кожний. Якщо в останньому векторі координат менш n, то доповнюємо цей вектор до довжини n пробілом (наприклад). Розташовуємо вектори v_j по стовпцях матриці розміру $n\times k$, де k – кількість векторів v_j. Добуток Av_j дає стовпці матриці шифрованого тексту: $B = \left(Av_1 \middle| Av_2 \middle| ... \middle| Av_k\right)$. Усі обчислення проводяться за модулем N.

Приклад 3.3

Нехай маємо такий алфавіт:

A	B	…	Z	.	?	_
0	1		25	26	27	28

Потужність алфавіту $N = 29$, і будемо шифрувати біграми із фрази «HOW ARE YOU?» = (7 14 22 28 0 17 4 28 24 14 20 27). Нехай матриця, що шифрує:

$$A = \begin{pmatrix} 3 & 12 \\ 2 & 13 \end{pmatrix},$$

$\det A = 15 \pmod{29}$.

Тоді:

$15^{-1} \equiv 2 \pmod{29}$,

$$A^{-1} = \begin{pmatrix} 26 & 5 \\ 25 & 6 \end{pmatrix} \pmod{29}.$$

Зашифрований текст біграм відкритого тексту:

$Av_1 = (15, 22) = (P, W)$,

$Av_2 = (25, 2) = (Z, C)$,

$Av_3 = (1, 18) = (B, S)$,

$Av_4 = (0, 24) = (A, Y)$,

$Av_5 = (8, 13) = (I, N)$,

$Av_6 = (7, 2) = (H, C)$.

Зашифрований текст приймає такий вигляд:

PWZCBSAYINHC

Для розшифрування законний одержувач розбиває отриманий текст на біграми й до кожної з них застосовує матрицю A^{-1}, одержуючи вихідний відкритий текст:

$A^{-1}(15, 22) \equiv (7, 14)$ і т.д.

3.5 Криптологія в Новий час

Новий час привніс нові досягнення в криптографію. Темпи розширення застосування шифрів змусили поставити нову вимогу до них - легкість масового використання, а стара вимога - стійкість до аналізу не тільки залишилася, але й була посилена.

В Англії та США стали виходити періодичні видання, присвячені питанням криптографії, де професіонали й аматори, обмінюючись досвідом, пропонували нові типи шифрів і аналізували їхню стійкість до зламу. Можливо, одного із найбільших успіхів XX століття криптоаналітика домоглася, коли Британська морська розвідка на початку 1917 року передала уряду США текст секретної розшифрованої телеграми (телеграма була перехоплена із трансатлантичного кабелю), відомої як послання Циммермана, який був міністром закордонних справ Німеччини. У ній німецькому послові в Мексиці пропонувалося укласти союз, щоб Мексика захопила американські штати Техас, Нью-Мехіко й Аризону. Ця телеграма, зробила ефект вибуху і, як вважають на даний час історики, стала головним приводом для вступу Північної Америки в Першу світову війну проти Німеччини, принісши її розгром. Так криптографія вперше серйозно заявила про свою винятково велику значущість у сучасному світі.

У XIX столітті із розширенням зв'язних комунікацій зайнялися автоматизацією процесу шифрування. З'явився телеграф, потрібно шифрувати і його. Однак перша практично використовувана криптографічна машина була запропонована Жильбером Вернамом лише в 1917 році. Застосування машин у криптографії розширювалося, що привело до створення приватних фірм, що займаються їхнім серійним випуском. Шифрувальна апаратура створювалася в Німеччині, Японії, США й ряді інших розвинених країн.

У всіх найбільших боях незримо брали участь шифрувальники й розшифровувачі: без їхньої підтримки ціна перемоги могла б стати набагато вища. У романах, популярних статтях і спогадах нам доводилося читати про знаменитого розвідника Кузнєцова, що назвав дату настання німецьких військ під Курським. Можливо, така версія має право на існування, але остаточне рішення про цю битву було прийнято після того, як буквально за добу вітчизняні криптоаналітики розкрили шифрований наказ Гітлера про напад. Усе було начебто звичайно: перехопивши радіограму, зв'язківці пізнали

почерк радиста ставки головнокомандуючого супротивника, а за характером передачі допустили, що вона містить дуже важливий наказ. Криптологи знали, що мова може йти про великий наступ й припустили, що наприкінці документа перебуває підпис єдиної людини, що могла видати цей наказ - Адольфа Гітлера. Далі йде вже техніка аналізу шифру: через відому довжину тексту розкривається ключ, а ключем розшифровується весь інший текст. Можна було сумніватися в правильності повідомлення Кузнєцова: чи немає там дезінформації, гри контррозвідки супротивника, але не довіряти дійсності наказу військам уже не доводилося.

4 МАТЕМАТИЧНІ ОСНОВИ

4.1 Алгебра

4.1.1 Відношення еквівалентності

Почнемо з формального визначення. Підмножина R множини $A \times A$ задає бінарне відношення на множині A [1].

Наведемо такі приклади.

1. На множині Q задамо бінарне відношення R, припустивши $\{(x, y)\}_{0 \le x \le 1, 1 \le y \le 2}$.

Якщо $(a,b) \in R$, то пишуть aRb і говорять, що a перебуває у відношенні R до b Так, наприклад $(1,2) \in R$, тобто $1R2$, а $(2,1) \notin R$.

2. Множина A складається з усіх цілих чисел: $A = Z$. Елементи множини можуть бути парними або непарними числами. Два парних числа перебувають у відношенні R (або два непарних числа), якщо нас цікавить тільки їхня подільність на два. Це бінарне відношення можна задати правилом

$$(m,n) \in R \Leftrightarrow \frac{m-n}{2} \in \boldsymbol{Z},$$

або, інакше,

$R = \{(2m, 2n) \cup (2k+1, 2l+1)\}_{m.n.k.l \in Z}$.

Множина Z всіх цілих чисел розпадається на дві підмножини

$\boldsymbol{Z} = \{0, \pm 2, \pm 4, ...\} \cup \{1, \pm 3, \pm 5, ...\}$,

складаються з однакових з погляду даного бінарного відношення чисел.

Бінарне відношення ~ на множині A називається відношенням еквівалентності, якщо виконуються три умови:

E_1: $a \sim a$ (рефлексивність);

E_2: якщо $a \sim b$, то $b \sim a$ (симетрія);

E_3: якщо $a \sim b$, $b \sim c$, то $a \sim c$ (транзитивність).

3. Множина $A = \{0, 1, 2, 3, ...\}$. Якщо числа m й n при діленні на 7 мають однакові залишкові частини, то вони вважаються еквівалентними. Отже, елементи 1, 8, 15 еквівалентні.

4. Серед усіх функцій $P(x) = x^2 + px + 1$ (це множина A) еквівалентні ті функції, які рівні в точці x_0.

5. На множині всіх підмножин даної множини X підмножини Y й Z еквівалентні, якщо $Y \subseteq Z$.

Повернемося до прикладу 3 і випишемо множини еквівалентних між собою елементів:

$A_0 = \{0, 7, 14, 21, ...\}$;

$A_1 = \{1, 8, 15, 22, ...\}$;

$A_2 = \{2, 9, 16, 23, ...\}$;

$A_3 = \{3, 10, 17, 24, ...\}$;

$A_4 = \{4, 11, 18, 25, ...\}$;

$A_5 = \{5, 12, 19, 26, ...\}$;

$A_6 = \{6, 13, 20, 27, ...\}$.

Відношення між елементами множини A, що задовольняє умови $E_1 - E_3$ (відношення еквівалентності), має важливу властивість, через яку було уведене поняття еквівалентності.

Теорема 4.1

Якщо відношення ~ є відношенням еквівалентності на множині A, то множина A розбивається на непересічні (без загальних елементів) класи еквівалентних елементів.

Множина класів еквівалентних елементів називається фактор множиною множини A по відношенню еквівалентності ~ і позначається $A/\sim$.

Таким чином, елементами множини $A/\sim$ є класи еквівалентних елементів множини A. Нагадаємо, що класи еквівалентних елементів позначають за допомогою квадратних дужок $[\ ]$. У дужках записаний (любий) представник класу. У прикладі 3 виходить сім класів $[0]$, $[1]$, $[2]$, $[3]$, $[4]$,.$[5]$, $[6]$. Ті самі класи можна записати й інакше (наприклад, $[14]$, $[22]$, $[72]$, $[143]$, $[81]$,.$[82]$, $[132]$).

4.1.2 Відображення

Досить часто мова буде йти про різні відображення однієї множини A в інше B:

$f: A \to B$.

Якщо з рівності $f(a) = f(a')$ слідує, що $a = a'$, то відображення $f: A \to B$ називається ін'єктивним відображенням або, інакше, якщо із $a \neq a'$ слідує, що $f(a) \neq f(a')$, то $f: A \to B$ – ін'єктивне відображення.

Відображення $f: \boldsymbol{R} \to \boldsymbol{R}$, де $f(x) = e^x$ ін'єктивне, а відображення $f(x) = x^2$ не є таким, тому що, наприклад, $f(-1) = 1$, $f(1) = 1$.

Відображення $f: A \to B$ називається сюр'єктивним (відображення на), якщо для кожного $b \in B$ існує $a \in A$ таке, що $f(a) = b$ або, інакше, область значень відображення f – уся множина B.

Так, відображення $f(x)=e^x$ сюр'єктивне, якщо $f:\boldsymbol{R}\to(0,+\infty)$, і не є таким, якщо $f:\boldsymbol{R}\to[0,+\infty)$.

Відображення $f:A\to B$ називається бієктивним, якщо воно ін'єктивне й сюр'єктивне.

Одиничним (або тотожним) відображенням $i_A:A\to A$ називається відображення, що переводить кожний елемент $x\in A$ у себе. Це бієктивне відображення.

Будь-яка строго монотонна функція, яка визначена на множині $X\subset\boldsymbol{R}$ з областю значень $Y\subset\boldsymbol{R}$ дає приклад бієктивного відображення:

$f:X\to Y$.

Відображення $f:\boldsymbol{R}\times\boldsymbol{R}\to\boldsymbol{R}$, задане співвідношенням $f(x,y)=ax+by$, буде сюр'єктивним, але не бієктивним відображенням, тому що, наприклад $f(b,-a)=f(-b,a)$.

Нехай $f:A\to B$, $g:B\to C$ – відображення. Композицією відображень f і g (позначається gf) називається відображення $gf:A\to C$, що визначається співвідношенням $(gf)(x)=g[f(x)]$ для всіх $x\in A$.

Так, наприклад, якщо $f:R\to R$, де $f(x)=\pi x$, а $g:R\to R$, де $g(y)=\sin y$, те $(gf)(x)=\sin\pi x$.

Важливою властивістю композиції відображень є ассоціативність: якщо $h:A\to B$, $g:B\to C$, $f:C\to D$, то

$f(gh)=(fg)h$.

Нехай $f:A\to B$ – відображення. Якщо існує відображення $g:B\to A$ із властивостями:

$fg=i_B;\ gf=i_A$,

де $i_A(a)=a$, $i_B(b)=b$ при всіх a із A, b із B, то g називається оберненим відображенням і позначається f^{-1}.

Теорема 4.2

Для того щоб відображення f мало обернене, необхідно й достатньо, щоб воно було бієктивним.

Теорема 4.3

Якщо відображення $f : A \to B$ має обернене, то це останнє визначається однозначно.

За допомогою відображення $f : A \to B$ можна задати відношення еквівалентності. Будемо вважати, що $x, y \in A$ перебувають у відношенні ~ тоді й тільки тоді, коли $f(x) = f(y)$:

$x \sim y \langle = \rangle f(x) = f(y)$.

Відношення ~ рефлексивне, тому що $f(x) = f(x)$, симетричне, тому що $f(x) = f(y) \Rightarrow f(y) = f(x)$, і транзитивне, тому що $f(x) = f(y),\ f(y) = f(z) \Rightarrow f(x) = f(z)$.

Введемо канонічне відображення P:

$$P : \begin{cases} A \to A/\sim, \\ x \to [x] \end{cases},$$

і відображення

$$\overline{f} : \begin{cases} A/\sim \to B, \\ [x] \to f(x) \end{cases}.$$

Неважко перевірити, що f задано правильно (говорять, що воно задано коректно), тобто, що значення f не залежить від вибору представника класу $[x]$. Дійсно, нехай $x' \in [x]$. Тоді $f(x) = f(x')$ й $\overline{f}([x]) = f(x') = f(x)$.

Тепер можна відображення f представити у вигляді композиції сюр'єктивного й ін'єктивного відображень:

$$f = \overline{f} P, \qquad (4.1)$$

де P – сюр'єктивне, а $\overline{f}$ – ін'єктивне.

Вираз (4.1) називається факторизацією відображення f.

Слід додати, що кожне відношення еквівалентності породжує деяке відображення f. При цьому, факторизуючи отримане відображення, одержуємо вихідне відношення еквівалентності.

Приклад 4.1

Нехай $A = \boldsymbol{Z}_7$ - множина класів лишків із прикладу 3. Відображення $f : \boldsymbol{Z}_7 \to \boldsymbol{Z}_7$, де $f([x]) = [2x^5 + x^3 - 2x]$, бієктивне, тому що $f([5]) = [2]$, а $f([i]) = [i]$ для $i = 0,1,2,3,4,6$.

4.1.3 Групи

Наведемо визначення й приклади.

Якщо на множині E визначений внутрішній закон композиції T, (тобто віднесення парі елементів a і b третього елемента $c = aTb$), що задовольняє вимогам:

1) він асоціативний - $cT(aTb) = (cTa)Tb$,

2) у E є нейтральний елемент e - $aTe = eTa = a$, (тепер він буде називатися одиничним елементом або одиницею групи),

3) для кожного елемента існує симетричний йому елемент a^{-1} - $a^{-1}Ta = aTa^{-1} = e$ (тепер він буде називатися оберненим до a), то множина E разом із цим законом композиції називається групою.

Наведемо приклади.

1. Множина Z з додаванням, як закон композиції є групою. Нейтральним елементом є число 0, симетричним елементу N є число $-N$.

2. Множина цілих чисел, кратних фіксованому цілому числу $p \neq 0$, утворює групу відносно додавання цілих чисел. Ця група позначається $p\boldsymbol{Z}$. Так, всі парні цілі числа утворюють групу $2\boldsymbol{Z}$.

3. Множина класів лишків за модулем p з додаванням $[a]+[b]=[a+b]$ утворює групу. Нейтральним елементом є клас $[0]$, а симетричним до класу $[a]$ є клас $[-a]$. Зокрема, позначаючи клас, симетричний до $[a]$, через $-[a]$, маємо, що $-[a]=[-a]$. Крім того, ясно, що $-[1]=[p-1]$, $-[2]=[p-2]$ і т.д.

Група прикладу 3 (з розділу 4.1.1) позначається $\boldsymbol{Z}/p\boldsymbol{Z}$ й називається групою лишків цілих чисел за модулем p. Ця група скінчена й містить p елементів.

4. Множина всіх бієктивних відображень $f: E \to E$ множини E в себе є група відносно закону $g \cdot f$. Дійсно, цей закон асоціативний, має одиничний елемент (тотожнє відображення $1: E \to E$) і кожне відображення $f: E \to E$ має обернене $f^{-1}: E \to E$.

5. Назвемо словом довжини N послідовність із N нулів і одиниць і на множині E всіх слів довжини N введемо операцію + в такий спосіб. Нехай $\varepsilon = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_N)$, $\eta = (\eta_1, \eta_2, ..., \eta_N)$ - слова довжини N.

Тоді покладемо:

$(\varepsilon_1, \varepsilon_2, ..., \varepsilon_N) + (\eta_1, \eta_2, ..., \eta_N) = (\varepsilon_1 + \eta_1 \pmod 2,$

$\varepsilon_2 + \eta_2 \pmod 2,$

…

$\varepsilon_N + \eta_N \pmod 2)$.

Наприклад, $(0,1,1,0,1) + (1,1,0,0,1) = (1,0,1,0,0)$.

Доведемо, що множина E є група відносно операції $+$. Закон $+$ асоціативний. Для доведення потрібно перевірити, що $\varepsilon + (\eta + \chi) = (\varepsilon + \eta) + \chi$. Але це відразу слідує з таблиці додавання по $(\mathrm{mod}\, 2)$:

$0+0=0$, $1+0=1$, $0+1=1$, $1+1=0$.

Нейтральний елемент – слово $(0,0,...,0)$. Симетричним елементу $\varepsilon=(\varepsilon_1,\varepsilon_2,...,\varepsilon_N)$ є саме слово $\varepsilon=(\varepsilon_1,\varepsilon_2,...,\varepsilon_N)$.

Для того випадку, коли закон групи комутативний $(a\text{т}b=b\text{т}a)$, група називається комутативною або абелевою, її закон композиції позначається $+$, нейтральний елемент називається нулем групи й позначається 0, а обернений елемент називається протилежним і позначається $-a$.

4.1.4 Підгрупи

Група $G=\{1,-1,i,-i\}$ відносно множення містить частину $H=\{+1,-1\}$, яка відносно того самого множення утворює групу. Така можливість виділяється таким визначенням: підгрупою H групи G називається така підмножина множини G, яка сама утворює групу відносно закону композиції групи G.

Теорема 4.4

Підмножина H групи G утворює підгрупу тоді й тільки тоді, коли приналежність x, y до H породжує приналежність до H елементів xy і x^{-1}.

Теорема 4.5

Якщо K – підгрупа групи H, H – підгрупа групи G, то K – підгрупа групи G.

1. Знайдемо всі підгрупи адитивній (відносно додавання) групи Z. Нехай $H\in \boldsymbol{Z}$, – підгрупа групи Z. Якщо H відмінно від підмножини $\{0\}$, то H містить деяке найменше $p>0$. Тоді – $p\in H$ і $np\in H$ при всіх $n\in Z$. Нехай $b\in H$, $b=kp+r$, $k\in Z$, $0\le r<p$. Тоді $b-r=kp\in H$ й $r=(b-r)-b\in H$. Тому що $r<p$ й $r\in H$, то $r=0$. Отже, $H=\{kp\}_{k\in Z}$.

Інших підгруп адитивна група Z не має.

2. Знайдемо всі підгрупи групи $Z/6Z$. Якщо H – підгрупа групи $Z/6Z$ й $[1]\in H$, то $H=Z/6Z$, тому що разом із класом $[1]$ H містить класи $[2]=[1]+[1]$, $[3]=[2]+[1]$. Нехай клас $[1]\overline{\in} H$, а клас $[2]\in H$. Тоді клас $[4]\in H$ і $H=\{[0],[2],[4]\}$, причому класи $[2]$ і $[4]$ взаємно протилежні. Нехай класи $[1]\overline{\in} H$, $[2]\overline{\in} H$, а клас $[3]\in H$. Тоді $H=\{[0],[3]\}$ і клас $[3]$ збігається зі своїм протилежним.

Інших підгруп група $Z/6Z$ не має, тому що якщо клас $[4]\in H$, то й клас $[2]=[4]+[4]\in H$, а якщо клас $[5]\in H$,те й клас $[5]=[1]\in H$.

3. Група $Z/5Z$ не має нетривіальних підгруп. Дійсно, якщо H – її підгрупа й клас $[1]\in H$, то $[2]=[1]+[1]\in H$ й т.д., тобто $H=Z/5Z$. Якщо клас $[3]\in H$, то $[1]=[3]+[3]\in H$. Якщо клас $[4]\in H$, то $[1]=-[4]\in H$.

Надалі буде показано, що група лишків по простому модулю p не має нетривіальних підгруп.

Теорема 4.6

Перетин будь-якого числа підгруп H_α групи G є підгрупою групи G.

Група G називається циклічної, якщо існує такий елемент $a\in G$, що кожний елемент $b\in G$ має вигляд $b=a\cdot a\cdot\ldots\cdot a=a^k$ (в адитивній групі відповідно $b=a+a+\ldots+a=k\cdot a$).

Група G має скінченний порядок N, якщо вона містить N елементів. Якщо циклічна група з утворюючим елементом a має порядок N, то $a^n=e$. Дійсно, кожний елемент групи має вигляд a^k, $k=0,1,\ldots$Зауважимо, що всі елементи $e,a,a^2,\ldots,a^{n-1}$ різні. Дійсно, якби $a^m=a^k$ при $m\neq k$, $m,k<n$, то $a^{|m-k|}=e$ й

число елементів групи менше N. Якщо $a^n \neq e$, то обов'язково $a^n = a^m$ при $0 < m < n$, тобто $a^{n-m} = e$, що неможливо.

Нехай G – комутативна група, H – її підгрупа.

Твердження $y^{-1}x \in H\left(xy^{-1} \in H\right)$ рівносильне твердженню $x \in yH\left(x \in Hy\right)$. Використовуючи нові позначення, можна сказати, що кожна підгрупа H визначає два відношення еквівалентності. Класами еквівалентних елементів є множини $[y] = yH$, $\left([y] = Hy\right)$. Ці класи називаються лівими (правими) класами суміжності по підгрупі H, а для комутативної групи ліві й праві класи очевидно збігаються.

Число різних класів суміжності по підгрупі H називається індексом підгрупи H й позначається $(G: H)$. Індекс $(G: H)$ може бути скінченим (і підгрупа H називається підгрупою кінцевого індексу) і нескінченним (підгрупа нескінченного індексу) числом.

Приклад 4.7

В адитивній групі Z число суміжних класів по підгрупі nZ дорівнює n: $\left(Z : nZ\right) = n$.

Дійсно, елементи $0,1,2,...,N-1$ породжують різні класи суміжності (тому що $k-1$ при $k \neq l$, $0 < k$, $l < n$ не є кратним N). Будь-яке ж інше ціле число m можна записати у вигляді $m = p \cdot n + r$, $0 \leq r < p$ і, отже, як наслідок, $m - r = p \cdot n \in H$.

Тому $m \in r + H$ (замість $m \in rH$, тому що група Z – абелева), тобто $m \in [r]$.

Позначимо порядок групи G через $(G:1); (H:1)$ - порядок її підгрупи.

Теорема 4.8 (Лагранжа)

Нехай G – скінчена група, а H – її підгрупа. Тоді $(G:H) \cdot (H:1) = (G:1)$.

Підгрупа H називається нормальною підгрупою групи G, якщо $xH = Hx$, $\forall x \in G$.

Теорема 4.9

Множина класів суміжності по нормальній підгрупі H групи G утворює групу із законом композиції, обумовленим співвідношенням $[x]\cdot[y]=[x\cdot y]$, *або* $(xH \cdot yH = xy \cdot H)$.

Ця група називається фактор-групою групи G по нормальній підгрупі H й позначається G/H.

4.1.5 Циклічні групи

Група G називається циклічної, якщо існує елемент $a \in G$ такий, що кожний елемент $b \in G$ є деяким степенем (при мультиплікативному позначенні) елемента a:

$b = a^n$, $n \in Z$. (4.2)

Якщо позначення для групового закону адитивне $aTb = a + b$, то замість (4.2) пишуть $b = na$, $n \in Z$.

Елемент a називається утворюючим групи. Найчастіше лише скінчені циклічні групи називають циклічними (ми залишимо цю назву й для нескінченних груп).

Наведемо приклади.

1. Адитивна група Z – циклічна, якщо $n \in \boldsymbol{Z}$, то $n = n \cdot 1$, де $1 \in \boldsymbol{Z}$.

2. Адитивна група $\boldsymbol{Z}/n\boldsymbol{Z}$ – циклічна. Елемент $[1]$ породжує групу $\boldsymbol{Z}/n\boldsymbol{Z}$: $[q] = q \cdot [1]$.

3. Множина, що містить два елементи e й a, які «перемножуються» за правилами: $e \cdot e = e$, $e \cdot a = a \cdot e = a$, $a \cdot a = e$ утворить циклічну групу.

4. Розглянемо множину G матриць 2×2 виду:

$$A_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Якщо $n \in \boldsymbol{Z}$, то відносно множення матриць G – нескінченна циклічна група з утворюючим елементом

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Дійсно,

$$A_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

а

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix} \in G$$

й

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

т.ч.

$$A_n \cdot A_m = A_{n+m},\ A_n \cdot A_{-n} = A_{-n} \cdot A_n = I \Rightarrow A_{-n} = A_n^{-1}.$$

Таким чином,результат множення матриць не виходить за межі множини G (композиція визначена правильно) і кожний елемент має обернений.

Нехай тепер $n \in \boldsymbol{Z} / p\boldsymbol{Z}$. Тоді група G скінчена, тому що $A_p = I$, (нагадаємо, що в $\boldsymbol{Z} / p\boldsymbol{Z}$ справедливе порівняння $p \equiv 0 \pmod{p}$.

4.1.6 Симетрична група

Нехай $A_n = \{1, 2, ..., n\} \subset \boldsymbol{Z}$.

Підстановкою множини A_n називається бієктивне відображення $A_n \to A_n$.

Якщо π – деяка підстановка множини A_n, то:

$\pi : 1 \to i_1$, $\pi : 2 \to i_2$, …, $\pi : n \to i_n$, $i_j \neq i_k$, при $k \neq j$, $1 \leq i_1, i_2, ..., i_n \leq n$.

Зручний (але трохи громіздкий) запис підстановки:

$$\pi = \begin{pmatrix} 1 & 2 & 3 \dots n \\ i_1 & i_2 & i_3 \dots i_n \end{pmatrix}.$$

Наприклад, при $n = 3$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

дві підстановки, з яких e – тотожна.

Підстановки σ, τ перемножуються відповідно до загального правила композиції відображень: $\sigma \cdot \tau$ визначається так:

$$(\sigma \cdot \tau)(k) = \sigma\left[\tau(k)\right].$$

Наприклад, для підстановок

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

маємо

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

До речі, зауважимо, що $\sigma \cdot \tau \neq \tau \cdot \sigma$.

Множина S_n підстановок елементів з A_n із так визначеним множенням своїх елементів – група. Нейтральний елемент групи - підстановка

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Якщо

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix},$$

то π^{-1} переводить $\pi(k)$ в. k Наприклад,

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Група підстановок S_n елементів з A_n називається симетричною групою степеня n.

Очевидно множина підстановок S_n перебуває в бієктивній відповідності із множиною всіх перестановок елементів $1, 2, ..., n$. Тому справедлива така теорема.

Теорема 4.10

Порядок групи S_n дорівнює $n!$.

Розглянемо деякі прості підстановки.

Транспозицією (p, q), $p \neq q$ називається підстановка, що задовольняє умови:

$\pi(p) = q$,

$\pi(q) = p$,

$\pi(k) = k$, при $k \neq p$, $k \neq q$.

Циклом $(i_1, i_2, ..., i_l)$ довжини l називається підстановка π така, що:

$\pi(i_1) = i_2$, $\pi(i_2) = i_3, \dots$, $\pi(i_{l-1}) = i_l$, $\pi(i_l) = i_1$

$\pi(k) = k \quad k \neq i_1, i_2, ..., i_l$.

Приклади

1. У S_6 підстановка

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{pmatrix},$$

є цикл (2, 3, 4, 5), а підстановка

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix},$$

є добуток циклів

$\tau = (1,6)\cdot(2,3,4,5)$.

2. Цикли (2, 3, 4, 5) і (4, 5, 2, 3) однакові як і (2, 3, 4, 5), (3, 4, 5, 2), (5, 2, 3, 4).

Цикли $(i_1, i_2, ..., i_p)$ й $(j_1, j_2, ..., j_q)$ називаються незалежними, якщо жодне i не дорівнює жодному з j. Ясно, що якщо π й τ – незалежні цикли, те $\pi \cdot \tau = \tau \cdot \pi$.

Значення циклів і транспозицій (для симетричної групи) з'ясовується в таких двох теоремах.

Теорема 4.11

Кожна підстановка є добутоком попарно незалежних циклів.

Наприклад,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 1 & 7 & 8 & 6 & 2 \end{pmatrix} = (1,3,4)\cdot(2,5,6,7,8).$$

Теорема 4.12

Кожний цикл є добуток транспозицій.

Дійсно,

$(i_1, i_2, ..., i_l) = (i_1, i_l)\cdot(i_1, i_{l-1})\cdot ... \cdot (i_1, i_2)$.

Як наслідок, кожна підстановка є добуток транспозицій.

Зауваження. Подання підстановки у вигляді добутку транспозицій не є однозначним. Наприклад,

$(1,3)\cdot(1,2) = (1,2)\cdot(2,3) = (1,2,3)$.

Відзначимо ще таку теорему.

Теорема 4.13

Усяка кінцева група G порядку n ізоморфна деякій підгрупі симетричної групи S_n.

4.1.7 Задачі з розв'язками

Тут сформульовані й наведені розв'язки деяких задач.

Задача 1

У циклічній групі кожна підгрупа також циклічна. Якщо d – дільник порядку групи, то є точно одна підгрупа порядку d.

Розв'язок

Нехай H – підгрупа циклічної групи G й k – найменший позитивний показник, з яким a^k належить H. Всі елементи з H мають вигляд a^l. Якщо $l>0$ й $l=mk+r$, $0\le r<k$, то $a^l=\left(a^k\right)^m\cdot a^r$. Ураховуючи, що $a^l,\left(a^k\right)^m\in H$, то й $a^r\in H$. Але k – найменший позитивний показник. Тому $r=0$. Отже, підгрупа H складається зі степенів елемента a^k, тобто вона циклічна.

Нехай тепер група G скінчена й n – її порядок, а a – утворюючий елемент групи. Якщо d – дільник числа n, то $n=d_1d$. Підгрупа $H=\left\{e,a^{d_1},a^{2d_1},...,a^{d_1(d-1)}\right\}$ має порядок d.

Нехай H' – підгрупа того ж порядку d. Це також циклічна підгрупа з деяким утворюючим a^k. У цьому випадку $a^{kd}=e$ й $a^{kj}\ne e$ при $0<j<d$. Якщо $k<d_1$, то $kd<d_1d=n$ й $a^{kd}\ne e$. Якщо $k\ge d_1$, то $kd\ge n$ й $a^{kd}=a^{ln+j}=a^j$, де $kd=ln+j$, $0\le j<n$. Отже, $j=0$ і $k=ld_1$. У цьому випадку підгрупа складається з елементів $a^{vk}=a^{vid_1}=\left(a^{d_1}\right)^{vl}$, тобто з елементів підгрупи H. Оскільки порядки H й H' збігаються, то $H=H'$.

Задача 2

Довести, що група S_n при $n>2$ не є комутативною.

Розв'язок

Розглянемо підстановки:

$$\sigma=\begin{pmatrix}1&2&3&4&...&n\\2&3&1&4&...&n\end{pmatrix},\ \tau=\begin{pmatrix}1&2&3&4&...&n\\2&1&3&4&...&n\end{pmatrix}.$$

Маємо

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix},\ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 2 & 4 & \dots & n \end{pmatrix}.$$

4.1.8 Кільце

Визначення й приклади.

Якщо на множині A визначені два внутрішніх закони композиції $+$ і $\circ$, перший з яких є закон комутативної групи в A, а другий асоціативний і, крім того, подвійно дистрибутивний щодо першого, тобто:

$a\cdot(b+c)=a\cdot b+a\cdot c$, $(b+c)\cdot a=b\cdot a+c\cdot a$,

то множина A називається кільцем.

Таким чином, закони композиції $+$ і $\circ$ повинні задовольняти таким умовам:

1) $a+(b+c)=(a+b)+c$ (асоціативність);

2) $a+b=b+a$ (комутативність);

3) існує нейтральний елемент 0 такий, що

$a+0=0+a=a$;

4) для кожного елемента a існує симетричний (тепер його називають протилежним) елемент $-a$, причому:

$a+(-a)=(-a)+a=0$;

$a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (асоціативність множення);

$a\cdot(b+c)=a\cdot b+a\cdot c$;

$(b+c)\cdot a=b\cdot a+c\cdot a$ (подвійна дистрибутивність).

Якщо множення в кільці A має нейтральний елемент, то цей елемент називають одиницею кільця A й часто позначають 1.

Кільце A називають комутативним, якщо множення в кільці комутативне.

Наведемо приклади.

1. Визначаючи на множині $\boldsymbol{Z}$ цілих чисел операції додавання й множення цілих чисел, одержуємо приклад комутативного кільця з одиницею.

2. Множина, що складається із двох елементів 0 і 1, у якому додавання й множення визначаються правилами:

$0+0=0,\ 0+1=1,\ 0\cdot 0=0,\ 0\cdot 1=0,1+0=1,\ 1+1=0,\ 1\cdot 0=0,\ 1\cdot 1=1$

є кільце.

3. Сукупність усіх квадратних матриць із n рядками й із цілими (або з дійсними, або з комплексними) елементами зі звичайним додаванням і множенням матриць дає приклад кільця.

4. Сукупність усіх многочленів від однієї змінної x із цілими коефіцієнтами є комутативним кільцем.

5. Розглянемо більш загальний приклад. Нехай A – комутативне кільце. Множина B – сукупність усіх многочленів від однієї змінної x з коефіцієнтами з кільця A. Додавання й множення виконуються за звичайними правилами додавання й множення многочленів. Якщо A – кільце прикладу 2, то в кільці B:

$$\left(x^4+x^3+x+1\right)+\left(x^3+x^2+1\right)=x^4+x^2+x,$$

$$\left(x^4+x^3+x+1\right)\cdot\left(x^3+x^2+1\right)=x^7+x^5+x^3+x^2+x+1.$$

4.1.9 Підкільця, ідеали, фактор-кільця

Підмножина B кільця A, що є кільцем відносно законів композиції кільця A, називається підкільцем кільця A.

Наведемо приклади.

1. Кільце $\boldsymbol{Z}$ прикладу 1 п.4.1.8 є підкільцем кільця $\boldsymbol{R}$ дійсних чисел.

2. Кожна підгрупа $n\boldsymbol{Z}$ адитивної групи $\boldsymbol{Z}$ є підкільцем кільця $\boldsymbol{Z}$, тому що добуток цілих чисел, кратних n, кратний n.

3. Перетин підкілець кільця A є знову підкільцем кільця A.

Визначимо відношення еквівалентності в кільці, що не суперечать заданим у кільці A законам. Для цього дамо таке визначення.

Лівим (правим) ідеалом кільця A називають підгрупу B адитивної групи A таку, що при $x \in B$, $y \in A$: $x \cdot y \in B$, ($y \cdot x \in B$) або, що те саме, $BA \subset B$.

Якщо множина B є одночасно лівим і правим ідеалом кільця A, то його називають двостороннім ідеалом кільця A.

Наведемо приклади.

1. Кільце A є своїм двостороннім ідеалом. Множина $\{0\}$ також є двостороннім ідеалом.

2. У групі $\boldsymbol{Z}$ кожний ідеал, будучи підгрупою, повинен мати вигляд $n\boldsymbol{Z}$. Разом з тим будь-яка підгрупа $n\boldsymbol{Z}$ групи $\boldsymbol{Z}$ є ідеалом в $\boldsymbol{Z}$, тому що добуток будь-якого цілого числа на число, кратне n, буде кратним n, тобто належить $n\boldsymbol{Z}$.

3. Який би не був елемент a кільця A, множини aA, Aa є відповідно лівим і правим ідеалами кільця A.

4. Лівий ідеал не обов'язково буде правим ідеалом. Для доведення досить розглянути кільце матриць порядку 2×2 з дійсними елементами, а в ньому лівий ідеал I, що складається з матриць

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Це дійсно лівий ідеал, тому що

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} \in I.$$

Але добуток

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

не обов'язково належить I:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \overline{\in} I.$$

Теорема 4.14

Якщо ~ є відношення еквівалентності, що не суперечить законам композиції кільця A, то існує такий двосторонній ідеал B кільця A, що

$$a \sim b <=> a - b \in B. \qquad (4.3)$$

Навпаки, нехай B – двосторонній ідеал кільця A. Тоді говорять, що елементи a й b еквівалентні, якщо $a - b \in B$, то ми можемо задати відношення еквівалентності, що не суперечить законам кільця A.

Множина A розбивається на класи еквівалентних елементів: $[a], [b], \ldots$

Якщо $c \in [a]$, то $c \sim a$ й $[a] = [c]$. Оскільки відношення ~ задається ідеалом B, то замість $a \sim b$ пишуть

$$a \sim b \,(\mathrm{mod}\, B)$$

або

$$a \sim b(B)$$

і відношення ~ називають порівнянням за модулем B.

Вважаючи, що $[a]+[b]=[a+b]$, $[a]\cdot[b]=[a\cdot b]$, уведемо у фактор-множину множини A по відношенню ~ два закони композиції, що перетворюють $A/\sim$ у кільце. (Перевірка того, що множення класів визначене коректно, тобто, що результат множення $[a]$ на $[b]$ не залежить від вибору представників a і b класів $[a]$ і $[b]$ не приводиться. Цю перевірку рекомендується виконати самостійно).

Це кільце називається фактор-кільцем кільця A за двостороннім ідеалом B й позначається A/B.

Щоб довести, що A/B – кільце, потрібно перевірити, що A/B – адитивна група відносно додавання класів (а це вже раніше було виконано), і що множення класів задовольняє аксіомам множення в кільці. Але

$$[a]\cdot[b]=[a\cdot b]\in A/B,$$

$$[a]\cdot([b]\cdot[c])=[a]\cdot[b\cdot c]=\big[a\cdot(b\cdot c)\big]=\big[(a\cdot b)\cdot c\big],$$

$$([a]\cdot[b])\cdot[c]=[a\cdot b]\cdot[c]=\left[(a\cdot b)\cdot c\right],$$
$$[a]\cdot([b]+[c])=[a]\cdot[b+c]=\left[a\cdot(b+c)\right]=[a\cdot b+a\cdot c],$$
$$[a]\cdot[b]+[a]\cdot[c]=[a\cdot b]+[a\cdot c]=[a\cdot b+a\cdot c].$$

Наведемо приклади.

1. Фактор-кільце A/A зводиться до одного нульового елемента, тому що будь-які елементи $a,b\in A$ еквівалентні: $a-b\in A$. Тому фактор-кільце A/A складається з одного класу $[0]=A$.

2. Множина $\{0\}$ – ідеал кільця A, що складається з одного елемента 0. Фактор-кільце $A/\{0\}$ можна ототожнити з кільцем A: якщо $[a]=[b]$, то $a\sim b(\mathrm{mod}\{0\})$,тобто $a-b=0$. Тому кожний клас $[a]$ складається з одного елемента a.

3. У кільці $\boldsymbol{Z}$ візьмемо ідеал $n\boldsymbol{Z}$.Фактор-група $\boldsymbol{Z}/n\boldsymbol{Z}$ є й фактор-кільце кільця $\boldsymbol{Z}$. Його елементами є класи еквівалентних елементів: $x, y\in[z]$, якщо $x-z$ й $y-z$ є кратними n. $\boldsymbol{Z}/n\boldsymbol{Z}$ складається з n елементів $[0]$, $[1]$, $[2]$, …, $[n-1]$.

Зауважимо, що фактор-кільце $\boldsymbol{Z}/n\boldsymbol{Z}$ може мати дільники нуля (тоді, як саме кільце $\boldsymbol{Z}$ не має дільників нуля). В $\boldsymbol{Z}/4\boldsymbol{Z}$ ***2≈0 (mod 4)***, але $2\cdot 2\sim 0(\mathrm{mod}\,4)$.

Розглянемо більш докладно останній приклад.

Ідеал B кільця A називається головним, якщо $B=a\cdot A$ при деякому $a\in A$, і позначається (a).

Кільце, у якому кожний ідеал головний, називається кільцем головних ідеалів.

Приклад 4.2

Раніше було показано, що кожний ідеал кільця $\boldsymbol{Z}$ має вигляд $n\boldsymbol{Z}$.

Із приклада 3 видно, що кільце $\boldsymbol{Z}/n\boldsymbol{Z}$ може мати дільники нуля. Але справедлива така теорема.

Теорема 4.15

Кільце $\boldsymbol{Z}/n\boldsymbol{Z}$ *тоді й тільки тоді не має дільників нуля, коли* n *– просте число.*

Приклад 4.3

Нехай $m \geq 1, n \geq 1, m, n \in \boldsymbol{Z}$. Розглянемо суму ідеалів (m) і (n), що складає із усіх елементів виду:

$r + s, r \in (m), s \in (n)$.

Неважко довести, що це знову ідеал кільця $\boldsymbol{Z}$. У кільці $\boldsymbol{Z}$ кожний ідеал головний і, отже, $(m)+(n)=(d)$ при будь-якому d, $(d \geq 1)$. Ідеал (d) містить елементи m й n. Тому $m = m_1 \cdot d$, $n = n_1 \cdot d$ і, отже, d – дільник чисел m і n. Але якщо будь-яке d_1 є дільником m і n, то $m \in (d_1)$, $n \in (d_1)$ і $(m)+(n) \subset (d_1)$. Отже, d – найбільший загальний дільник чисел m і n. Зауважимо також і інше: оскільки $(d) \in (m)+(n)$, то найдуться такі $k_1, k_2 \in Z$, що

$d = k_1 \cdot m + k_2 \cdot n$.

Так, для будь-яких двох взаємно простих чисел m і n найбільший загальний дільник $d = 1$, і, отже, завжди найдуться такі цілі числа k_1 й k_2, що

$1 = k_1 \cdot n + k_2 \cdot m$.

Аналогічно визначається найменше загальне кратне чисел m і n за допомогою перетину ідеалів

$(m) \cap (n)$.

Нехай A, A' - кільця, а $f : A \to A'$ – відображення кільця A в кільце A' таке, що:

$f(a+b) = f(a) + f(b)$,

$f(a \cdot b) = f(a) \cdot f(b)$.

Відображення f називається гомоморфізмом кілець A і A'.

Якщо f – бієктивний гомоморфізм кілець A і A', то він називається ізоморфізмом кілець, а кільця A й A' – ізоморфними.

4.1.10 Кільце многочленів з коефіцієнтами з поля

Широке застосування знаходять кільця многочленів одного змінного X з коефіцієнтами з якогось поля K. Ці кільця позначаються $K[X]$. При множенні й додаванні многочленів коефіцієнти знову одержуваних многочленів не виходять за межі поля K. Точніше,

$p(X), q(X) \in K[X] \Rightarrow p(X) + q(X) \in K[X]$,

$p(X) \cdot q(X) \in K[X]$.

Степенем многочлена $p(X)$ (позначається $\deg p$) називається найбільший степінь X^k, що входить у многочлен, степінь многочлена $p \equiv k$, $k \in K$, $k \in K$, уважається рівною нулю ($\deg p = 0$).

Многочлен називається нормованим, якщо коефіцієнт при найвищому степені X дорівнює 1.

Якщо $p(X), q(X), r(X) \in K[X]$ і $p(X) \cdot q(X) = r(X)$, то многочлен $p(X)$ (або $q(X)$) називається дільником многочлена $r(X)$, а $r(X)$ ділиться на $p(X)$ (або на $q(X)$).

Теорема 4.16

$K[X]$ – кільце без дільників нуля.

Надамо ще одне важливе визначення.

Якщо многочлен $p(X)\in K[X]$ не має дільників меншого степеня, чим $\deg p(X)$, відмінних від константних $(\in K)$ і приналежних $K[X]$, то він називається незвідним у полі K.

Наприклад, багаточлен не X^2+1 приводимо в поле $\boldsymbol{R}$, але не є таким у поле $\boldsymbol{C}$. Багаточлен

$$X^4+4=\left(X^2-2X+2\right)\cdot\left(X^2+2X+2\right)$$

звідний у кожному полі $\boldsymbol{Z}$, $\boldsymbol{Q}$ або $\boldsymbol{R}$. У свою чергу, кожний його співмножник незвідний ні у $\boldsymbol{R}$ ні, тим більше, в $\boldsymbol{Q}$ або $\boldsymbol{Z}$.

Нехай A – поле $\boldsymbol{Z}/(2)$. У кільці $A[X]$ багаточлен X^2+1 звідний, оскільки

$$X^2+1=(X+1)\cdot(X+1).$$

Многочлен X^2+X+1 незвідний у кільці $A[X]$. Дійсно, перепишемо всі можливі багаточлени степеня 1 у кільці $A[X]$. Це X, $X+1$. Якби многочлен X^2+X+1 був звідним у полі A, то він розкладався б на множники степеня 1. Але

$$X^2+X+1\neq X\cdot X,$$
$$X^2+X+1\neq X\cdot(X+1),$$
$$X^2+X+1\neq(X+1)\cdot(X+1).$$

Разом з тим, многочлени X^2+1, X^2+X+1 незвідні (наприклад) у полі $\boldsymbol{R}$. Ми бачимо, що звідність або незвідність многочлена істотно залежить від поля K.

Як і у випадку кільця $Z[X]$ доводиться така теорема.

Теорема 4.17

Для многочленів $p(X)\in K[X]$ і $q(X)\in K[X]$ - діленого й дільника, існують многочлени $d(X)\in K[X]$, $r(X)\in K[X]$ – частка від ділення й остача такі, що

$$p(X)=d(X)\cdot q(X)+r(X), \qquad (4.4)$$

причому степінь $r(X)$ *менше степеня* $q(X)$, *і многочлени* $d(X)$ *й* $r(X)$ *визначені однозначно.*

Розглядаючи ідеал $(p)\cap(q)$, знайдемо многочлен $r(X)$ по формулі

$$(r)=(p)\cap(q),$$

який буде найменшим загальним кратним (НЗК) многочленів $p(X)$ і $q(X)$.

Неважко довести, що для будь-яких многочленів $p(X)$, $q(X)$ найдуться многочлени $s(X)$, $r(X)$ такі, що

$$p(X)\cdot s(X)+q(X)\cdot r(X)=d(X),$$

де

$$d(X)=\textbf{\textit{НСД}}\left(p(X),q(X)\right).$$

Для знаходження НСД двох многочленів можна застосувати алгоритм ділення Евкліда.

4.1.11 Алгоритм ділення Евкліда

Алгоритм ділення Евкліда [18, 20] застосовується для знаходження НСД двох многочленів. Нехай $r_1(x), r_2(x)\in K[X]$, де K – деяке поле, і нехай степінь $r_1(x)$ не менше степеня $r_2(x)$

$$r_1(x)=p_1(x)\cdot r_2(x)+r_3(x),\ \deg r_3(x)<\deg r_2(x). \qquad (4.5)$$

Якщо $r_3(x)\equiv 0$, то, очевидно, що НСД $\left(r_1(X),r_2(X)\right)=r_2(X)$. Нехай $r_3(x)\not\equiv 0$. Тоді

$$r_2(x)=p_2(x)\cdot r_3(x)+r_4(x).$$

Продовжуємо процес ділення до тих пір, поки не одержимо нульову остачу $r_{k+1}(X)=0$. Отже,

$$r_{j-1}(x)=p_{j-1}(x)\cdot r_j(x)+r_{j+1}(x),$$

$$r_{j+1}(X)\equiv 0,\ j=2,3,...,k-1, r_{k+1}(X)\equiv 0.$$

Доведемо, що $r_k(X) = \boldsymbol{НСД}\left(r_1(X), r_2(X)\right)$. Насамперед відзначимо, що

$$r_{k-1}(X) = p_{k-1}(X) \cdot r_k(X),$$

$$r_{k-2}(X) = p_{k-2}(X) \cdot r_{k-1}(X) + r_k(X) =$$

$$= \left[p_{k-2}(X) \cdot p_{k-1}(X) + 1 \right] \cdot r_k(X).$$

Оскільки

$$r_{k-3}(X) = p_{k-3}(X) \cdot r_{k-2}(X) + r_{k-1}(X),$$

і обидва доданки кратні $r_k(X)$, то й $r_{k-3}(X)$ кратне $r_k(X)$. Продовжуємо цей процес до тих пір, поки не прийдемо до многочленів $r_2(X)$ і $r_1(X)$. Отже, $r_k(X)$ – дільник многочленів $r_2(X)$ і $r_1(X)$.

Якщо $d(X)$ – інший дільник тих же многочленів, то

$$r_1(X) = d(X) \cdot q_1(X),$$

$$r_2(X) = d(X) \cdot q_2(X).$$

З цих співвідношень і з (4.5) випливає, що $d(X)$ є дільником многочлена $r_3(X)$. Подібним чином багаточлен $d(X)$ є дільником всіх інших залишків і, зокрема, $r_k(X)$. Таким чином, $r_k(X)$ – найбільший спільний дільник многочленів $r_2(X)$ і $r_1(X)$.

Зауваження. НСД двох многочленів визначається з точністю до постійного множника з K.

4.1.12 Поле

Наведемо визначення й приклади.

Комутативне кільце A, множина ненульових елементів якого утворить групу відносно множення в A, називається полем.

Наведемо приклади.

1. Множина $\boldsymbol{Q}$ раціональних чисел утворює поле відносно звичайного додавання й множення.

2. Множина дійсних чисел $\boldsymbol{R}$ і множина комплексних чисел $\boldsymbol{C}$ утворюють поля відносно законів $+$ і $\times$.

Теорема 4.18

Якщо в кільці A є дільники нуля, то кільце A не може бути полем.

Дійсно, якщо $xy = 0$, $x \neq 0$, $y \neq 0$ й x^{-1} існує, то

$$0 \neq y = 1 \cdot y = x^{-1}xy = \overline{x}^{1}(xy) = x^{-1} \cdot 0 = 0,$$

що неможливо.

Теорема 4.19

Якщо в кільці $A(\neq \{0\})$, що має у своєму складі одиницю, не існує жодного лівого ідеалу, відмінного від $\{0\}$ і A, то A – поле.

Теорема 4.20

Кільце $\boldsymbol{Z}/p\boldsymbol{Z}$ тоді й тільки тоді поле, коли p – просте число (тепер це кільце позначається через $\boldsymbol{Z}_p$ або $\boldsymbol{Z}/(p)$).

Доведення

Як слідує з попередньої теореми, якщо $\boldsymbol{Z}/(p)$ не містить нетривіальних ідеалів, то $\boldsymbol{Z}/(p)$ – поле. Але кожний ідеал кільця $\boldsymbol{Z}/(p)$ є, зокрема, підгрупа адитивної групи $\boldsymbol{Z}/p\boldsymbol{Z}$. Раніше ж було показано , що якщо p просте, то $\boldsymbol{Z}/p\boldsymbol{Z}$ не має нетривіальних підгруп. Навпаки, якщо p – не просте число, то по теоремі 4.18 кільце $\boldsymbol{Z}/(p)$ має дільники нуля й тому не може бути полем.

4.1.13 Скінченні поля

Розглянемо деякі властивості скінченних полів [20]. Нехай G – таке поле. Зважаючи на скінченність поля при деякому $n \in Z$,

$n \cdot e = 0$.

Це значить, що характеристика скінченного поля відмінна від нуля (нагадаємо, що найменше $n > 0$, при якому $n \cdot e = 0$, є характеристика скінченного поля). Виявляється, що не будь-яке число може бути характеристикою скінченного поля.

Теорема 4.21

Характеристика скінченного поля - просте число.

Доведення

Нехай p – характеристика скінченного поля K. Тоді

$p \cdot e = 0$.

Якщо $p = s \cdot t$, $s, t \in N$, $s \neq 1$, $t \neq 1$, то

$(se)(te) = 0$,

а оскільки $se \neq 0$, $te \neq 0$, то поле K має дільники нуля, що неможливо.

Теорема 4.22

У полі K характеристики p справедлива властивість

$(a+b)^p = a^p + b^p$, $a, b \in K$.

Доведення

При $p = 1$ рівність очевидна. Нехай $p > 1$. Тоді

$(a+b)^p = a^p + C_p^1 a^{p-1} \cdot b + C_p^2 a^{p-2} \cdot b^2 + ... + C_p^{p-1} a b^{p-1} + b^p$.

При $0 < k < p$

$kC_p^k = p(p-1) \cdot ... \cdot (p-k+1)$

і

$(k! C_p^k) e = 0$.

Отже,

$(k!e)(C_p^k e) = 0$.

Але $k!e = (1 \cdot e) \cdot (2 \cdot e) ... (k \cdot e) \neq 0$, оскільки p – найменше з тих, при яких $pe = 0$. Оскільки в полі немає дільників нуля, то $C_p^k \cdot e = 0$. Тому $C_p^k \cdot a^{p-k} \cdot b^k = 0$ при $0 < k < p$.

Така теорема показує, що скінченне поле не може мати у своєму складі довільне число елементів.

Теорема 4.23

Будь-яке скінченне поле характеристики p має порядок (тобто кількість елементів поля) p^n при деякому цілому додатному n.

Доведення

Нехай H - поле характеристики p. Якщо $x \in H$, то $p \cdot x = 0$, $(p+1) \cdot x = 1 \cdot x, ...$ Тому можна розглядати поле, як векторний простір над полем $\boldsymbol{Z}/(p)$. Ясно, що цей векторний простір скінченновимірний. Нехай $v_0, v_1, ..., v_{n-1}$ – його базис. Тоді кожний елемент поля можна представити єдиним образом у вигляді

$x = \alpha_0 \cdot v_0 + \alpha_1 \cdot v_1 + ... + \alpha_{n-1} \cdot v_{n-1}$.

Оскільки α_j може набувати тільки $0,1,..., p-1$ значення, то всього різних елементів x є рівно p^n.

Без доведення сформулюємо теорему про ізоморфізм скінченних полів.

Теорема 4.24

Скінченні поля з однаковим числом елементів ізоморфні.

Скінченні поля називаються полями Галуа й позначаються $GF(p^n)$.

Наведемо приклади скінченних полів.

1. Як було раніше показане, якщо p – просте число, то $Z/(p)$ – поле.

2. Поле $GF(2)$ має два елементи 0 і 1, і для них таблиця додавання й множення такі:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	1
1	1	0

3. Поле $GF(4)$ має чотири елементи. Щоб навести приклад поля $GF(4)$ (а всі скінченні поля з однаковим числом елементів ізоморфні), реалізуємо $GF(4)$ як поле класів лишків кільця $K[X]$, де $K = GF(2)$, за модулем деякого незвідного у $K[X]$ многочлена степеня 2. Оскільки в полі $GF(2)$ лише два елементи 0 і 1, то досить знайти серед многочленів:

X^2, X^2+1, X^2+X, X^2+X+1

(більше немає многочленів степеня 2 з коефіцієнтами з $GF(2)$) ті, що є незвідними. Це $p(X) = X^2 + X + 1$. Отже, поле

$$GF(4) = K[X]/(X^2+X+1),\ K = GF(2)$$

має чотири елементи, які можна записати у вигляді

$[0], [1], [X], [1+X]$.

У деяких випадках зручніше користуватися двійковим записом:

$[0] = 00$,

$[1] = 01$,

$[X] = 10$,

$[X+1] = 11$.

Тоді таблиці додавання й множення виглядають так:

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

×	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

4. Розглянемо поле $GF(8)$. Серед усіх многочленів степеня 3 з коефіцієнтами з $GF(2)$:

$X^3,\ X^3+1,\ X^3+X^2,\ X^3+X+1,\ X^3+X^2+1,\ X^3+X^2+X,\ X^3+X^2+X+1$

знайдемо незвідні в $GF(2)$ многочлени. Це, наприклад, X^3+X^2+1. Отже,

$$GF(8)=K[X]/\left(X^3+X^2+1\right),$$

де $K=GF(2)$. Елементи з $GF(8)$ такі

$[0],\ [1],\ [X],\ [X+1],\ \left[X^2\right],\ \left[X^2+1\right],\ \left[X^2+X\right],\ \left[X^2+X+1\right]$

або

$000,\ 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111.$

Побудову таблиць додавання й множення в $GF(8)$ пропонується виконати самостійно.

4.1.14 Класи лишків

Нехай K – поле, B – ідеал кільця $K[X]$. Раніше було встановлено, що $B=(p)$, де $p(X)\in K[X]$. Фактор-кільце $K[X]/(p)$ складається із класів лишків $\left[q(X)\right]$, причому $q_2(X), q_2(X)\in\left[q(X)\right]$, якщо $q_1(X)-q_2(X)\in(p)$, тобто $q_1(X)-q_2(X)$, ділиться на $p(X)$.

Наведемо ряд тверджень відносно класів лишків за модулем (p).

1. У кожному класі $[\cdot]$ лишків є многочлен $q(X)$, степінь якого менше степеня многочлена $p(X)$. Дійсно, якщо

$$q(X)\in[\cdot]\ \text{і}\ q(X)=p(X)\cdot s(X)+r(X),$$

то

$$q(X)-r(X)=p(X)\cdot s(X)\in(p)$$

і тому

$$q(X)\sim r(X)\big(\mathrm{mod}(p)\big).$$

Отже,

$$\big[q(X)\big]=\big[r(X)\big],$$

а степінь многочлена $r(X)$ менше степеня многочлена $p(X)$.

2. Нехай степені многочленів $q_1(X)$, $q_2(X)$ менші степеня многочлена $p(X)$ й, крім того $q_1(X)\neq q_2(X)$. Тоді $\big[q_1(X)\big]\neq\big[q_2(X)\big]$.

Якби $\big[q_1(X)\big]=\big[q_2(X)\big]$, то $q_1(X)-q_2(X)=p(X)\cdot s(X)$. Але степінь многочлена $q_1(X)-q_2(X)$ менше степеня многочлена $p(X)\cdot s(X)$ й тому $s(X)=0$, тобто $q_1(X)=q_2(X)$.

3. Нехай $p(X)\in K[X]$. Кільце $K[X]/(p)$ є полем тоді й тільки тоді, коли $p(X)$ – незвідний у полі K многочлен.

Приклад 4.4

Нехай $K=\boldsymbol{R}$ і $p(X)=X^2+1$. Тоді кільце $\boldsymbol{R}[X]/\big(X^2+1\big)$ є полем, тому що в полі $\boldsymbol{R}$ многочлен X^2+1 незвідний. У кожному класі $[\cdot]$ є представник – многочлен степеня ≤ 1. Класи $[1]$, $[X]$ різні. Тому кожний клас лишків можна задати у вигляді

$$[\alpha+\beta X],$$

де $\alpha,\beta\in\boldsymbol{R}$. У цьому полі

$$[X]^2+[1]=[0],$$

тому що

$[X]^2+[1]=\left[X^2+1\right]=[0]$.

Клас $[X]$ є «розв'язком» рівняння $X^2+1=0$. Таким чином, крім елементів виду

$[\alpha], \alpha\in \boldsymbol{R}$,

(а всі такі елементи різні) поле $F=R[X]/\left(X^2+1\right)$ містить якийсь «новий» елемент $[X]$, який можна вважати розв'язком рівняння X^2+1, не маючий у полі $\boldsymbol{R}$ розв'язків. Поле F «ширше» поля K за рахунок додавання нових елементів.

Наведемо приклади.

У прикладах, що будуть розглядатися $K=\boldsymbol{Z}/(2)$.

1. $\boldsymbol{НСД}\left(X^2+1, X+1\right)=X+1$, тому що $X+1$ – дільник многочлена X^2+1.

2. $НСД\left(X^3+X, X^4+X^3+X^2+X\right)=X\left(X+1\right)^2=X^3+X$, тому що в полі K

$X^3+X=X\left(X^2+1\right)=X\left(X+1\right)^2$,

$X^4+X^3+X^2+X=X\left(X^3+X^2+X+1\right)=X\left(X+1\right)^3$.

$НСК\left(X^3+X, X^4+X^3+X^2+X\right)=X\left(X+1\right)^3=$

$=X^4+X^3+X^2+X$

3. $НСД\left(X^2+X+1, X^3+X\right)=1$, тому що многочлен X^2+X+1 незвідний, і X^2+X+1 не є дільником многочлена X^3+X.

$НСК\left(X^2+X+1, X^3+X\right)=\left(X^2+X+1\right)\times\left(X^3+X\right)=$

$=X^5+X^4+X^2+X$.

4.2 Теорія Чисел

4.2.1 Визначення

Множина цілих чисел $\{...,-3,-2,-1,0,1,2,3,...\}$ позначається символом Z.

Якщо ціле число a ділить ціле b націло, то a – дільник b (divisor) або множник b (factor), тобто існує ціле c таке, що $b = a \cdot c$ й пишуть a/b. Наприклад, $3/18$, $173/0$.

Доречними будуть такі елементарні твердження.

Для всіх $a,b,c \in Z$:

1) a/a;

2) якщо a/b й b/c то a/c;

3) якщо a/b й a/c, то $a/(bx+cy)$ для всіх $x, y \in Z$;

4) якщо a/b й b/a, то $a = \pm b$.

5) ділення цілих чисел (division for integers) - якщо a й b – цілі числа й $b \neq 1$, то найдуться q - частка від ділення (the quotient), r – остача від ділення (the remainder) такі, що $a = qb + r$, де $0 \le r < b$.

Крім того, q і r визначаються єдиним чином. Остача позначається $a(\mathrm{mod}\, b)$, а частка – $a(\boldsymbol{div} b)$.

Наприклад, якщо $a = 73$, $b = 17$, то $q = 4$ й $r = 5$. Отже, $73(\mathrm{mod}\, 17) = 5$ і $73(\boldsymbol{div}\, \boldsymbol{17}) = \boldsymbol{4}$.

Наведемо визначення.

Ціле число c називається загальним дільником a і b, якщо c/a й c/b.

Найбільший із усіх загальних дільників d цілих a і b позначається $\gcd(a,b)$ або $НСД(a,b)$.

За визначенням $\gcd(0,0) = 0$.

Приклад 4.4

Загальні дільники 12 і 18 є $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, а $\gcd(12,18) = 6$.

Наведемо визначення.

Ціле число d є найменший спільне кратне чисел a і b (позначається $\boldsymbol{lcm}(\boldsymbol{a,b})$ або $НСК(a,b)$), якщо a/d й b/d; і якщо a/c й b/c, то d/c, або, що те саме, $\boldsymbol{lcm}(\boldsymbol{a,b})$ є найменше невід'ємне ціле число, що ділиться й на a й на b.

Лема 4.1

Якщо a й b – невід'ємні цілі числа, то $\gcd(a,b)\cdot \boldsymbol{lcm}(\boldsymbol{a,b}) = a\cdot b$.

Приклад 4.5

Оскільки $\gcd(12,18)=6$, то $\boldsymbol{lcm}(\boldsymbol{12,18}) = 12\cdot 18/6 = 36$.

Наведемо визначення.

1. Два цілих числа a й b називаються взаємно простими (relatively prime or coprime), якщо $\gcd(a,b)=1$.

2. Ціле число $p\geq 2$ називається простим (prime), якщо його дільниками є тільки 1 і саме p. А якщо ні, то p називається складеним (composite).

Лема 4.2

Якщо p – просте й p/ab, то або p/a, або p/b (або p ділить обидва числа).

Теорема 4.25

Існує нескінченно багато простих чисел.

Теорема 4.26

Нехай $\pi(x)$ означає кількість простих чисел менших від x. Тоді $\dfrac{\pi(x)}{x/\ln x}\to 1$ *при* $x\to\infty$.

Теорема 4.27 (Основна теорема арифметики)

Кожне ціле число $n \geq 2$ *може бути представлене, як добуток степенів простих чисел:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k},$$

де p_i *- різні прості числа, а показники* e_i *- додатні цілі. Більше того, зазначене розкладання єдине (якщо не враховувати порядок співмножників).*

Лема 4.3

Якщо $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}, b = p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_k^{f_k}$, де $e_i \geq 0$ й $f_i \geq 0$, то

$$\gcd(a,b) = p_1^{\min(e_1, f_1)} \cdot \ldots \cdot p_k^{\min(e_k, f_k)}$$

і

$$\boldsymbol{lcm}(\boldsymbol{a,b}) = p_1^{\max(e_1, f_1)} \cdot \ldots \cdot p_k^{\max(e_k, f_k)}.$$

Приклад 4.5

Нехай $a = 4864 = 2^8 \cdot 19$, $b = 3458 = 2 \cdot 7 \cdot 13 \cdot 19$.

Тоді

$$\gcd(4864, 3458) = 2 \cdot 19 = 38,$$

$$\boldsymbol{lcm}(\boldsymbol{4864,3458}) = 2 \cdot 7 \cdot 13 \cdot 19 = 442624.$$

Наведемо визначення.

Для $n \geq 1$, нехай $\varphi(n)$ є кількість цілих чисел з $[1, n]$, які взаємно прості з n. Функція φ - функція Ейлера.

Лема 4.4

Якщо p - просте число, то $\varphi(p) = p - 1$.

Якщо $\gcd(m,n) = 1$, то $\varphi(m,n) = \varphi(m) \cdot \varphi(n)$.

Якщо $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ – розкладання числа n на прості множники, то

$$\varphi(n) = n(1 - 1/p_1) \cdot \ldots \cdot (1 - 1/p_k).$$

Лема 4.5

Якщо a й b – додатні цілі числа й $a > b$, то $\gcd(a,b) = \gcd(b, a \bmod b)$.

4.2.2 Алгоритм Евкліда

Алгоритм Евкліда – алгоритм обчислення найбільшого спільного дільника двох чисел [20].

INPUT: два цілих невід'ємних числа a й b, $a \geq b$.

OUTPUT: $\gcd(a,b)$.

1. While $b \neq 0$ do the following:

1.1 Set $r := a \pmod b$, $a := b$, $b := r$.

2. Return (a).

Приклад 4.6

Знайти $\gcd(4864, 3458)$:

$\boldsymbol{4864 = 1 \cdot 3458 + 1406}$,
$\boldsymbol{3458 = 2 \cdot 1406 + 646}$,
$\boldsymbol{1406 = 2 \cdot 646 + 114}$,
$\boldsymbol{646 = 5 \cdot 114 + 76}$,
$\boldsymbol{114 = 1 \cdot 76 + 38}$,
$\boldsymbol{76 = 2 \cdot 38 + 0}$.

$\gcd(4864, 3458) = 38$.

Алгоритм Евкліда може бути розширений так, щоб знаходити не тільки найбільший загальний дільник d двох цілих чисел a і b, але й два цілих числа x й y, що задовольняють умові:

$ax + by = d$.

Розширений алгоритм Евкліда.

INPUT: два цілих невід'ємних числа a й b, $a \geq b$.

OUTPUT: $d = \gcd(a,b)$ і $x, y : ax + by = d$.

1. $r_{-1} = a$, $r_0 = b$, $x_{-1} = 1$, $x_0 = 0$, $y_{-1} = 0$, $y_0 = 1$.

2. While $r_j \neq 0$ do.

2.1. $r_j = r_{j-2} \left(\mathrm{mod}\, r_{j-1}\right)$;

2.2. $q_j = \left\lfloor \dfrac{r_{j-2}}{r_{j-1}} \right\rfloor$;

2.1. $x_j = x_{j-2} - x_{j-1} q_j$;

2.1. $y_j = y_{j-2} - y_{j-1} q_j$.

3. Return $d = r_{j-1} = \gcd(a,b)$, $x = x_{j-1}$, $y = y_{j-1}$.

Приклад 4.7

Нехай $a = 1234$ і $b = 54$.

j	r_j	q_j	x_j	y_j
-1	1234	*	1	0
0	54	*	0	1
1	46	22	$1-22\cdot 0=1$	$0-22\cdot 1=-22$
2	8	1	$0-1\cdot 1=-1$	$1-1\cdot(-22)=23$
3	6	5	$1-5\cdot(-1)=6$	$-22-5\cdot(23)=-137$
4	2	1	$-1-1\cdot 6=-7$	$23-1\cdot(-137)=160$
5	0	3	*	*

4.2.3 Цілі числа за модулем n

Наведемо визначення.

Якщо a й b – цілі числа, то a називається порівнянним з b за модулем n, і приводиться запис

$a = b\left(\mathrm{mod}\, n\right)$,

якщо n ділить $(a-b)$.

Наведемо приклади.

1. $24 = 9\left(\mathrm{mod}\, 5\right)$, тому що $24 - 9 = 3\cdot 5$,

2. $-11 = 17 \pmod 7$, тому що $-11-17 = -4 \cdot 7$.

Лема 4.6

Для всіх a, a_1, b, b_1, $c \in Z$ справедливі такі властивості:

1. $a = b \pmod n$ тоді й тільки тоді, коли числа a й b мають однакові залишки при діленні на n;

2. (властивість рефлексивності) $a = a \pmod n$.

3. (властивість симетрії). Якщо $a = b \pmod n$, то $b = a \pmod n$.

4. (властивість транзитивності). Якщо $a = b \pmod n$ й $b = c \pmod n$, то $a = c \pmod n$.

5. Якщо $a = a_1 \pmod n$, $b = b_1 \pmod n$, то $a + b = a_1 + b_1 \pmod n$ й $ab = a_1 b_1 \pmod n$.

Множина порівнянних за $\bmod n$ цілих чисел утворює клас еквівалентних елементів. Із тверджень (2), (3) і (4) випливає, що множина Z розбивається на неперетинні класи еквівалентних n елементів і кожне належить деякому класу. Якщо $a = qn + r$, де $0 \le r < n$, то $a = r \pmod n$. Отже, кожне $a \in Z$ порівнянне за модулем n з єдиним b: $0 \le b \le n-1$, називаним найменшим лишком числа a за модулем n.

Наведемо визначення.

Множина класів, еквівалентних за модулем n елементів позначається символом Z_n. Додавання, віднімання й множення в Z_n представлені прикладами.

$Z_{25} = \{0, 1, 2, ..., 24\}$.

В Z_{25} $13 + 16 = 4$, оскільки $13 + 16 = 29 = 4 \pmod{25}$. Очевидно, $13 \cdot 16 = 8$ в Z_{25}.

Наведемо визначення.

Нехай $a \in Z_n$. Оберненим до елемента a за модулем n називається таке $x \in Z_n$, що $ax = 1 (\mathrm{mod}\, n)$. Якщо таке число існує, то воно єдине, і позначається як a^{-1}.

Лема 4.7

Нехай a належить Z_n. Елемент a має обернений у Z_n тоді й тільки тоді, коли виконується рівність $\gcd(a, n) = 1$.

Приклад 4.8

Обернені елементи в Z_9 - 1, 2, 4, 5, 7, 8. Наприклад, $4^{-1} = 7$, оскільки $4 \cdot 7 = 1 (\mathrm{mod}\, 9)$.

Лема 4.8

Нехай $d = \gcd(a, n)$. Порівняння $ax = b (\mathrm{mod}\, n)$ має розв'язок x, тоді й тільки тоді, коли d ділить b. У цьому випадку існує точно d розв'язків між 0 і $n-1$; ці розв'язки порівнянні по $\mathrm{mod}(n/d)$.

Теорема 4.28 (Китайська теорема про залишки, CRT)

Якщо цілі числа n_1, n_2, n_3, …, n_k попарно взаємно прості, то система порівнянь

$x = a_1 (\mathrm{mod}\, n_1)$,

$x = a_2 (\mathrm{mod}\, n_2)$,

……,

$x = a_k (\mathrm{mod}\, n_k)$. (4.2.3.1)

має єдиний розв'язок по $\mathrm{mod}\, n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$.

Алгоритм Гауса розв'язку системи (4.2.3.1).

Розв'язок x системи (4.2.3.1) такий

$x = \sum_{i=1}^{k} a_i N_i M_i (\mathrm{mod}\, n)$, де $N_i = n / n_i$, $M_i = N_i^{-1} (\mathrm{mod}\, n_i)$.

Приклад 4.9

Система порівнянь $x = 3(\mathrm{mod}\,7)$, $x = 7(\mathrm{mod}13)$ має єдиний розв'язок $x = 59(\mathrm{mod}\,91)$.

Лема 4.9

Якщо $\gcd(n_1, n_2) = 1$, то пара порівнянь $x = a(\mathrm{mod}\,n_1)$, $x = a(\mathrm{mod}\,n_2)$ має єдиний розв'язок $x = a(\mathrm{mod}\,n_1 n_2)$.

Наведемо визначення.

Мультиплікативна група групи Z_n є $Z_n^* = \{a \in Z_n : \gcd(a, n) = 1\}$. Зокрема, якщо n просте, то $Z_n^* = \{a \in Z_n : 1 \le a \le n-1\}$.

Наведемо визначення.

Порядок групи Z_n^* – кількість елементів в Z_n^*, і позначається – $|Z_n^*|$.

З теореми Ейлера (див. нижче) випливає, що $|Z_n^*| = \varphi(n)$.

Теорема 4.29 (Теорема Ейлера)

1. Якщо $a \in Z_n^*$, *то* $a^{\varphi(n)} = 1(\mathrm{mod}\,n)$.

2. Якщо n *є добуток двох різних простих чисел* r *і* s, *і якщо* $r = s(\mathrm{mod}\,\varphi(n))$, *то* $a^r = a^s(\mathrm{mod}\,n)$ *для всіх цілих чисел* a.

Теорема 4.30 (Теорема Ферма)

1. Нехай p *просте число,* $\gcd(a, p) = 1$, *тоді* $a^{p-1} = 1(\mathrm{mod}\,p)$.

2. Якщо $r = s(\mathrm{mod}\,p-1)$, *то* $a^r = a^s(\mathrm{mod}\,p)$ *для всіх цілих* a.

3. Зокрема, $a^p = a(\mathrm{mod}\,p)$ *для всіх цілих чисел* a.

Наведемо визначення.

Нехай $a \in Z$. Порядком елемента a, позначення $ord(a)$, називається найменше додатне ціле число t таке, що $a^t = 1 (\mathrm{mod}\, n)$.

Лема 4.10

Якщо порядок a з Z_n^* рівний t, $a^s = 1 (\mathrm{mod}\, n)$, то t ділить s. Зокрема, t ділить $\varphi(n)$.

Нехай $n = 21$. Тоді $Z_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Зауважимо, що $\varphi(21) = \varphi(7) \cdot \varphi(3) = 12$, значить $|Z_{21}^*| = 12$. Порядки елементів групи Z_{21}^* наведені в такій таблиці.

a	1	2	4	5	8	10	11	13	16	17	19	20
$ord(a)$	1	6	3	6	2	6	6	2	3	6	6	2

Наведемо визначення.

Нехай $\alpha \in Z_n^*$. Якщо порядок α є $\varphi(n)$, то α називається генератором або примітивним елементом Z_n^*. Якщо Z_n^* має генератор, то Z_n^* є циклічною групою.

Теорема 4.31

1. Z_n^* *має генератор тоді й тільки тоді, коли* $n = 2, 4, p^k$ *або* $2p^k$, *де* p *є просте непарне число, а* $k > 0$.

2. Якщо α *- генератор в* Z_n^*, *то*

$Z_n^* = \{\alpha^i (\mathrm{mod}\, n) : 0 \le i \le \varphi(n) - 1\}$.

3. Припустимо, що φ *- генератор в* Z_n^*. *Тоді* $b = \alpha^i \bmod n$ *також генератор у* Z_n^* *тоді й тільки тоді, коли* $\gcd(i, \varphi(n)) = 1$. *Звідси випливає, що якщо* Z_n^* *- циклічна, то кількість генераторів дорівнює* $\varphi(\varphi(n))$.

4. α з Z_n^* є генератор в Z_n^*, тоді й тільки тоді, коли $\alpha^{\varphi(n)/p} \neq 1 (\mathrm{mod}\, n)$ для кожного простого дільника p числа $\varphi(n)$.

Приклад 4.10

Z_{25}^* - циклічна, тому що має генератор $n = 2$.

Розглянемо квадратичне порівняння

$$x^2 \equiv a (\mathrm{mod}\, p) \qquad (4.6)$$

с простим p.

Теорема 4.32

Якщо $a \equiv 0 (\mathrm{mod}\, p)$, то порівняння (4.6) має тільки один розв'язок $x \equiv 0 (\mathrm{mod}\, p)$.

(Довести самостійно).

Наведена система лишків – це

$$-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2}. \qquad (4.7)$$

Якщо порівняння (4.6) має розв'язок, то a називається квадратичним лишком (за модулем p) (a quadratic residue modulo p), а якщо розв'язку немає,то a називається квадратичним не лишком (за модулем p) (a quadratic non-residue).

Теорема 4.33 (Критерій Ейлера)

Нехай $p > 2$ просте число. Число a, яке не має спільних дільників з p, є квадратичним лишком за модулем p тоді й тільки тоді, коли

$$a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p), \qquad (4.8)$$

або є квадратичним нелишком за модулем p тоді й тільки тоді, коли

$$a^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p). \qquad (4.9)$$

Доведення.

За теоремою Ферма $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Тому $a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 (\mathrm{mod}\, p)$.

Оскільки p - просте, то принаймні один зі співмножників ділиться на p. Обоє одночасно не діляться на p, тому що їхня різниця не ділиться на непарне число p. Отже, a задовольняє одному й тільки одному порівнянню (4.8) або (4.9).

Нехай порівняння (4.6) має розв'язок x, тоді й $-x \equiv p - x$ - теж розв'язок. Легко бачити, що це різні розв'язки. Але більше двох розв'язків порівняння другого степеня по простому модулю мати не може.

Наведемо загальне визначення.

Нехай n – довільне ціле додатне число й нехай $a \in Z_n^*$. a називається квадратичним лишком (a quadratic residue modulo n), або квадратом за модулем n, якщо існує $x \in Z_n^*$ таке що $x^2 = a (\mathrm{mod}\, n)$. Якщо таке x не існує, то a називається квадратичним нелишком (a quadratic non-residue) за модулем n. Множина всіх квадратичних лишків за модулем n позначається, як Q_n, а множина квадратичних нелишків – $\overline{Q}_n$.

Лема 4.11

Нехай p – просте непарне число й нехай α - генератор в Z_p^*. Тоді $a \in Z_p^*$ є квадратичним лишком за модулем p тоді й тільки тоді, коли $a = a^i \bmod p$, де i є парне ціле число. Звідси випливає, що $|Q_p| = (p-1)/2$ і також $|\overline{Q}_p| = (p-1)/2$; таким чином, половина елементів в Z_p^* - квадратичні лишки, а інша половина – квадратичні нелишки.

Теорема 4.34

$\alpha = 6$ є генератор в Z_{13}^*. Степені числа 6 наведені в таблиці.

i	0	1	2	3	4	5	6	7	8	9	10	11
$6^i \pmod{13}$	1	6	10	8	9	2	12	7	3	5	4	11

Отже, $Q_{13} = \{1,3,4,9,10,12\}$ *і* $\overline{Q}_{13} = \{2,5,6,7,8,11\}$.

Лема 4.12

Нехай n є добуток двох простих непарних чисел p і q, $n = pq$.

Т.ч. $a \in Z_n^*$ є квадратичним лишком за модулем n тоді й тільки тоді, коли $a \in Q_p$ й $a \in Q_q$. Звідси випливає, що $|Q_n| = |Q_p| \cdot |Q_p| = (p-1)(q-1)/4$ й $|\overline{Q}_n| = 3(p-1)(q-1)/4$.

Приклад 4.11

Нехай $n = 21$.

Тоді $Q_{21} = \{1,4,16\}$ й $\overline{Q}_{21} = \{2,5,8,10,11,13,17,19,20\}$.

Наведемо визначення.

Нехай $a \in Q_n$. Якщо $x \in Z_n^*$ задовольняє порівнянню $x^2 = a \pmod{n}$, то x називається коренем квадратним з a за модулем n.

Лема 4.13

1. Якщо p – непарне просте число й $a \in Q_p$, то має в точності два квадратні корені за модулем p.

2. Більш загально, нехай $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, де p_i - різні непарні прості числа, а $e \geq 1$.

Якщо $a \in Q_n$, то a має в точності 2^k квадратних кореня за модулем n.

Приклад 4.12

Корінь квадратний з 12 за модулем 37 є 7 і 30. Корінь квадратний з 121 за модулем 315 є 11, 74, 101, 151, 164, 214, 241 і 304.

Алгоритм швидкого піднесення до степеня за модулем.

INPUT: $a \in Z_n$; ціле число b, що можна представити у двійковому вигляді $b = \sum_{i=0}^{t} b_i 2^i$.

OUTPUT: $a^b \pmod n$.

1. If $b = 0$ then $a_t^* = 1$ and Go To (4).
2. Let $a_t^* = a$, $b_t = 1$.
3. For i from $t-1$ to 0

3.1 $a_i^* = \left(a_{i+1}^*\right)^2 \cdot a^{b_i} \pmod n$.

4. Return $a_0^* = a^b \pmod n$.

4.2.4 Символи Лежандра і Якобі

Символ Лежандра використовуються для визначення, чи є ціле число a квадратичним лишком, чи ні по простому/складеному модулю p.

Наведемо визначення.

Нехай p є непарне просте число й a – ціле число. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається таким чином

$\left(\frac{a}{p}\right) = 0$, якщо p / a;

$\left(\frac{a}{p}\right) = 1$, якщо $a \in Q_p$;

$\left(\frac{a}{p}\right) = -1$, якщо $a \in \overline{Q}_p$.

Лема 4.14

Нехай p – непарне просте число й $a,b\in Z$. Тоді

1. $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}\pmod p$.

Зокрема, $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. Отже, $-1\in Q_p$, якщо $p=1\pmod 4$, і $-1\in \overline{Q}_p$, якщо $p=3\pmod 4$.

2. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Отже, якщо $a\in Z_p^*$, то $\left(\frac{a^2}{p}\right)=1$.

3. Якщо $a=b\pmod p$, то $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

4. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Отже, $\left(\frac{2}{p}\right)=1$, якщо $p=1$ або $7\pmod 8$, і $\left(\frac{2}{p}\right)=-1$, якщо $p=3$ або $5\pmod 8$.

5. Закон взаємності. Якщо q є непарне просте число, відмінне від p, то $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$.

Символ Якобі узагальнює поняття символа Лежандра.

Наведемо визначення.

Нехай $n\ge 3$ - ціле непарне число, факторизація якого має вигляд $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e_k}$. Символ Якобі визначається так

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{e_1}\ldots\left(\frac{a}{p_k}\right)^{e_k}.$$

Зауважимо, що якщо n просте, то символ Якобі співпадає із символом Лежандра.

Лема 4.15

Нехай $m \geq 3$, $n \geq 3$ – непарні цілі числа, і $a, b \in Z$. Тоді символ Якобі задовольняє таким співвідношенням:

1) $\left(\frac{a}{n}\right) = 0$, 1 або -1. Більше того, $\left(\frac{a}{n}\right) = 0$ тоді й тільки тоді, коли $\gcd(a, n) \neq 1$;

2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{b}\right)\left(\frac{b}{n}\right)$.

Отже, якщо $a \in Z_p^*$, то $\left(\frac{a}{n}\right) = 1$.

3) $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$.

4) Якщо $a = b \pmod n$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

5) $\left(\frac{1}{n}\right) = 1$.

6) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n(n-1)}{2}}$.

Отже, $\left(\frac{-1}{n}\right) = 1$, якщо $n = 1 \pmod 4$, і $\left(\frac{-1}{n}\right) = -1$, якщо $n = 3 \pmod 4$.

7) $\left(\frac{2}{n}\right) = (-1)^{\left(\frac{n^2-1}{8}\right)}$.

Отже, $\left(\frac{2}{n}\right) = 1$, якщо $n = 1$ або $7 \pmod 8$, і $\left(\frac{2}{n}\right) = -1$, якщо $n = 3$ або $5 \pmod 8$.

8) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$.

Наслідок

Якщо n непарне, і $a = a_1 2^e$, де a_1 непарне ціле число, то

$$\left(\frac{a}{n}\right)=\left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right)=\left(\frac{2}{n}\right)^e\left(\frac{n \bmod a_1}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}.$$

Це спостереження дозволяє увести рекурсивний алгоритм обчислення символа Якобі без знання розкладання n на прості множники.

INPUT: непарні числа $n \geq 3$, $0 \leq a < n$.

OUTPUT: $\left(\frac{a}{n}\right)$.

1. If $a = 0$ Then Return 0.
2. If $a = 1$ Then Return 1.
3. If $\gcd(a, n) \neq 1$ Then Return 0.
4. Let $r = 1$.
5. If $a < 0$ Then
5.1 $a = -a$;
5.2 If $n \pmod 4 = 3$ Then $r = -r$.
6. Let $t = 0$.
7. While $a \pmod 2 = 0$ Do
7.1 $t = t + 1$;
7.2 $a = a/2$.
8. If $t \pmod 2 = 1$ Then
8.1 If $n \pmod 8 = 3$ or $n \pmod 8 = 5$ Then $r = -r$.
9. If $a \pmod 4 = 3$ and $n \pmod 4 = 3$ Then $r = -r$.
10. Let $c = a$
10.1 $a = n \pmod c$;
10.2 $n = c$.
11. If $a \neq 0$ Then Go To (6).
12. Return $r = \left(\frac{a}{n}\right)$.

Приклад 4.13 (Обчислення символа Якобі)

Нехай $a = 158$ і $n = 235$.

Тоді

$$\left(\frac{158}{235}\right)=\left(\frac{2}{235}\right)\left(\frac{79}{235}\right)=(-1)\left(\frac{235}{79}\right)(-1)^{\frac{78-234}{4}}=$$

$$=\left(\frac{77}{79}\right)=\left(\frac{79}{77}\right)(-1)^{\frac{76-78}{4}}=\left(\frac{2}{77}\right)=-1.$$

Зауваження

Якщо $a\in Q_n$, то квадратичні лишки за модулем n. Але якщо $\left(\frac{a}{n}\right)=1$, то необов'язково $a\in Q_n$.

Наведемо визначення.

Нехай $n>2$ – непарне ціле число, і нехай $J_n=\left\{a\in Z_n^*:\left(\frac{a}{n}\right)=1\right\}$. Множина псевдоквадратів за модулем n, яке позначається $\tilde{Q}_n$, і визначається як множина J_n-Q_n.

Лема 4.16

Нехай $n=pq$ – добуток двох простих непарних чисел. Справедливе таке $|Q_n|=\left|\tilde{Q}_n\right|=(p-1)(q-1)/4$.

4.2.5 Числа Блюма

Наведемо визначення.

Числом Блюма називається складене число виду $n=pq$, де p й q – різні прості числа, кожне з яких $=3 \bmod 4$.

Лема 4.17

Нехай $n=pq$ – число Блюма, і нехай $a\in Q_n$. Тоді a має в точності чотири квадратні корені за модулем n, один з яких також належить Q_n. Взагалі, єдиний корінь квадратний, що належить Q_n, називається головним значенням кореня за модулем n.

Лема 4.18

Якщо $n = pq$ – число Блюма, то функція $f : Q_n \to Q_n$, визначена, як $f(x) = X^2 (\mathrm{mod}\, n)$ є перестановкою. Оберненою є функція: $X^{\left[\left((p-1)(q-1)+\frac{4}{8}\right)\right]} (\mathrm{mod}\, n)$.

5 ОСНОВИ КЛАСИЧНОЇ КРИПТОГРАФІЇ

У цьому розділі будуть викладені теоретичні основи класичної криптографії, наведені описи основних компонентів сучасних систем шифрування заміною, перестановкою й блочним взбиванням, а також наведений аналіз стійкості цих класів шифрів до спроб їх зламу. Слід зазначити, що криптографічні системи, винайдені аматорами й непрофесіоналами, завжди вкрай непрактичні в застосуванні й нестійкі до розкриття. Зокрема багато із самоучок бачать основу стійкості шифру в таємності системи шифрування. Професіонали ж, навпаки, вважають систему шифрування загальновідомою й доводять стійкість шифру через стійкість до зламу секретного ключа.

5.1 Шифри заміни

Тепер подивимося, як звичайно на практиці виконується шифрування заміною за допомогою ЕОМ. Найпростіший спосіб зробити текст непрочитуваним - сховати його, змішавши його з послідовністю випадкових чисел, що задана ключем, на основі бітової операції XOR (операція XOR виконує такі дії: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$; $\oplus$ - інше позначення операції XOR). Позначивши через t вектор повідомлення, y - вектор випадкової послідовності й s - шифрування, одержуємо

$s = t \oplus y$.

Якщо біти у використовуваній для шифрування випадкової послідовності статистично незалежні один від одного, то й у

шифрування вони стають такими самими . Текст перетворюється у будь-що, тобто в шум. Через специфіку операції XOR процедура шифрування збігається із процедурою розшифрування:

$t = s \oplus y$ і $s = t \oplus y$.

5.2 Шифри перестановки

Шифр заміни в чистому його вигляді майже ніколи не застосовується, а завжди виконується разом з перестановкою. Якщо після заміни символи повідомлення перетворювалися в що завгодно, але зберігали в шифровці своє вихідне місце розташування, то після перестановки вони змінювали своє місце, що надійно захищає шифровку від атак криптологів. Перестановку можна розглядати як множення вектора повідомлення на матрицю перестановки бітів P з елементами 0 і 1, і розміром з довжину повідомлення в бітах. Розглянемо два випадки.

1. Перестановка може виконуватися до накладення на повідомлення випадкової послідовності, тобто $s' = Pt + y$. У випадку, якщо текст у повідомленні відсутній $t = 0$ і йдуть нулі або пробіли, то $s' = y$, а в канал зв'язку попадає чистий ключ.

2. Перестановка може виконуватися й після накладення на повідомлення випадкової послідовності, тобто $s'' = P(t + y)$. У випадку, якщо текст у повідомленні відсутній $t = 0$ і йдуть нулі або пробіли, як $s'' = Py$, а в канал зв'язку попадає ключ, шифрований перестановкою.

Тому, звичайно перевага віддається другій схемі, коли під час відсутності тексту шифротекст являє собою не чистий ключ, а ускладнений перестановкою. В іншому випадку накладення на шифровку свого тексту для уведення одержувача в оману нічого не дає. Однак перестановки необхідні й для того, щоб атака на ключ стала неефективною. Якщо передача йде побайтно, то досить лише переставляти біти в середині байта, щоб з

імовірністю 0,97 видозмінити його й зробити перехоплення ключа описаним способом неможливим.

Перестановка може виконуватися окремими бітами або групами біт як байти, що програмно куди зручніше, хоча й не перемішує бітові послідовності повністю. Перестановку можна було б зробити й побітно, але це був би дуже дорогий процес.

Тимчасова складність перестановки залежить від квадрата числа елементів, що переставляються, тому перестановка біт була б в 64 рази дорожче перестановки байт. Обчислювальних способів перестановок існує велика кількість, на будь-який смак. Наприклад, у програмах широко застосовується перестановка за номерами N від 0 до $L-1$ на основі рекурентного виразу:

$$N_{i+1} = (K - N_i + M) (\mathrm{mod}\, L)$$

при виконанні таких 4-х умов:

1) K і M беруться з інтервалу $[1, L-1]$,

2) M взаємно просте з L,

3) $K-1$ ділиться на будь-який простий дільник L,

4) $K-1$ ділиться на 4, якщо L ділиться на 4.

Для гарного заплутування в цьому випадку доводиться кілька разів робити перестановку, міняючи випадковим способом K і M.

Цікава схема перестановки, що нагадує тасування колоди карт. Так, якщо $S = A + B + C$ являє собою вихідний блок тексту, що переставляється побайтно, то результатом такої перестановки буде $S' = C + B + A$, де розбивка на фрагменти A, B й C робиться випадковим чином. Після декількох тасувань вихідний текст виявляється дуже заплутаним. Це тасування здатне після багаторазового повторення здійснити будь-яку перестановку. Однак число тасувань при цьому повинно бути дуже велике, і для швидкого одержання якісної перестановки краще виконувати перестановку пар.

Перестановка тасуванням найчастіше дуже зручна, тому що одиночний її крок практично не залишає жодного символа на своєму місці.

Шифр заміни, ускладнений перестановкою, являв собою раннє покоління машинних криптографічних перетворень. Він остаточно звів надію на розкриття шифру хитромудрими методами відгадування тексту повідомлення, залишивши криптоаналітикам лише можливість прямого підбору ключа. Розкриття випадкової перестановки без знання ключа неоднозначне, що не дозволяє достатньо впевнено розшифрувати повідомлення. Однак за збереженою статистикою використаних у повідомленні символів можна робити більш або, скоріше, менш чіткі прогнози про його загальний зміст.

5.3 Шифри збивання й стандарт DES

Здавалося б, що межа можливостей схову повідомлення вже досягнута, але це не так. Результат можна значно поліпшити, якщо замість перестановки використовувати лінійне перетворення:

$s = L \times t$,

де L - невироджена матриця випадкового лінійного перетворення біт.

І хоча розшифровування в цьому випадку доведеться виконувати на основі розв'язку системи лінійних рівнянь, але вже кожний біт шифрування починає залежати від кожного біта тексту. Шифри на основі цього перетворення називають скрамблерами за те, що вони збивають текст повідомлення. На жаль, частка невироджених матриць зі збільшенням їх розміру швидко спадає. Детермінант матриці L, як і її елементи, може дорівнювати або 0, або 1. Якщо $\det(L) = 0$, то матриця вироджена.

Для того щоб матриця L була невиродженою, випадковою й при розшифровуванні не потрібно було робити багато обчислень, американськими криптографами був запропонований алгоритм, який був покладений в основу стандартного криптографічного перетворення DES. Суть його одного кроку можна описати такою схемою.

Вхідний блок даних ділиться навпіл на ліву L' й праву R' частини. Після цього формується вихідний масив так, що його ліва частина L'' представлена правою частиною R' вхідного, а права R'' формується, як сума L' й R' операцією XOR. Далі, вихідний масив зашифровується перестановкою із заміною. Можна переконатися, що всі проведені операції можуть бути обернені й розшифровування може бути виконано за число операцій, що лінійно залежить від розміру блоку. У той самий час, після декількох таких змішувань можна вважати, що кожний біт вихідного блоку шифрування може залежати від кожного біта повідомлення.

Система шифрування DES була розроблена IBM під іменем Lucifer і запропонована Національним Бюро Стандартів США в 1976 році як стандарт шифрування. У ній застосований ключ із 56 біт. Слід зазначити, що в стандарті DES застосовані перестановки лише спеціального типу, що наводило критиків цього стандарту на думку, що АНБ добре знало їхню теорію й могло для зламу скористатися заздалегідь відомими слабкими місцями. Однак принцип цього шифрування пройшов саму широку апробацію і йому присвячена велика кількість публікацій. Дорікання викликали лише обрані короткі довжини блоку в 64 біта й ключа в 56 біт, що недостатньо для таких задач, як національна безпека. Свій розвиток DES одержав у Держстандарті 28147-89, який збільшив довжину ключа до 256 біт і допустив довільні перестановки.

Шифр DES прийнятий федеральним стандартом США, і підходить у використанні для багатьох комерційних систем. Однак, уряд, сам ніколи не використовує шифри, пропоновані бізнесменами, щоб закрити свої дані, тому що вони недостатньо стійки від атак аналітиків. Наприклад, 16-кратний DES був зламаний Шаміром, який застосував диференціальний криптоаналіз, і Матсуї, який використовував лінійний криптоаналіз. Найбільш серйозну практичну атаку на DES здійснив Мішель Вінер, який розробив і випробував мікросхему, що перевіряє в секунду 50 мільйонів ключів DES. ЕОМ, яка коштувала досить дорого і складалась з кілька десятків тисяч

таких мікросхем, здатних перебрати всі ключі DES за 7 годин. АНБ і ФАПСИ витрачають на обчислювальну техніку такі гроші, що можуть побудувати ЕОМ, що зламує, DES за секунду. Це означає, що DES не бути використаний для серйозних систем.

5.4 Елементи криптоаналізу - 1

Без описів загальних підходів до проблеми розкриття шифрів не можна зрозуміти еволюцію криптографії, дати поняття стійкості шифрів. Тому, хоча б коротко викладемо підходи до розкриття ряду простих шифрів, що дасть загальну картину підходів, що використовуються у цій області. Існує велика різниця між ручними й машинними способами шифрування. Ручні шифри досить різноманітні й можуть бути самими несподіваними. Крім того, повідомлення, які закриваються ними, дуже короткі. Із-за цієї причини їх розкриття набагато більш ефективно виконується людьми. Машинні шифри більш стереотипні, чисельно гранично складні й призначені для приховування повідомлень дуже великої довжини. Ясно, що вручну їх розкрити навіть і не треба намагатися. Однак і тут криптоаналітики відіграють головну роль.

Завжди вважаються відомими тип шифру й мова повідомлення. Тому невідомим є тільки ключ, який необхідно розкрити.

При традиційному криптоаналізі систем шифрування можливість їх розкриття залежить, значною мірою, від кваліфікації зламщика. Криптоаналітик повинен добре володіти методами дискретної математики, теорії чисел, теорії складності, абстрактної алгебри, статистики, алгоритмічного аналізу й інших споріднених до криптографії математичних дисциплін, а також мати розвинену інтуїцію, щоб знайти метод, що веде до розкриття шифру, припускаючи, що він існує. Процес криптоаналізу щораз починається із самого початку при підході до нової системи й досвід, отриманий при розкритті

однієї системи шифрування, рідко може бути застосований для розкриття іншої. Успіх криптоаналізу визначається алгоритмом шифрування – складність розкриття шифру залежить лише від його конструкції. Це означає, що існує дуже мало загальних принципів криптоаналізу, які можна було б практично використовувати для розкриття будь-яких шифрів і автоматичний криптоаналіз є ефективним відносно дуже обмеженого класу алгоритмів.

Тому на практиці стійкість шифрів до зламу береться за міру криптографічної стійкості їх алгоритмів. Чим триваліше шифр не піддається розкриттю, тим більше причин уважати його стійким. Однак стійкість шифру необов'язково означає, що він є безпечним. Це означає лише, що метод, на основі якого виконати успішну атаку ще не знайдений аматорами або не опублікований професіоналами. Як приклад можна привести шифри, де крім ключа шифрування є ще головний ключ, який називають ключем від чорного входу. Такі шифри можуть бути стійкими, але вони не є безпечними, тому що власник головного ключа може читати будь-які шифрування. Отже, процес криптоаналізу може бути дуже тривалим через те, що криптоаналітику мало користі від успішного розкриття інших систем шифрування і йому невідомий інший захід криптографічної стійкості шифру, крім тривалості його опору до зламу. Навіть якщо зламщик не може прочитати повідомлення, однаково необхідно бути обережним. У любому випадку він може одержати багато інформації, знаючи відправника, одержувача, час і довжину повідомлення.

5.5 Випробування шифрів

Починають злам шифрів звичайно зі статистичних методів випробувань тексту шифрування, що дає загальні дані про їхню стійкість на початковому етапі аналізу. Оскільки мета криптографії полягає в тому, щоб перетворити відкритий текст у шифровку, зміст якої недоступний незаконному одержувачеві інформації, то можна в ідеалі представити шифрувальну

систему, як «чорний ящик», вхід і вихід якого взаємонезалежні, оскільки для встановлення ключа, який дасть рівність вхідного тексту із шифром, буде потрібно провести перебір усіх допустимих варіантів. Якщо простір пошуку ключа дуже великий і неможливо за допомогою наявних обчислювальних засобів перевірити кожний ключ за обмежений допустимий час, то шифр є чисельно безпечним.

6 ШИФРИ З ВІДКРИТИМ КЛЮЧЕМ

Розвиток криптографії в XX столітті був стрімким, але нерівномірним. Виділяється три основних періоди.

1. Початковий, який мав справу лише з ручними шифрами; він почався в сивій давнині, закінчився лише наприкінці тридцятих років XX століття. Криптографія за цей час пройшла довгий шлях від магічного мистецтва прадавніх жерців до буденної прикладної професії чиновників секретних відомств.

2. Наступний період відзначений створенням і широким упровадженням у практику спочатку механічних, потім електромеханічних і, нарешті, електронного обладнання для шифрування, створенням мереж секретного зв'язку. Його початком можна вважати застосування телеграфних шифрувальних машин, які використовує довгий одноразовий ключ. Триває він по наші дні. Однак до середини сімдесятих років було досягнуто рівня, коли підвищення стійкості шифрів відійшло на другий план. З розвитком розгалужених комерційних мереж зв'язку, електронної пошти й глобальних інформаційних систем найголовнішими стали проблеми розподілу секретних ключів і підтвердження авторства.

3. Початком третього періоду розвитку криптології, як правило, вважають 1976 рік, коли американські математики Діффі й Хеллман [4] запропонували принципово новий вид організації секретного зв'язку без попереднього надання абонентам секретних ключів, так зване шифрування з відкритим ключем. У результаті стали з'являтися криптографічні системи,

побудовані на підході, сформульованому ще в сорокових роках Шеноном. Він запропонував будувати шифр у такий спосіб, щоб його розкриття було еквівалентне розв'язку математичної задачі, що вимагає виконання об'ємних обчислень, що перевищують можливості сучасних ЕОМ. Новий період розвитку криптографії характеризується появою повністю автоматизованих систем шифрованого зв'язку, у яких кожний користувач має свій індивідуальний пароль для підтвердження авторства, зберігає його, наприклад, на магнітній карті, і пред'являє при вході в систему, а весь інший процес проведення секретного зв'язку відбувається автоматично.

У традиційних криптосистемах тим самим секретним ключем здійснюється як шифрування, так і дешифрування повідомлення. Це дає змогу вважати, що відправник і одержувач повідомлення отримали ідентичні копії ключа кур'єром. Це припущення майже не допускається для комерційних фірм і абсолютно недоступне приватним особам через свою ціну.

При шифруванні з відкритим ключем (асиметричний шифр) для шифрування й розшифровування використовуються різні ключі, і знання одного з них не дає практичної можливості визначити другий. Тому ключ для шифрування може бути загальнодоступним без втрати стійкості шифру, якщо ключ для розшифровування зберігається в таємниці, наприклад, генерується й зберігається тільки одержувачем інформації.

Нові ідеї почали швидко реалізовуватися на практиці. Шифрують і зараз традиційними методами, але розсилання ключів і цифровий підпис стали виконуватися вже по-новому [2,3,9,18,20]. Зараз два методи шифрування з відкритим ключем одержали визнання й закріплені в стандартах. Національний інститут стандартів і технологій США NIST (колишній ANSI) прийняв стандарт MD 20899, заснований на алгоритмі Ель-Гамаля, а на основі алгоритму RSA прийняті стандарти ISO/IEC/DIS 9594-8 міжнародною організацією по стандартизації й X.509 міжнародним комітетом зв'язку.

На даний час термін «асиметрична криптографія» покриває велику групу механізмів, алгоритмів, протоколів і ідей, що

застосовуються при розробленні систем захисту інформації. Наведемо приклади основних із них і коротко прокоментуємо, що конкретно мається на увазі під кожним терміном.

1) однобічна функція (one-way function) [20];

2) однобічна функція із секретом (one-way trap-door function) [20] - це деяка функція $F_k : X \to Y$, що залежить від параметра k (її можна розглядати також як параметризоване сімейство функцій), яка має такі властивості:

а) при будь-якому значенні параметра k існує поліноміальний алгоритм обчислення значення функції в будь-якій точці $F_k(x)$ за умови, що параметр k відомий;

б) при невідомому значенні параметра k не існує поліноміального алгоритму інвертування функції F_k;

в) при відомому значенні параметра k існує поліноміальний алгоритм інвертування функції F_k;

3) криптографічні протоколи - це така процедура взаємодії абонентів, у результаті якої вони досягають своєї мети, а їх супротивники - не досягають. Під це неформальне визначення підпадають усі практично цікаві способи застосування асиметричної криптографії.

Поняття однобічної функції із секретом стало вихідним для асиметричної криптографії. Той факт, що для обчислення самої функції з поліноміальною складністю й для її інвертування потрібно різна вихідна інформація (тобто наявність певної асиметрії), і дав назву новому напрямку в криптографії.

6.1 Однобічні функції

Поняття однобічної функції й однобічної функції з «лазівкою» є центральними поняттями всієї криптографії з відкритим ключем [3, 4].

Розглянемо дві довільні множини X й Y. Функція $f : X \to Y$ називається однобічною, якщо $f(x)$ може бути легко обчислена для кожного x з X, тоді як майже для всіх y з Y

обчислення такого x з X, що $f(x)=y$ (за умови, що хоча б один такий x існує), є складним. Це поняття не потрібно плутати з функціями, які є математично необернеными через те, що вони невзаємно однозначні (тобто через те, що існує декілька різних x, таких що $f(x)=y$, або їх немає зовсім). Наш нинішній стан знань не дозволяє нам довести, що однобічні функції взагалі існують, тому що їхнє існування дало б розв'язок так званої $P=NP$ проблеми.

Однак незважаючи ні на що, у нас є кандидати в цьому контексті серед функцій, як ефективно обчислити значення, які ми знаємо, тоді як ніяких ефективних алгоритмів їх оберненого обчислення (у всякому разі серед загальнодоступних) невідомо.

Простий приклад кандидата на однобічну функцію є множення цілих чисел. Відомо, що множити навіть дуже великі числа відносно неважко, у той час, як навіть самий потужний комп'ютер не може розкласти на множники з найкращим наявним у його розпорядженні алгоритмом багатозначне десяткове число, що є добутком двох приблизно однакових за розміром простих чисел.

Звичайно, необхідно розуміти, що « не в змозі» означає «не в змозі за прийнятний час (таке, як час людського життя або вік всесвіту)».

Іншим важливим прикладом кандидата на однобічну функцію є модульне піднесення до степеня або модульне експонування (з фіксованими підставою й модулем). Нехай n і a – цілі числа, такі, що $1<a<n$, і нехай $Z_n=\{0,1,2,...,n-1\}$. Тоді модульне піднесення до степеня (відносно підстановки значень a і модуля n) це така функція $f:Z_n\to Z_n$, яка задана $f(a,m,n)=a^m(\mathrm{mod}\,n)$.

За аналогією з дійсним аналізом обернена операція відома як задача дискретного логарифмування: дані цілі числа a, n і x, потрібно знайти таке ціле m (якщо воно існує), що $a^m(\mathrm{mod}\,n)=x$. Наприклад, $5^4(\mathrm{mod}\,21)=16$. Отже, 4 це дискретний логарифм 16 з підстановкою 5 за модулем 21. При

бажанні можна перевірити, що, наприклад, число 3 взагалі не має логарифма з підставою 5 за модулем 21. Незважаючи на те, що обчислення великих модульних експонент може бути виконано ефективно, у цей час невідомо жодного алгоритму для обчислення дискретних логарифмів великих чисел за прийнятний час навіть на самих швидкодіючих комп'ютерах.

При цьому, хоча ми й не можемо довести, що таких алгоритмів взагалі не існує, є припущення, що модульне піднесення до степеня (з фіксованими підстановкою й модулем) дійсно є однобічною функцією.

Очевидно, що однобічні функції не можуть безпосередньо використовуватися в якості криптосистем (коли m зашифровується, як $f(m)$), оскільки тоді навіть законний одержувач не зможе розкрити відкритий текст! Але, незважаючи на це, вони дуже часто використовуються для захисту паролів.

Більш часто уживаним у криптографії є поняття однобічної функції із секретним ходом (лазівкою). Функція $f: X \to Y$ називається однобічною функцією із секретним ходом, якщо вона може бути ефективно обчислена прямо і обернено, більше того, може бути навіть відомий ефективний алгоритм обчислення f такий, при наявності інформації про функціонування якого, як цей алгоритм працює, не дає ніякої можливості розробити ефективний алгоритм обчислення оберненої до неї функції.

Секрет, за допомогою якого можна отримати обидва ефективних алгоритмів, саме й називається секретним ходом.

Наш перший кандидат на однобічну функцію із секретним ходом дуже схожий на нашого другого кандидата - на просто однобічну функцію: модульне піднесення до степеня з фіксованою експонентою й модулем. Нехай m і n - цілі числа, а Z_n визначене так само, як і раніше. Тоді модульне піднесення до степеня (відносно експоненти m й модуля n) є функція $g: Z_n \to Z_n$, визначена в такий спосіб: $g(a,m,n) = a^m \pmod n$.

Необхідно більш чітко пояснити відмінності між функціями $f(a,m,n)$ й $g(a,m,n)$.

Знову за аналогією з дійсним аналізом, операція обернена до $g(a,m,n)$ відома як знаходження кореня m-го степеня з x за модулем n: дані цілі числа m, n і x, знайти таке ціле a (якщо воно існує), що $a^m \pmod n = x$. Наприклад, 5 це корінь 4-го степеня з 16 за модулем 21, тому що ми вже бачили, що вірно $5^4 \pmod{21} = 16$. Очевидно, що 2 також є коренем 4-го степеня з 16 за модулем 21. Чи можете Ви знайти інший корінь 4-го степеня з 16 за модулем 21? Знайдіть ціле число x, яке не має корінь 4-го степеня за модулем 21.

У тому випадку, коли експонента m й модуль n фіксовані, ми вже приводили ефективний алгоритм обчислення $g(a,m,n)$ для будь-якої підстановки a.

На противагу задачі дискретного логарифмування, відомо, що існує також і ефективний алгоритм знаходження кореня m-го степеня з x за модулем n (або з'ясування, що його не існує) для будь-якого заданого x. Цікавий феномен полягає в тому, що невідомо, як ефективно побудувати цей ефективний алгоритм при заданих лише m й n. Інакше кажучи, функція $g(a,m,n)$ в дійсності не є однобічною, оскільки ми знаємо, що вона може бути ефективно обернена, але незважаючи на цей факт ми не знаємо, як це зробити!

Проте, легко побудувати ефективний алгоритм обчислення m-го кореня за модулем n за умови, що відоме розкладання n на прості множники. Саме із цієї причини $g(a,m,n)$ і є кандидатом на однобічну функцію із секретним ходом, для якої m й n використовуються як відкрита інформація, тоді як розкладання служить у якості секретного ходу. Ми ще побачимо, яким чином цей факт може бути використаним, коли будемо вивчати відому криптосистему RSA.

6.2 Протокол обміну сеансовими ключами (протокол Діффі - Хеллмана)

Одна з основних складних задач у більшості криптосистем з великою кількістю користувачів, яку слід відзначити, полягає в тому, що кожна пара користувачів повинна обмінюватися секретними ключами. Припустимо, що два конкретні користувачі поки ще не починали обмін один з одним заздалегідь ніякою секретною інформацією, і що вони раптом захотіли встановити секретний зв'язок між собою. Загальноприйнятим розв'язком для них було б десь зустрітися, щоб передати один одному секретний ключ, або використовувати щось схоже на довірчого кур'єра. Обидва розв'язки є дуже повільними й дорогими, і до того ж вони не можуть бути абсолютно надійними. Призначення системи з відкритим розподілом ключів полягає в тому, щоб вона дозволяла двом таким користувачам отримати секретний ключ у результаті переговорів по несекретному каналу зв'язку таким чином, щоб можливий «підслуховувач» не зміг отримати цей ключ навіть після прослуховування повністю всіх цих переговорів.

Точніше, хотілося б мати такий протокол, за допомогою якого Аліса й Боб обмінювалися б повідомленнями m_1 (від Аліси до Боба), m_2 (від Боба до Аліси),..., доти поки Аліса й Боб остаточно не домовляться про деякий ключ k, таким чином, щоб визначити k, знаючи тільки m_1, m_2, було б практично неможливо. Підкреслимо ще раз, що цього необхідно добитися навіть незважаючи на те, що Аліса й Боб заздалегідь не обмінюються ніякою інформацією, яка не була б відома підслухувачеві.

Перший протокол, який досяг цієї бажаної неможливої мети, був запропонований Діффі (W. Diffie) і Хеллманом (M. E. Hellman) [4] в 1976 р. Він ґрунтується на задачі дискретного логарифмування, розглянутої в попередньому розділі. Нехай n деяке велике ціле число й нехай g інше ціле,

що лежить строго між 1 і $n-1$. У якості першої дії протоколу Діффі-Хеллмана Аліса й Боб домовляються про параметри n й g за допомогою несекретного каналу зв'язку (альтернативно n й g могли б бути стандартними параметрами, застосовуваними всіма користувачами системи).

Потім Аліса вибирає деяке велике ціле число x й обчислює $X = g^x \pmod n$. Відповідно, Боб вибирає y й обчислює $Y = g^y \pmod n$. Після цього Аліса й Боб обмінюються X й Y по одному несекретному каналу зв'язку, зберігаючи при цьому в секреті x й y (x знає тільки Аліса, а y – тільки Боб). Нарешті, Аліса обчислює $Y^x \pmod n$, відповідно, Боб обчислює $X^y \pmod n$. Обоє ці значення рівні між собою, тому що кожне з них дорівнює $g^{xy} \pmod n$. Це і є саме той ключ k, який вони хотіли спільно сгенерувати.

Загальний алгоритм має такий вигляд.

Відкрито вибирається велике просте число n, а в групі G_n^* знаходимо елемент g - генератор (алгоритм пошуку g описаний нижче).

1. Аліса генерує $a \in [1, n-1]$, обчислює $g_a \equiv g^a \pmod n$ й посилає Бобу.

2. Боб генерує $b \in [1, n-1]$, обчислює $g_b \equiv g^b \pmod n$ й посилає до Аліси.

3. Аліса обчислює $k_1 \equiv g_b^a \pmod n$.

4. Боб обчислює $k_2 \equiv g_a^b \pmod n$.

Обидва значення збігаються й дають величину загального ключа.

Приклад 6.1

Нехай $p = 43$. Алгоритм пошуку g дає $g = 3$. Аліса вибирає $a = 8$, Боб вибирає $b = 37$.

Тоді $g_a = 3^8 \equiv 25 (\mathrm{mod}\, 43)$, $g_b = 3^{37} \equiv 20 (\mathrm{mod}\, 43)$. Таким чином, загальний ключ має вигляд

$k = 20^8 \equiv 25^{37} \equiv 9 (\mathrm{mod}\, 43)$.

Доповнення до протоколу.

1) p слід вибирати так, щоб число $p-1$ мало досить великий простий множник $p' \geq 2^{160}$;

2) достатньо, щоб g породжувало не всю групу, але досить велику її підгрупу;

3) Аліса й Боб повинні перевірити, щоб $g_b \neq 1$ і $g_a \neq 1$;

4) по закінченню протоколу Аліса й Боб повинні стерти a й b. Це є завчасна таємність (forward secrecy).

Незважаючи на те, що дуже великі дискретні логарифми можливо і є важко обчислювальними, хотілося б відзначити, що для їхнього обчислення існують алгоритми набагато кращі, ніж пошук перебором.

Якщо припустити, що n і g є стандартними параметрами, цікавою альтернативою описаному раніше інтерактивному протоколу є в знаходженні й використанні для поширення деякого єдиного для всіх довідника. Кожний користувач записує в цей довідник свій власний X, обчислений, як $g^x (\mathrm{mod}\, n)$ для свого випадково обраного секретного x. Це дозволяє двом користувачам сформувати їхній спільний секретний ключ навіть до того, як вони почнуть вести обмін інформацією. Основний недолік такого доступу до довідника полягає в тому, що він не дає можливість частої зміни користувачам своїх секретних ключів досить часто.

Алгоритм випадкового вибору первісного кореня за простим модулем.

Означення: p – просте число, q_1, q_2, …, q_k – усі прості множники числа $p-1$.

INPUT: p, q_1, q_2, …, q_k.

OUTPUT: g.

1. Let $g \in [2, p-1]$.

2. For $i:1..k$ Do

2.1 If $g^{\left(\frac{p-1}{q_i}\right)} \equiv 1 (\mathrm{mod}\, p)$ Go To (1).

3. Return g.

6.3 Криптоалгоритм RSA

Криптосистема RSA, названа так на честь її винахідників R. Rivest, A. Shamir, L. Adleman, є найбільш застосовуваною криптосистемою з відкритим ключем (public-key cryptosystem). Вона може використовуватися як для шифрування інформації, так і для цифрового підпису [7, 9, 17, 20].

Алгоритм генерації ключів має такий вигляд.

Кожен учасник (нехай це будуть Аліса, Боб, …) робить таке:

1. Обирає два великих простих і не співпадаючих випадкових числа p й q, приблизно одного розміру.

2. Обчислює $n = pq$ й $\varphi(n) = (p-1)(q-1)$. ($\varphi(n)$ - функція Ейлера).

3. Підбирає випадкове ціле число, $1 < e < \varphi(n)$, таке що $\gcd(e, \varphi(n)) = 1$.

4. Застосовуючи розширений алгоритм Евкліда, обчислює ціле, $1 < d < \varphi(n)$, таке що $ed = 1 (\mathrm{mod}\, \varphi(n))$.

5. Відкритим ключем є пара чисел (n, e), секретним ключем є пара чисел (n, d).

Алгоритм шифрування.

Боб шифрує повідомлення m, яке потім відсилається на адресу Аліси.

1. Шифрування. Боб виконує такі дії:

а) бере відкритий ключ Аліси (n, e);

б) представляє повідомлення у вигляді цілого числа m з інтервалу $[0, n-1]$;

в) обчислює $c = m^e (\mathrm{mod}\, n)$;

г) відсилає шифрований текст Алісі.

2. Розшифрування. Одержуючи відкритий текст m із c, Аліса виконує такі дії:

а) використовуючи свій секретний ключ (n,d) обчислює $m = c^d \pmod n$.

Дійсно, оскільки $ed = 1 \pmod \varphi$, то при деякому цілому k вірна рівність $ed = 1 + k\varphi$. Далі, якщо $\gcd(m, p) = 1$, то по теоремі Ферма $m^{p-1} = 1 \pmod p$.

Якщо піднести обидві частини останнього порівняння до степеня $k(q-1)$ і помножити обидві частини на m, одержуємо

$$m^{1+k(p-1)(q-1)} = m \pmod p.$$

З іншого боку, якщо $\gcd(m, p) = p$, то останнє порівняння теж вірне, тому що обидві частини порівнянні з 0 за модулем p. Таким чином, у всіх випадках

$$m^{ed} = m \pmod p.$$

Аналогічно,

$$m^{ed} = m \pmod q.$$

Нарешті, оскільки p й q різні прості числа, то

$$m^{ed} = m \pmod n,$$

і, отже,

$$c^d = \left(m^e\right)^d = m^{ed} = m \pmod n.$$

Приклад 6.2

Генерація ключів.

Користувач Аліса вибирає прості $p = 2357$, $q = 2551$, і обчислює $n = pq = 6012707$, $\varphi = (p-1)(q-1) = 6007800$. Аліса вибирає $e = 3674911$ й, використовуючи розширений алгоритм Евкліда, знаходить $d = 422191$ таким, що $ed = 1 \pmod \varphi$. Відкритий ключ Аліси – це пара $(n = 6012707, e = 3674911)$, а секретний ключ – це пара $(n = 6012707, d = 422191)$.

Процес шифрування.

Відкрите повідомлення Боба $m = 5234673$. Боб використовує алгоритм для піднесення до степеня і обчислює $c = m^e \pmod n = 5234673^{3674911} \pmod{6012707} = 3650502$, і посилає Алісі.

Процес розшифрування.

Розшифровуючи, Аліса обчислює

$c^d \bmod n = 3650502^{422191} \pmod{6012707} = 5234673$.

Деякі зауваження.

1. Число $\lambda = lcm(p-1, q-1)$ іноді може бути використане замість $\varphi = (p-1)(q-1)$.

2. Алгоритм RSA і інші вимагають залучення великих і дуже великих простих чисел. Як перевірити, що деяке число p є простим?

6.4 Кілька тестів на простоту числа

6.4.1 Решето Ератосфена [14, 20]

Нехай потрібно на множині цілих чисел $2,3,4,..,n$ знайти всі прості. Число 2 просте, а всі парні числа (через одне, починаючи з 2) не є простими й ми їх викреслюємо. 2 залишилося не викресленим і воно - просте. Знаходимо перше не викреслене більше двох число. Це буде 3. Викреслюємо всі числа, кратні трьом, але не саме це число (через два, починаючи з 3). Продовжуємо процес викреслювання доти, поки є числа, які можна викреслити. Легко перевірити, що потрібно повторювати ці дії для чисел, що не є більшими за $\sqrt{n}$. Дійсно, якщо $m = ab$, $a, b > 1$, $m \le n$ то найменший дільник числа m (нехай це буде a) задовольняє нерівність $a \le \sqrt{m} \le \sqrt{n}$ і число m було викреслено раніше.

Цей алгоритм дуже простий, але якщо число x дуже велике, то час роботи алгоритму занадто довгий.

Даний метод дозволяє будувати множину простих чисел, але він незручний для перевірки простоти заданого числа. Проте

ідея решета і її узагальнення на даний час часто використовуються для «просівання» множин чисел, що володіють тими чи іншими умовами. Більше того, розробляються спеціальні мікропроцесори, на яких операції «просівання» виконуються дуже ефективно.

6.4.2 Тест Вільсона

У 1770 р. Є. Варинг опублікував таку теорему, приписувану Д. Вільсону.

Теорема 6.1

Число n *є простим тоді й тільки тоді, коли виконується* $(n-1)!\equiv -1(\mathrm{mod}\, n)$.

Доведення

У випадку $n=2$ твердження очевидне. Якщо $n=p>2$ – просте, то кожний елемент поля Z_p^*, відмінний від 1 і від -1, має обернений a^{-1}, причому $a\neq a^{-1}$. Тому

$$(n-1)!\equiv(-1)\prod_{a\neq 1,-1} aa^{-1}\equiv -1(\mathrm{mod}\, n).$$

Якщо $n=ab$ - складене, $1<a<n$, то a ділить $(n-1)!$ і, отже, $(n-1)!$ не має оберненого елемента з кільця Z_n. Тому $(n-1)!\neq -1(\mathrm{mod}\, n)$. Теорема доведена.

Даний критерій іноді буває зручний у доказах, але застосовувати його для перевірки простоти неможливо через великий об'єм роботи.

6.4.3 Тест на основі малої теореми Ферма

Мала теорема Ферма стверджує, що якщо n - просте, то виконується умова:

1) при всіх $a\in\{2,3,...,n-1\}$ має місце порівняння

2) $a^{n-1}\equiv(\mathrm{mod}\, n)$. (6.1)

Зворотне твердження невірне.

З цієї теореми випливає, що якщо це порівняння не виконується хоча б для одного $a \in \{2,3,...,n-1\}$, то n - складене. Тому можна запропонувати такий імовірнісний тест простоти числа:

1) вибираємо випадкове $a \in \{2,3,...,n-1\}$ й перевіряємо за допомогою алгоритму Евкліда умову $\gcd(a,n)=1$;

2) якщо воно не виконується, то відповідь n - складене;

3) перевіряємо порівняння $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$;

4) якщо порівняння (6.1) не виконується, то відповідно n - складене;

5) якщо порівняння (6.1) виконується, то відповідь невідома, але можна повторити тест ще декілька разів. При його використанні виникає тільки дві ситуації:

а) число n - просте й тест завжди говорить «невідомо»;

б) число n - складене й тест з імовірністю успіху не менше 1/2 дає відповідь «n - складене».

Якщо виконується порівняння (6.1), то говорять, що число n є псевдопростим на основі підстановки a. Треба зауважити, що існує нескінченно багато пар чисел (a,n), де n - складене й псевдопросте. Наприклад, при $(a,n)=(2,341)$ одержуємо $2^{340} = \left(2^{10}\right)^{34} \equiv 1 (\mathrm{mod}\, n)$, хоча $431 = 11 \times 31$.

Для кожного $a > 1$ є нескінченно багато псевдопростих на основі підстановки a. Наприклад, якщо пар $(2,n)$ задовольняє порівняння (6.1), то й пара $\left(2,2^n - 1\right)$ його задовольняє.

6.4.4 Тест Рабина – Міллера

Нехай n - непарне, а $n-1 = 2^s t$, t - непарне. Якщо число n є простим, то буде виконуватися порівняння $a^n \equiv 1 (\mathrm{mod}\, n)$. Тому, розглядаючи елементи a^t, a^{2t},…, $a^{2^{s-1}t}$, можна помітити, що або серед них знайдеться рівний $-1 (\mathrm{mod}\, n)$, або $a^t \equiv 1 (\mathrm{mod}\, n)$.

На цьому твердженні заснований імовірнісний тест простоти числа:

1) вибираємо випадкове число a з інтервалу $\{1,2,...,n-1\}$ й перевіряємо за допомогою алгоритму Евкліда $\gcd(a,n)=1$;

2) якщо умова не виконується, то відповідь «n - складене»;

3) обчислюємо $a^t \pmod n$;

4) якщо $a^t \equiv \pm 1 \pmod n$, то переходимо до п.1;

5) обчислюємо $\left(a^t\right)^2 \pmod n$, $\left(a^t\right)^4 \pmod n$, …, $\left(a^t\right)^{2^{s-1}} \pmod n$ доти, поки не з'явиться -1;

6) якщо жодне із цих чисел не дорівнює -1, то відповідь «n - складене»;

7) якщо ми отримали -1, то відповідь невідома (і тест можна повторити ще раз).

6.5 Криптоалгоритм Ель-Гамаля

Криптографи постійно вели пошук більш стійких систем відкритого шифрування, і в 1985 р. Ель-Гамаль запропонував таку схему на основі піднесення в степінь за модулем великого простого числа. Для цього задається велике просте число p. Повідомлення представляються цілими числами s з інтервалу $[0, p-1]$. Оригінальний протокол передачі повідомлення s виглядає у варіанті Шаміра, одного з авторів RSA, таким чином.

1. Відправник Аліса й одержувач Боб знають лише p. Аліса генерує випадкове число x з інтервалу $[2, p-1]$ й, Боб теж генерує випадкове число y з того самого інтервалу.

2. Аліса шифрує повідомлення $s_1 = s^x \pmod p$ й посилає Бобу.

3. Боб шифрує його своїм ключем $s_2 = s_1^y \pmod p$ і посилає до Аліси.

4. Аліса «знімає» свій ключ $s_3 = s_2^{(-x)} \pmod p$ і повертає Бобу.

5. Одержувач Боб розшифровує повідомлення:

$s = s_3^{(-y)} (\mathrm{mod}\ p)$.

Цей протокол можна застосувати, наприклад, для таких несподіваних цілей, як гра в очко або блэкджек по телефону.

У системі Ель-Гамаля більший степінь захисту, ніж в алгоритму RSA, досягається з тим же за розміром модулем, що дозволяє майже на порядок збільшити швидкість шифрування й розшифрування. Криптостійкість системи Ель-Гамаля заснована на тому, що можна легко обчислити степінь цілого числа, тобто зробити множення його самого на себе будь-яке число раз так само, як і при операціях зі звичайними числами. Однак важко знайти показник степеня, до якого потрібно піднести задане число, щоб одержати інше, теж задане. У загальному випадку ця задача дискретного логарифму буде більш складною, ніж розкладання великих чисел на прості співмножники, на підставі чого можна припустити, що складності розкриття систем RSA і Ель-Гамаля будуть подібними. З точки зору практичної реалізації, як програмним, так і апаратним способом відчутної різниці між цими двома стандартами немає. Однак у криптостійкості вони помітно відрізняються. Якщо розглядати задачу розкладання довільного цілого числа довжиною в 512 біт на прості множники й задачу логарифмування цілих чисел по 512 біт, друга задача, за оцінками математиків, набагато складніше від першої. Однак є одна особливість. Якщо в системі, що побудована за допомогою алгоритму RSA, криптоаналітику вдалося розкласти відкритий ключ n одного з абонентів на два простих числа, то можливість зловживань обмежується тільки цим конкретним користувачем. У випадку ж системи, побудованої за допомогою алгоритму Ель-Гамаля, погрозі розкриття піддадуться всі абоненти криптографічної мережі. Крім того, Ленстра й Манассі не тільки похитнули стійкість RSA, розклавши дев'яте число Ферма на прості множники за дуже короткий час, але й, як було наголошено деякими експертами, указали «пролом» у способі Ель-Гамаля. Справа в тому, що підхід, що застосовувався при розкладанні на множники дев'ятого числа Ферма, дозволяє

суттєво вдосконалити методи дискретного логарифмування для окремих спеціальних простих чисел. Тобто той, хто пропонує просте p для алгоритму Ель-Гамаля, має можливість вибрати спеціальне просте, для якого задача дискретного логарифмування буде цілком під силу звичайним ЕОМ.

Слід помітити, що цей недолік алгоритму Ель-Гамаля не фатальний. Досить передбачити процедуру, яка буде гарантувати випадковість вибору простого p в цій системі, і тоді тільки що висловлене заперечення втрачає силу. Варто відзначити, що чисел спеціального виду, що послабляють метод Ель-Гамаля, дуже мало й випадковістю їхнього вибору можна зневажити.

6.6 Ще одна схема шифрування Ель-Гамаля

Схема Ель-Гамаля опирається на складність розв'язку задачі дискретного логарифма.

Просте число p й випадкове число $q < p$ входять до відкритого ключа й можуть використовуватися групою користувачів. Випадкове число $x < p$ є закритим ключем (Аліси).

Обчислюється $y = g^x \pmod p$, яке також входить у відкритий ключ і може використовуватися групою користувачів.

Отже, відкритий ключ – (y, g, p).

Нехай m – відкрите повідомлення. Боб шифрує це повідомлення й посилає його до Аліси. Для цього він вибирає випадкове число k й знаходить

$$a = g^k \pmod p,$$

$$b = y^k \cdot m \pmod p,$$

а число k рекомендується забути. Пара (a, b) є шифрованим текстом.

Дешифрування робить Аліса, обчислюючи

$$m \equiv b \cdot \left(a^x\right)^{-1} \pmod p.$$

Дійсно,

$$b \cdot \left(a^x\right)^{-1} (\mathrm{mod}\ p) = g^{kx} \cdot m \cdot \left(g^{kx}\right)^{-1} (\mathrm{mod}\ p) = m (\mathrm{mod}\ p).$$

Приклад 6.3

Нехай $p = 23$, $g = 2$, $x = 13$, $m = 19$, $k = 5$.

Обчислюємо $y = 2^{13} (\mathrm{mod}\, 23) = 4 (\mathrm{mod}\, 23)$.

Відкритий ключ – $(4,2,23)$.

Відкрите повідомлення $m = 13$. Шифруємо його:

$a = 2^5 (\mathrm{mod}\, 23) = 9 (\mathrm{mod}\, 23)$,

$b = 4^5 \cdot 13 (\mathrm{mod}\, 23) = 18$.

Шифрований текст – $(9,18)$.

Розшифрування:

$$m = 18 \cdot \left(9^{13}\right)^{-1} (\mathrm{mod}\, 23) = 18 \cdot \left(9^{-1}\right)^{13} (\mathrm{mod}\, 23) = 13.$$

6.7 Алгоритм «Рюкзака»

У цьому розділі ми опишемо інший тип криптосистем з відкритим ключем, який використовує так звану «задачу про рюкзак» [5, 12, 15]. Є рюкзак об'єму v і є k предметів з об'ємами v_i, $i = 0,1,...,k-1$, які можна покласти в рюкзак. Потрібно так вибрати частину (або всі) предметів, щоб повністю заповнити весь об'єм v рюкзака. Передбачається, що числа v й v_i цілі. Точне формулювання задачі таке: задані цілі числа v й v_i, $i = 0,1,...,k-1$. Потрібно так визначити вектор $n = \{\varepsilon_0, \varepsilon_1, ..., \varepsilon_{k-1}\}$, де $\varepsilon_i = 0$ або 1, щоб

$$v = \sum_{i=0}^{k-1} v_i \varepsilon_i .$$

Задача може не мати розв'язків, може мати одне або кілька розв'язків.

Є окремий випадок, коли задача про рюкзак має простий розв'язок (або простий доказ відсутності розв'язку). Назвемо

вектор $a=\{v_0,v_1,...,v_{k-1}\}$ рюкзачним вектором і припустимо, що його компоненти v_i впорядковані: $v_i \le v_{i+1}$. Такий вектор назвемо зростаючим. Якщо ж $v_0+...+v_i < v_{i+1}$ (кожний наступний компонент зростаючого вектора більше суми всіх попередніх), то вектор a називається надзростаючим.

Відомо, що загальна задача про рюкзак відноситься до класу дуже важких задач, названих «NP - повними задачами». Але задача про рюкзак з надзростаючим вектором a є простою й має такий алгоритм розв'язку.

1. Нехай w буде рівним v і j рівним k.

2. Починаючи з ε_{k-1} і послідовно зменшуючи j від $k-1$, вважаючи всі $\varepsilon_j = 0$, доти, поки не прийдемо до першого такого значення i (позначимо його через i_0), що $v_{i_0} \le w$. Допустимо $\varepsilon_{i_0} = 1$.

3. Замінимо w на $w - v_{i_0}$, допустимо $j = i_0$ й, якщо $w > 0$, то переходимо до п.2.

4. Якщо $w = 0$, то мета досягнута. Якщо $w > 0$ й усі останні $v_i > w$, то ясно, що розв'язку $n=\{\varepsilon_{k-1},...,\varepsilon_0\}$ не існує. Зауважимо, що розв'язок, якщо він існує, єдиний.

Приклад 6.4

Нехай $a=\{2,3,7,15,31\}$, $v=24$. Тоді проходячи вектор a справа наліво, ми бачимо, що $\varepsilon_3 = 1$ (у цей момент ми заміняємо 24 на 24-15=9), $\varepsilon_2 = 1$ (у цей момент ми заміняємо 9 на 9-7=2), $\varepsilon_1 = 0$, $\varepsilon_0 = 1$. Таким чином, $n=(0,1,1,0,1)$.

Тепер опишемо, як побудувати рюкзачну криптосистему. Спочатку припустимо, що елементи відкритого тексту мають у якості своїх числових кодів k-розрядні двійкові числа P. Наприклад, якщо ми маємо справу з окремими буквами 26-ти буквеного алфавіту, то кожній букві ставиться у відповідність своє пятирозрядне двійкове число від 0=(00000) до 25=(11001).

Далі кожний користувач вибирає надзростаючий вектор $\{v_0,...,v_{k-1}\}$, ціле число m, більше $v_0+...+v_{k-1}$, і взаємно просте із m ціле число a, $0<a<m$. Потім обчислюються $b=a^{-1}(\mathrm{mod}\, m)$ й k -елементний набір $\{w_i\}$, обумовлений рівностями $w_i \equiv av_i(\mathrm{mod}\, m)$. Користувач тримає числа v_i, m, a, b в секреті, а набір $\{w_i\}$ робить загальновідомим. Таким чином, ключем шифрування K_E є набір $\{w_0,...,w_{k-1}\}$, а ключем дешифрування K_D – пара (b,m) (яка разом із ключем шифрування дозволяє визначити набір $\{v_0,...,v_{k-1}\}$).

Бажаючий передати повідомлення P користувачеві, чий відкритий ключ шифрування $\{w_i\}$, обчислюємо $C=f(P)=\sum_{i=0}^{k-1}\varepsilon_i w_i$ й передаємо це ціле число.

Щоб прочитати отримане повідомлення, одержувач спочатку знаходить найменший додатній лишок V числа bC за модулем m.

Оскільки

$$bC=\sum_{i=0}^{k-1} b\varepsilon_i w_i \equiv \sum_{i=0}^{k-1}\varepsilon_i v_i(\mathrm{mod}\, m),$$

то $v \equiv \sum \varepsilon_i v_i$. Замість знака порівняння можна поставити знак рівності, тому що в лівій і правій частині стоять цілі числа, менші m. Тепер можна скористатися наведеним вище алгоритмом для задачі про рюкзак з надзростаючим рюкзачним вектором і знайти єдиний розв'язок $n=(\varepsilon_{k-1},...,\varepsilon_1,\varepsilon_0)$. Так ми відновлюємо повідомлення P.

Зауважимо, що зловмиснику, який знає тільки набір $\{w_i\}$, доведеться вирішувати задачу про рюкзак $C=\sum w_i\varepsilon_i$ уже не з надзростаючим набором, оскільки властивість надшвидкого росту $\{v_i\}$ перетворюється множенням на a й приведенням за модулем m.

Нова задача, що виникає перед зловмисником є значно більш складнішою.

Приклад 6.5

Припустимо, що елементами відкритого тексту є букви 26-буквеного алфавіту, яким, як і вище, відповідають двійкові числа від 0=(00000) до 25=(11001), а наш секретний ключ дешифрування – це надзростаючий вектор з попереднього прикладу - (2, 3, 7, 15, 31). Виберемо $m = 61$, $a = 17$. Тоді $b = 18$ й ключ шифрування – це вектор (34, 51, 58, 11, 39). Щоб передати повідомлення "WHY", наш кореспондент повинен обчислити коди

$W = (10110) \Rightarrow 51 + 58 + 39 = 148$,

$H = (00111) \Rightarrow 34 + 51 + 58 = 143$,

$Y = (11000) \Rightarrow 11 + 39 = 50$.

Щоб прочитати повідомлення 148, 143, 50, ми спочатку множимо ці числа на 18 і приводимо результати за модулем 61; і одержимо 41, 12, 46. Далі, беручи по черзі $v = 41$, $v = 12$, $v = 46$ ми відновимо повідомлення (10110), (00111), (11000).

Деякий час багато фахівців оптимістично оцінювали можливості рюкзачних систем. Однак у 1982 році криптограф Шамір знайшов поліноміальний алгоритм розв'язку задач про рюкзак. Разом з тим, можна так ускладнити рюкзачний алгоритм, що він буде захищений від алгоритму Шаміра. Досить застосувати послідовно два перетворення з параметрами (a_1, m_1) й (a_2, m_2) при деяких умовах для них [16].

7 ЕЛЕКТРОННИЙ ПІДПИС

Досить часто діючі системи передачі даних мають недолік, який полягає в тому, що вони не дають можливості перевірки дійсності й авторства документів, що пересилаються. З їхньою допомогою в цей час неможливий висновок угод, що юридично визнаються, і пересилання юридично підтверджуваних

документів, начебто платіжних доручень. Це часто зводить нанівець їх перевагу в порівнянні з поштовим пересиланням.

Розв'язок проблеми авторства документа може бути досягнуте лише з використанням електронного цифрового підпису - засобу, що дозволяє на основі криптографічних методів належно встановити авторство й дійсність документа. Цей засіб дозволяє замінити при електронному документообігу традиційні печатку й підпис. Електронний цифровий підпис залежить від тексту документа завірення, що вимагає, секретного ключа, доступного, що тільки завіряє, і несекретного загальнодоступного ключа. Перетворення, використовуване для вироблення цифрового підпису, є криптографічною функцією від зазначених величин. Воно вибирається таким чином, щоб при відсутності у зловмисника секретного ключа унеможливити підробку цифрового підпису, непомітну зміну документа, а також дати можливість будь-якій особі при наявності в нього загальнодоступного ключа, документа й цифрового підпису впевнитися в дійсності документа й відповідної до цифрового підпису. Тільки секретний ключ гарантує неможливість підробки зловмисником документа й цифрового підпису від шимени, що завіряє. Кожний користувач системи цифровому підпису повинен забезпечувати збереження в таємниці свій секретний ключ. Загальнодоступний несекретний ключ використовується для перевірки дійсності документа й цифрового підпису, а також попередженні шахрайства з боку особи, що завіряє.

Цифровий підпис не має нічого загального з послідовністю символів, відповідних до зображень печатки або підписи, приписаної до документа. Якби це було так, то, перехопивши один раз цю послідовність, зловмисник міг би надалі приписувати її до довільного документа від чужого імені. При побудові цифрового підпису замість звичайного зв'язку між печаткою або рукописним підписом і аркушем паперу виступає складна математична залежність між документом, секретним і загальнодоступним ключами, а також цифровим підписом. Неможливість підробки електронному підпису опирається не на

відсутність фахівця, який може повторити рукописний підпис і звичайну печатку, а на великий об'єм необхідних математичних обчислень. У сучасній криптографії є приклади описаних вище функцій, для яких складність підробки цифровому підпису при відсутності секретної інформації, що завіряє така, що сама потужна з існуючих надшвидкодіючих ЕОМ не зможе здійснити необхідні обчислення й за десятки років.

Через те що не важливо в який спосіб буде виконано операції множення в алгоритмі RSA не має значення, чи буде опубліковано d або e, для нього функції шифрування й розшифровування однакові. Це дозволяє реалізувати процедуру одержання цифрового підпису зміною d й e. Якщо відправник прагне, щоб одержувачі його повідомлень могли впевнитися, що ці повідомлення дійсно виходять від нього, то він посилає шифрування s разом з підписом r, обчислений, як

$$s = r^e \pmod{n}.$$

Для вирішення спорів між відправником і одержувачем інформації, пов'язаних з можливістю перевірки підміни ключа і підпису (s, r), достовірна копія цього ключа видається третій стороні, арбітрові, й застосовується ним при виникненні конфлікту. Кожний може розшифрувати повідомлення s, але, оскільки ключ e відомий тільки відправникові, то ніхто іншої крім нього не міг би послати шифроване повідомлення або підтвердити підпис як:

$$s = r^d \pmod{n}.$$

Для того, щоб забезпечити подібну процедуру підтвердження справжності відправника повідомлення, Ель-Гамаль запропонував такий простий протокол.

1. Відправник Аліса й одержувач Боб знають p і випадкове n число з інтервалу $(1, p)$. Аліса генерує випадкові числа x й y з того самого інтервалу. x потрібно зберігати в секреті, а y повинне бути взаємно простим з $p-1$.

2. Далі Аліса обчислює $q = n^x \pmod p$ й $q = n^y \pmod p$, вирішує відносно s рівняння $t = x \cdot r + y \cdot s \pmod p$ й передає Бобу документ із підписом (q, r, s, t).

3. Одержувач перевіряє підпис, контролюючи тотожність $a^s = b^r \cdot r^t \pmod p$.

У цій системі секретним ключем для підписування повідомлень є число x, а відкритим ключем для перевірки дійсності підписи число q.

Особливістю цих протоколів, як ми бачимо, є наявність в абонента секретного ключа, що служить цифровим підписом ідентифікатора, який не дозволяє абонентові самому перемінити свій ідентифікатор або виробити підпис для іншого ідентифікатора, а також те, що він пред'являє контролерові не сам секретний елемент, а деяке значення функції, що обчислюється за допомогою секретного ключа з випадкового запиту, тим самим доводячи, що має секрет, шляхом його непрямої демонстрації при обчисленнях. Саме звідси виходить розглянута нижче назва «доказ при нульовому знанні», тобто абонент доводить, що має секрет, не розкриваючи самого секрету.

Як окремий випадок алгоритму цифрового підпису можна розглядати шифрування й розшифровування переданої інформації на загальному секретному ключі абонентів, який обчислюється й поширенні заздалегідь, як це застосовується в класичних криптографічних системах.

7.1 Електронний підпис по Ель-Гамалю (другий варіант)

Просте число p й випадкове число $g < p$ входять у відкритий ключ і можуть використовуватися групою користувачів.

Випадкове число $x < p$ є закритим ключем (Аліси).

Обчислюється $y = g^x \pmod p$, яке також входить у відкритий ключ і може використовуватися групою користувачів.

Отже, відкритий ключ – (y, g, p).

Нехай m – відкрите повідомлення. Аліса, не шифруючи це повідомлення, повинна підписати його й послати Бобу. Для цього вона вибирає випадкове число k, взаємно просте з $p-1$, і обчислює

$$a = g^k \pmod p.$$

Потім, знаходячи $k^{-1} \pmod{p-1}$ (розширений алгоритм Евкліда), з порівняння

$$m = x \cdot a + k \cdot b \pmod{p-1}$$

обчислює b.

Підписом є пара (a,b).

Підпис дійсний, якщо вірне порівняння $y^a \cdot a^b = g^m \pmod p$. Дійсно,

$$y^a \cdot a^b = g^{ax} \cdot g^{kb} = g^{ax+kb \pmod{p-1}} \pmod p = g^m \pmod p.$$

Зауваження

Кожний підпис вимагає нового значення k, обраного випадковим чином. Якщо коли-небудь або хто-небудь довідається k, використовуване Алісою, він зможе знайти закритий ключ Аліси x.

Якщо хто-небудь зможе одержати два повідомлення, підписані з тим самим k (навіть не знаючи його), він зможе знайти x.

7.2 Однобічні хеш-функції

Однобічна функція $H(M)$ застосовується до повідомлення M довільної довжини й повертає значення h фіксованої довжини m

$$h = H(M).$$

Багато функцій дозволяють обчислювати значення фіксованої довжини за вхідним даними довільної довжини, але

для однобічних хеш-функцій є додаткові властивості, що роблять ці функції однобічними:

1) знаючи M, легко обчислити h;

2) знаючи H, важко визначити M, для якого $h = H(M)$;

3) знаючи M, важко визначити інше повідомлення M', для якого $H(M) = H(M')$.

Зміст однобічних хеш-функцій полягає в забезпеченні для M унікального ідентифікатора. Якщо Аліса підписала M за допомогою алгоритму цифрового підпису на базі $H(M)$, а Боб може створити інше повідомлення M', для якого $H(M) = H(M')$, то Боб зможе підтверджувати, що Аліса підписала M'.

У деяких моментах властивості однобічності недостатньо, необхідне виконання іншої вимоги, що називається стійкістю до зіткнень: повинно бути важко знайти два випадкові повідомлення M і M', для яких $H(M) = H(M')$.

Такий протокол показує, як, якщо не виконується вимога стійкості до зіткнень, Аліса може використовувати розкриття методом дня народження для обману Боба.

1. Аліса готує дві версії контракту: одну, вигідну для Боба, і іншу, що приводить його до банкрутства.

2. Аліса вносить кілька незначних змін у кожний документ і обчислює хеш-функції. Роблячи або не роблячи по одній зміні в кожному з n рядків, Аліса може легко одержати 2^n версій кожного документа.

3. Вона відновлює два документа, що дають однакове хеш-значення.

4. Аліса одержує підписану Бобом вигідну для нього версію контракту, використовуючи протокол, у якім він підписує тільки хеш-значення.

5. Через деякий час Аліса виконує підміну контракту, підписаного Бобом, іншим, який він не підписував. Тепер вона може переконати арбітра в тому, що Боб підписав інший контракт.

8 СТАНДАРТ ПІДПИСУ DSA (DIGITAL SIGNATURE ALGORITM)

Алгоритм має такі параметри:

p – просте число довжиною L біт, де L деяке значення, кратне 64, у діапазоні від 512 до 1024 (може використовуватися групою користувачів).

q – 160-бітове просте число, що ділить $p-1$ (може використовуватися групою користувачів).

$g = h^{\frac{(p-1)}{q}} \pmod p$,

де h – будь-яке число, менше $p-1$, для якого $h^{\frac{(p-1)}{q}} \pmod p$ більше 1 (може використовуватися групою користувачів).

x – число, менше q.

$y = g^x \pmod p$.

В алгоритмі також використовується однобічна хеш-функція $H(M)$. Стандарт визначає використання SHA-функції (тут не розглядається конструкція SHA).

Перші три параметри (g, q, p) відкриті й можуть бути загальними для користувачів мережі. Закритим ключем є x, а відкритим – y.

Щоб підписати повідомлення M, потрібно виконати такі дії.

1. Аліса генерує випадкове число k, менше q.

2. Аліса генерує:

$r = \left(g^k \pmod p\right) \pmod q$,

$s = \left(k^{-1}\left(H(m) + xr\right)\right) \pmod q$.

Її підписом служать параметри (r, s). Їх вона посилає Бобу.

3. Боб перевіряє підпис, обчислюючи:

$w = s^{-1} \pmod q$,

$u_1 = \left(H(M) \cdot w\right) \pmod q$, $u_2 = (r \cdot w) \pmod q$,

$v = \left(g^{u_1} \cdot y^{u_2} \pmod p\right) \pmod q$.

Якщо $v = r$, то підпис правильний.

9 КРИПТОАНАЛІЗ – 2

Щоб одержати уявлення про несанкціоновані й зловмисні дії стосовно інформації, процитуємо Г. Дж. Симмонса [6]:

«…Цілі й стратегії порушника.

1. Одержання несанкціонованого доступу, тобто порушення таємності або конфіденційності.

2. Видача себе за іншого користувача, щоб зняти із себе відповідальність або ж використовувати його повноваження з метою:

а) формування неправдивої інформації;

б) зміни законної інформації;

в) застосування неправильного посвідчення особи для одержання несанкціонованого доступу;

г) санкціонування неправильних обмінів інформації або ж їх підтвердження.

3. Відмова від факту формування інформації.

4. Твердження про те, що інформація отримана від деякого користувача, хоча насправді вона сформована самим же порушником.

5. Твердження про те, що одержувачеві (у певний момент часу) була послана інформація, яка насправді не посилала (або посилала в інший момент часу).

6. Відмова від факту одержання інформації, яка насправді була отримана, або неправильне твердження про час її одержання.

7. Розширення своїх законних повноважень (на доступ, формування, поширення і т.д.).

8. Зміна (без санкції на те) повноважень інших користувачів (неправильний запис у списки інших осіб, обмеження або розширення існуючих повноважень і т.д.).

9. Приховання факту наявності деякої інформації (схована передача) в іншій інформації (відкрита передача).

10. Підключення до лінії зв'язку між іншими користувачами у ролі активного (прихованого) ретранслятора.

11. Вивчення того, хто до якої інформації (джерела, факти і т.д.) одержує доступ і коли (навіть якщо сама інформація

залишається прихованою), тобто узагальнення даних, отриманих з аналізу потоку повідомлень у каналах зв'язку, на структуру баз даних, програмне забезпечення і т.д.

12. Заява про сумнівність протоколу забезпечення цілісності інформації шляхом розкриття інформації, яка згідно з умовами протоколу повинна залишатися секретною.

13. Модифікація програмного забезпечення, як правило шляхом непомітного додавання нових функцій.

14. Змушення інших порушувати протокол шляхом уведення неправильної інформації.

15. Підрив довіри до протоколу шляхом виклику очевидних порушень.

16. Спроба перешкодити передачам повідомлень між іншими користувачами, зокрема, внесення в повідомлення прихованих перешкод з тією метою, щоб це повідомлення при аутентифікації було відкинуто».

9.1 Атаки (розкриття) на шифри

Приклади атак.

1. Зловмисник перехоплює g_a від Аліси, блокуючи її повідомлення.

2. Зловмисник бере своє повідомлення m й під видом Аліси посилає Бобу g_a^m.

3. Аліса обчислює $k_1 = g^{am}$.

4. Аналогічно, Боб обчислює $k_2 = g^{bm}$.

Тепер між Алісою й зловмисником, Бобом і зловмисником є переписка, але тільки Аліса й Боб думають, що переписка йде між ними. Протистояти цій атаці можна за допомогою електронного підпису.

Зауваження

Є типовий приклад атаки «людина посередині». Слабкий гравець у шахи грає відразу із двома гросмейстерами. Відповідні ходи гросмейстерів, передані по лінії зв'язку, видає за свої.

У підсумку слабкий гравець або «зробить» дві нічиї, або одну партію програє, а іншу виграє!

Стійкість криптографічної схеми визначається щодо пари (атака, погроза). Одним із найважливіших напрямків теоретичних досліджень є пошук схем, стійких проти самої слабкої з відомих погроз, у припущенні, що супротивник може провести найсильнішу з можливих атак. Необхідно підкреслити, що ніяка криптографічна схема не може бути стійкою «взагалі». Класичним прикладом тут може служити шифр Вернама, абсолютно стійкий проти пасивного підслуховування. Однак, якщо задача активного супротивника полягає просто в зміні даного фіксованого біта відкритого тексту на протилежний, то він легко може здійснити цю атаку. Інший досить відомий приклад – криптосистема Рабіна, за доведенням стійка (у припущенні складності задачі факторизації цілих чисел) проти атаки з вибором відкритого тексту, але нестійка проти атаки з вибором шифрованого тексту.

Опишемо спочатку атаки на криптосистеми із секретним ключем.

Атака з відомим шифрованим текстом (ciphertext-only attack). Сама слабка із усіх можливих атак. Передбачається, що супротивник знає криптосистему, тобто алгоритми шифрування й дешифрування, але не знає секретний ключ. Крім цього, йому відомий лише набір перехоплених криптограм.

Атака з відомим відкритим текстом (known-plaintext attack). Те саме, що попередня, але супротивник одержує у своє розпорядження ще деякий набір криптограм і відповідних їм відкритих текстів.

Проста атака з вибором відкритого тексту (chosen-plaintext attack). Передбачається, що супротивник має можливість вибрати необхідну кількість відкритих текстів і одержати їхні криптограми. При цьому всі відкриті тексти повинні бути обрані заздалегідь, тобто, до одержання першої криптограми. У зарубіжній літературі цю атаку часто називають «опівнічною» атакою (midnight attack) або coffee-break attack, що відповідає реальній ситуації, коли персонал залишив обладнання

шифрування в робочому стані і їм тимчасово заволодів супротивник. Хоча секретний ключ йому недоступний, супротивник може зашифрувати підготовлені їм відкриті тексти, що дає йому додаткову інформацію для нападу на криптосистему.

Адаптивна атака з вибором відкритого тексту. Те саме, що попередня, але, вибираючи наступний відкритий текст, супротивник уже знає криптограми всіх попередніх.

Проста атака з вибором шифрованого тексту (chosen-ciphertext attack). Супротивник має можливість вибрати необхідна кількість криптограм і одержати відповідні їм відкриті тексти. При цьому всі криптограми повинні бути обрані заздалегідь, тобто до одержання першого відкритого тексту.

Адаптивна атака з вибором шифрованого тексту. Те саме, що попередня, але, вибираючи наступну криптограму, супротивник уже знає відкриті тексти, що відповідають усім попереднім.

Атака з вибором тексту (chosen-text attack). Супротивник має можливість атакувати криптосистему «з обох кінців», тобто, вибирати як криптограми (і дешифрувати їх), так і відкриті тексти (і шифрувати їх). Атака з вибором тексту може бути простою, адаптивною, а також простою «з одного кінця» і адаптивною з іншого.

Атаки перелічені у порядку зростання їх сили, тобто, атака з вибором тексту є найдужчою з усіх відомих атак на криптосистеми.

Для криптосистем з відкритим ключем класифікація атак аналогічна, але слід мати на увазі, що супротивник завжди знає криптосистему й відкритий ключ, а адаптивна атака з вибором відкритого тексту є самою слабкою з можливих атак на криптосистеми з відкритим ключем – супротивник завжди має можливість провести таку атаку.

Крім того, існують атаки, специфічні для криптосистем з відкритим ключем. Наприклад, якщо число можливих відкритих текстів невелике, то супротивник, знаючи відкритий ключ, може заздалегідь підготувати достатню кількість криптограм і потім,

порівнюючи ці «заготовки» з перехопленими криптограмами, з високою ймовірністю одержувати відповідні відкриті тексти. Така атака називається атакою з перевіркою тексту (verifiable-text attack).

Типи погроз не мають настільки чіткої класифікації як типи атак. У літературі найчастіше спостерігається така ситуація: дається досить точне визначення типу атаки, відносно якої розглядається стійкість криптосистеми, але нічого не говориться про те, що розуміється під розкриттям криптосистеми, тобто, у чому полягає задача супротивника. Виділимо такі (перелічені у порядку ослаблення) типи погроз.

Повне розкриття. У результаті проведеної атаки супротивник обчислює секретний ключ криптосистеми, або знаходить алгоритм, функціонально еквівалентний алгоритму дешифрування, який до того ж не вимагає знання секретного ключа.

Розкриття тексту. У результаті проведеної атаки супротивник повністю відновлює відкритий текст, відповідний до перехопленої криптограми. Звичайно передбачається, що відкритий текст вибирається випадковим чином з деякої множини відкритих текстів, а відновлення відкритого тексту за криптограмою становить погрозу для безпеки, якщо ймовірність такого відновлення не є в деякому змісті «дуже малою».

Часткове розкриття. Супротивник у результаті атаки одержує часткову інформацію про секретний ключ або про відкритий текст. Хоча така погроза досить часто обговорюється в літературі, у загальному випадку далі словесних формулювань справа не йде. Причина, очевидно, у тому, що саме поняття часткової інформації досить розмите й може бути уточнене множиною різних способів. Погроза часткового розкриття формалізована лише для абсолютно стійких (у шеннонівському змісті) криптосистем і криптосистем імовірнісного шифрування.

Наведемо тепер класифікацію типів атак на схеми електронного підпису, яку запропонували Гольдвассер, Микалі й Рівест. Атаки наведені в такому переліку, що кожна наступна сильніша від попередньої.

Атака з відомим відкритим ключем. Супротивник знає тільки відкритий ключ схеми електронному підпису. Це сама слабка з усіх можливих атак. Очевидно, що супротивник завжди може провести таку атаку.

Атака з відомими повідомленнями. Супротивник знає відкритий ключ схеми й, крім того, одержує деякий набір підписаних повідомлень. При цьому супротивник ніяк не може вплинути на вибір цих повідомлень.

Проста атака з вибором повідомлень. Супротивник має можливість вибрати необхідну кількість повідомлень і одержати підписи для них. Передбачається, що ці повідомлення вибираються незалежно від відкритого ключа, наприклад, швидше, ніж відкритий ключ стане відомий.

Спрямована атака з вибором повідомлень. Та сама, що попередня, але супротивник, вибираючи повідомлення, уже знає відкритий ключ.

Адаптивна атака з вибором повідомлень. Та сама, що попередня, але супротивник вибирає повідомлення послідовно, знаючи відкритий ключ і знаючи на кожному кроці підписи для всіх раніше обраних повідомлень.

Погрозами для схеми електронного підпису є розкриття схеми або підробка підпису. Гольдвассер, Микалі й Рівест уточнюють поняття погрози, визначаючи такі (перелічені у порядку ослаблення) типи погроз.

Повне розкриття, тобто, визначення секретного ключа.

Універсальна підробка. Супротивник знаходить алгоритм, функціонально еквівалентний алгоритму обчислення підпису й не вимагає знання секретного ключа.

Селективна підробка. Підробка підпису для повідомлення, обраного супротивником. При цьому передбачається, що це повідомлення вибирається апріорі (до початку атаки) і що якщо супротивник проводить атаку з вибором повідомлень, то повідомлення, для якого потрібно підробити підпис, не може входити до числа обраних під час атаки.

Екзистенціальна підробка. Підробка підпису хоча б для одного повідомлення, яке не було підписано під час атаки.

Супротивник не контролює вибір цього повідомлення. Воно може виявитися випадковим або безглуздим.

Стійкість схеми визначається щодо пари (тип атаки, тип погрози). Схема вважається нестійкою проти даної погрози, якщо існує метод її здійснення з імовірністю, якою можна знехтувати.

9.2 Парадокс днів народження

Нехай дано довільне відображення $f : X \to Y$, де множина Y скінченна й містить n елементів. При деяких значеннях аргументів x_i, x_j значення функції в них можуть збігатися. Нас цікавить таке питання: яка мінімальна кількість k значень аргументів x потрібно мати, щоб імовірність

$$\{f(x_i) = f(x_j)\} \geq \varepsilon$$

для деяких $i \neq j$ і заданого ε.

Збіг $f(x_i) = f(x_j)$ у криптографії називається колізією. Інакше кажучи, нас цікавить відповідь на запитання – при якій кількості обчислень функції колізія виникає з імовірністю не менше ε. Для цього знайдемо ймовірність протилежної дії. Імовірність того, що $f(x_i) = f(x_j)$, рівна $1 - \frac{1}{n}$. Імовірність того, що не трапиться ні однієї колізії після k обчислень дорівнює

$$\left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right) \cdot \ldots \cdot \left(1 - \frac{k-1}{n}\right).$$

З курсу аналізу відомо, що

$$\left(1 + \frac{x}{n}\right)^n \approx e^x$$

або

$$1 + \frac{x}{n} \approx e^{\frac{x}{n}}.$$

Отже,

$$\left(1-\frac{1}{n}\right)\cdot\left(1-\frac{2}{n}\right)\cdot\ldots\cdot\left(1-\frac{k-1}{n}\right)=\prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right)=\prod_{i=1}^{k-1}e^{-\frac{i}{n}}=e^{-\frac{k(k-1)}{2n}}$$

Імовірність виникнення хоча б однієї колізії дорівнює $1-e^{-\frac{k(k-1)}{2n}}$.

Знаходячи розв'язок рівняння

$$e^{-\frac{k(k-1)}{2n}}\approx 1-\varepsilon,$$

одержимо

$$k\approx\sqrt{2n\log\frac{1}{1-\varepsilon}}.$$

Якщо $\varepsilon=0{,}5$ (імовірність колізії не менше 50%), то $k\approx 1{,}1774\sqrt{n}$.

Отже, щоб виявити колізію для функції з n значеннями з імовірністю 0,5, необхідно виконати приблизно $\sqrt{n}$ обчислень.

Застосування парадокса дня народження. Дискретний логарифм і алгоритм $1+\frac{x}{n}$ Полларда [14, 20].

Задача обчислення значення x за заданим $y=a^x(\mathrm{mod}\,p)$, де p – просте число, $a\geq 2$, $y\leq p-1$ чисельно дуже складна. Значення функції $y=a^x(\mathrm{mod}\,p)$ розкидані в інтервалі $(0,p)$, практично, випадковим чином. Наприклад, нехай $p=19$, $a=10$, тоді

при $x=$	1	2	3	4	5	6	7	8	9	…	17	18
при $y=$	10	5	12	6	3	11	15	17	18	…	2	1

Проблема визначення значення x за заданим $y=a^x(\mathrm{mod}\,p)$, де p – просте число, називається задачею обчислення індексу $ind_a y$ або дискретного логарифма $\log_a y(\mathrm{mod}\,p)$.

Як знайти досить швидко працюючий алгоритм обчислення показника x? Якщо p не занадто велике $p\approx 2^{100}$, то можна

застосовувати парадокс днів народження. Алгоритм був винайдений J. M. Pollard'ом і називається - λ-методом або методом кенгуру.

10 ДОКАЗ ПРИ НУЛЬОВІМ ЗНАННІ

На підставі описаних алгоритмів шифрування [10, 18, 20], розподілу ключів і електронного підпису можна організовувати більш складні протоколи взаємодії користувачів криптографічної мережі, що реалізують підтвердження справжності й доказ при нульовім знанні. Так звані системи «доказу при нульовім знанні» не є властиво криптографічними системами. Вони служать для передачі повідомлень типу «Я знаю цю інформацію» без розкриття самого повідомлення.

Загальна ідея цих протоколів полягає в тому, що власник секретного ключа доводить, що він може обчислювати деяку функцію, що залежить як від секретного ключа, так і аргументів, що задаються перевіряючим. Перевіряючий, навіть знаючи ці аргументи, не може по даному ньому значенню функції відновити секретний ключ. При цьому функція повинна бути такою, щоб перевіряючий міг упевнитися в правильності її обчислення, наприклад, представляла цифровий підпис обраних їм аргументів. Дію такої системи розглянемо на наведеному нижче алгоритмі, де підтвердження справжності при використанні алгоритму RSA організоване в такий спосіб.

1. Підтверджуючий Аліса й контролер Боб обоє знають ідентифікатор I і відкритий ключ (n,e), але Аліса крім того знає ще, секретне число $S = I^d \pmod n$, сформоване за секретним ключу (n,d). Спочатку Аліса генерує випадкове число X й обчислює $Y = X^e \pmod n$. Потім вона відсилає (I,Y) до Боба.

2. Після цього Боб генерує й передає Алісі випадкове число V.

3. Потім Аліса обчислює й передає Бобу число $W = X \cdot Y^V \pmod n$.

4. Контролер Боб перевіряє приналежність ідентифікатора I Аліси, звіряючи тотожність $W^e = Y \cdot I^V \pmod n$.

Випадковий запит як правило представлений вектором, координати якого набувають значення 0 або 1, але він може бути будь-яким вектором, координати якого обчислюються за модулем числа e.

11 ПРО КРИПТОГРАФІЧНІ ПРОТОКОЛИ

11.1 Вступ

Математична криптографія виникла як наука про шифрування інформації, тобто як наука про криптосистеми. У класичній моделі системи секретного зв'язку є два учасники, що повністю довіряють один одному, яким необхідно передавати між собою інформацію, не призначену для третіх осіб. Така інформація називається конфіденційною або секретною. Виникає задача забезпечення конфіденційності, тобто захисту секретної інформації від зовнішнього супротивника. Ця задача, принаймні історично, перша задача криптографії. Вона традиційно вирішується за допомогою криптосистем. Представимо тепер собі таку ситуацію. Є два абоненти А и В мережі зв'язку, скажімо, комп'ютерної мережі. В – це банк, у якім в А має рахунок і А прагне переслати В по мережі в електронній формі платіжне доручення перевести, наприклад, 10 фантиків зі свого рахунку на рахунок іншого клієнта С. Чи потрібен у цьому випадку криптографічний захист? Такий захист необхідний. Але тут слід зазначити такий дуже важливий момент: в А і В немає ніякої конфіденційної інформації. Насправді, клієнти пересилають банку платіжні доручення як повідомлення, зміст яких стандартний й загальновідомий. Для банку важливо переконатися в тому, що дане повідомлення

дійсне прийшло від А, а останньому, у свою чергу, необхідно, щоб ніхто не міг змінити суму, зазначену в платіжному дорученні, або просто послати підроблене доручення від його імені. Іншими словами, потрібна гарантія передачі повідомлень із достовірного джерела й у неспотвореному виді. Така гарантія називається забезпеченням цілісності інформації й складає другу задачу криптографії. Легко бачити, що при пересиланні платіжних доручень в електронній формі виникає ще й зовсім інший тип погроз безпеки клієнтів: будь-який, хто перехопить повідомлення від А до В, довідається, що С одержав від А 10 у.о. Клієнтам необхідно щось аналогічне властивості анонімності звичайних паперових грошей. Хоча кожна паперова купюра має унікальний номер, визначити, хто її використовував і в яких платежах, практично неможливо. Аналог цієї властивості в криптографії називається невідслідовністю. Забезпечення невідслідовності – третя задача криптографії. Якщо задача забезпечення конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності й невідслідовності розробляються криптографічні протоколи. Є й інші відмінності криптографічних протоколів від криптосистем, з яких можна виділити такі:

1) протоколи можуть бути інтерактивними, тобто мати на увазі багатоетапний обмін повідомленнями між учасниками;

2) у протоколі можуть брати участь більше двох учасників;

3) учасники протоколу, у загальному випадку, не довіряють один одному.

Криптографічні протоколи повинні захищати їхніх учасників не тільки від зовнішнього супротивника, але й від нечесних дій партнерів. На жаль, поняття криптографічного протоколу, неможливо формалізувати. Те саме ставиться й до задач забезпечення цілісності й невідслідовності. Під протоколом (не обов'язково криптографічним) як правило розуміють розподілений алгоритм, тобто сукупність алгоритмів для кожного з учасників, плюс специфікації форматів повідомлень, що пересилаються між учасниками, плюс специфікації синхронізації дій учасників, плюс опис дій при

виникненні збоїв. На останній елемент цього списку слід звернути особливу увагу, оскільки його часто випускають з уваги, а некоректний повторний пуск може повністю зруйнувати безпеку учасників навіть у стійкому криптографічному протоколі. Криптографічні протоколи – порівняно молода галузь математичної криптографії. Перші протоколи з'явилися близько 30 років тому. З тих пір ця галузь бурхливо розвивалася, і на даний момент є вже не менше двох десятків різних типів криптографічних протоколів. Усі ці типи можна умовно поділити на дві групи: прикладні протоколи й примітивні. Прикладний протокол вирішує конкретну задачу, яка виникає (або може виникнути) на практиці. Примітивні ж протоколи використовуються як своєрідні «будівельні блоки» при розробленні прикладних протоколів. У банківських платіжних системах у наші дні замість платіжних доручень на папері використовується їхня електронна форма. Переваги від такої заміни настільки відчутні, що, скоріш за все, банки від неї вже ніколи не відмовляться, які б технічні й криптографічні (пов'язані із забезпеченням цілісності) труднощі при цьому не виникали. Але платіжні доручення – лише один із багатьох типів документів, що перебувають в обороті у сфері бізнесу. Але ж існують ще документи, з якими працюють державні органі й громадські організації, юридичні документи й т.д. В останні роки в розвинених країнах чітко прослідковується тенденція перекладу всього документообігу в електронну форму. Важливо відзначити, що, оскільки перехід на електронні документи представляється неминучим, виникає необхідність забезпечення, у кожному конкретному випадку, цілісності й невідслідовності, тобто розроблення відповідних криптографічних протоколів.

11.2 Цілісність. Протоколи аутентифікації й електронного підпису

Поняття цілісності інформації, очевидно, не допускає математичної формалізації. У даному розділі ми розглянемо методи забезпечення цілісності на прикладі двох найбільш

важливих й поширених типів криптографічних протоколів – схем аутентифікації й електронного підпису. Призначення й суть протоколів аутентифікації (називають їх також протоколами ідентифікації) легко зрозуміти на такому прикладі. Представимо собі інформаційну систему, яка працює в комп'ютерній мережі й забезпечує доступ до деяких даних. В адміністратора системи є список усіх її користувачів разом із зіставленим кожному з них набором повноважень, на основі яких здійснюється розмежування доступу до ресурсів системи. Ресурсами можуть бути, наприклад, деякі фрагменти інформації, а також функції, виконувані системою. Деяким користувачам може бути дозволено читати одну частину інформації, іншим – іншу її частину, а третім – ще й вносити в неї зміни. У даному контексті під забезпеченням цілісності розуміється запобігання доступу до системи осіб, що не є її користувачами, а також запобігання доступу користувачів до тих ресурсів, на які в них немає повноважень. Найпоширеніший метод розмежування доступу, парольний захист, має масу недоліків. Перейдемо до криптографічної постановки задачі. У протоколі є два учасники – Аліса, яка повинна довести свою автентичність, і Боб, який цю автентичність повинен перевірити. В Аліси є два ключі – загальнодоступний відкритий K_1 і секретний K_2. Фактично, Алісі потрібно довести, що вона знає K_2, і зробити це таким чином, щоб це доведення можна було перевірити, знаючи тільки K_1. Нижче ми приводимо протокол Шнорра [1], один з найбільш ефективних практичних протоколів аутентифікаціи. Для його опису нам будуть потрібні деякі позначення.

Нехай p і q – прості числа такі, що q ділить $p-1$. Шнорр пропонує [1] використовувати p довжини порядку 512 біт і – q довжини порядку 140 біт (рекомендації вже застаріли). Нехай $g \in Z_p$ таке, що $g^q \pmod p = 1$, $g \neq 1$. Нехай $x \in Z_q$ і $y = g^x \pmod p$. Задача обчислення значення x за заданим значенням y при відомих p і q, і q є параметром задачі дискретного логарифмування.

У якості секретного ключа схеми аутентифікації Аліса вибирає випадкове число x з $\{1,2,...,q-1\}$. Далі Аліса обчислює $y = g^x \pmod p$ й публікує відкритий ключ y. Відкриті ключі всіх учасників схеми повинні публікуватися таким чином, щоб виключалася можливість їх підміни (таке сховище ключів називається загальнодоступним сертифікованим довідником). Ця проблема, часто називається, як проблема автентичності відкритих ключів, становить окремий предмет досліджень у криптографії й тут не розглядається. Наведемо схему аутентифікації Шнорра.

1. Аліса вибирає випадкове число k із множини $\{1,2,...,q-1\}$, обчислює $r = g^k \pmod p$ й посилає r Бобу.

2. Боб вибирає випадковий запит e із множини $\{1,2,...,2^{t-1}\}$, де t – деякий параметр, і посилає e до Аліси.

3. Аліса обчислює $s = k + xe \pmod q$ й посилає s Бобу.

4. Боб перевіряє співвідношення $r = g^s \cdot y^e \pmod p$ й, якщо воно виконується, ухвалює доказ, а якщо ні, то відкидає.

11.3 Невідслідовність. Електронні гроші

Оскільки даний розділ присвячений електронним грошам, розглянемо цю погрозу на такому простому прикладі. Настільки популярна нині в усьому світі кредитна картка являє собою носій інформації, який при кожному платежі повністю ідентифікує свого власника. І якщо власник картки використовує її для покупки квитків на транспорт, то можна відстежити всі його поїздки, що в цивілізованім суспільстві без санкції прокурора неприпустимо. Аналогічним чином, для кожного власника кредитних карток можна збирати інформацію про те, які товари й де він купує, якими послугами користується, які заходи він відвідує і т.д. Далі – більше. Організація комп'ютерного доступу до сховищ інформації й обробка документів в електронну форму створюють передумови для

ведення досьє, що відбивають усе коло інтересів кожного із громадян. Цей перелік погроз правам і свободам особи, безумовно, можна продовжити. Підводячи підсумок, можна сказати, що комп'ютеризація створює безпрецедентні можливості для організації тотального стеження. Погроза ця на стільки серйозна, що вона дотепер ще не усвідомлена навіть багатьма фахівцями.

Для запобігання подібної погрози необхідна система контролю над доступом до ресурсів, яка задовольняє двом вимогам, що взаємно виключають друг друга. По-перше, будь-який бажаючий повинен мати можливість звернутися до цієї системи анонімно, а по-друге, при цьому все-таки довести своє право на доступ до того або іншого ресурсу. Звичайні паперові гроші забезпечують обидві ці властивості. Якщо ресурсом, наприклад, є деякий товар, то наявність у покупця достатньої кількості купюр є доказом його права на доступ до ресурсу. З іншого боку, хоча кожна паперова купюра й має унікальний номер, відслідковувати купюри за номерами практично неможливо. Кредитні картки задовольняють тільки другу вимогу. Під електронними грошима ми будемо розуміти електронні платіжні засоби, що забезпечують невідслідовність. Поняття невідслідовності, так як і цілісності, очевидно, не може бути формалізоване й буде пояснюватися на конкретних прикладах протоколів.

11.4 Про протокол типу «підкидання монети по телефону»

У даному розділі ми коротко обговоримо ті типи криптографічних протоколів, у яких два учасники повинні обмінятися деякою інформацією. Але учасники не довіряють один одному й кожний з них може виявитися ошуканцем. Тому, якщо один з учасників за необережністю «випустить інформацію з рук» передчасно, то в обмін він може одержати зовсім не те, про що домовлялися, або взагалі не одержати

нічого: проблеми тут ті ж, що й в «протоколі» обміну розписки на асигнації у Чичикова й Собакевича.

З усіх криптографічних протоколів даного типу, мабуть, найбільш наочним, і до того ж досить простим, є протокол підкидання монети. Припустимо, що двом учасникам, Алісі й Бобу, необхідно кинути жереб. У випадку, коли вони обоє фізично перебувають у тому самому місці, задачу можна розв'язати за допомогою звичайної процедури підкидання монети. Якщо хто-небудь з учасників не довіряє монеті, можна використовувати інші джерела випадковості. Правда, створення надійних джерел випадковості – досить непроста задача, але вона вже ставиться до математичної статистики, а не до криптографії. Якщо ж Аліса й Боб віддалені друг від друга й можуть спілкуватися лише по каналу зв'язку, то задача про жереб, на перший погляд, видасться нерозв'язною. Насправді, якщо, слідувати звичайній процедурі підкидання монети, перший хід робить Аліса, яка вибирає один з можливих варіантів – «орел» або «решка», то Боб завжди може оголосити той результат, який йому вигідний.

Проте ця задача була вирішена Блюмом. Цікаво, що навіть у заголовку своєї роботи Блюм охарактеризував запропонований їм метод як метод «розв'язку нерозв'язаних задач».

ДОДАТОК А

Короткий англо-російський словник термінів з криптографії.

access control–контроль доступу, керування доступом;

access method – метод доступу;

access mode – режим доступу;

access right – право доступу;

access scan – пошук з перебором;

adversary-attacker – порушник, супротивник;

alter – змінювати;

amplification – розширення прав;

ascertain – переконуватися;

associativity – асоціативність;

asymmetric – асиметричне шифрування;

asynchronous attack – шифрування типу «асинхронна атака»;

attack – спроба розкриття (криптосистеми), крипто аналіз;

attacker – порушник, супротивник;

audit log – журнал ревізії;

autentification – 1) аутентифікація, упізнавання; 2) підтвердження права на доступ; 3) перевірка дійсності;

autentification code – код аутентифікації;

autentification of message – аутентифікація повідомлень;

autentification of user – аутентифікація користувача;

autentication problem – проблема перевірки на вірогідність;

autorization – 1) дозвіл, надання права на доступ; 2) перевірка повноважень; 3) авторизація;

autorizized access – санкціонований доступ;

autorizized user – зареєстрований користувач, привілегійований користувач;

auxiliary key – вторинний ключ;

birthday attack – криптоаналіз на основі парадокса днів народження;

block chaining – зчеплення блоків;

block encryption – блокове шифрування;

candidate key – можливий ключ;

capabilities list – список повноважень;

capability – повноваження, мандат;

capability-based addressing – адресація з урахуванням повноважень;

central keying authority (CKA) – центр розподілу (поширення, керування) ключів, ЦРК;

certification – огляд;

chained key – зчеплений блок;

challendge and response procedure – процедура запиту й підтвердження;

cheating – обман;

chinese remainder theorem – китайська теорема про залишки;

cipher I – шифр, код, шифрований образ;

cipher II – v шифрувати, кодувати;

cipherer – шифратор обладнання, що кодує;

ciphertext – шифрований текст;

classical cipher – класичний шифр;

clear text – вихідний текст;

code – код (метод перетворення відкритого тексту в криптограму шляхом використання кодових таблиць);

coincidens – збіг;

common system area (CSA) – загальна системна область захисту;

complexity – складність;

composite number – складене число;

computational complexity – обчислювальна складність;

conputer security – захист (захищеність) ЕОМ від несанкціонованого доступу;

concatenated key – див. chained key;

conceptual integrity – концептуальна цілісність;

confinement – ізоляція;

confirmation – підтвердження;

consistency – цілісність, несуперечність;

Control Program Facility (CPF) – керуюча програма;

cryptanalysis – криптоаналіз, аналіз шифру;

cryptanalyst – криптоаналітик;

cryptography – криптографія;

cryptology – криптология (криптографія + криптоаналіз);

cryptosystem – криптографічна система;

data corruption – порушення цілісності даних;

Data Encryption Standard – див. DES;

data integrity – цілісність (збереженість, дійсність) даних;

data protection – захист даних;

data security – захист інформації (даних) від несанкціонованого доступу;

data set – набір даних;

decipher – розшифровувати, декодувати;

decryption – розшифровування, декодування;

decryption key – ключ розшифровування;

denial-of-access external security – зовнішня безпека на основі позбавлення доступу;

deny – заперечувати;

detection mechanism – система виявлення;

digital signature – цифровий підпис;

direct access method (DAM) – прямій метод доступу;

divisor – дільник;

greatest common – найбільший загальний;

division of responsibilities – поділ обов'язків;

eavesdropper – пасивний порушник;

encipherer – шифратор обладнання, що кодує;

enciphering key – ключ шифрування;

encode – шифрувати, кодувати;

encoder – 1) кодер, обладнання, що кодує; 2) кодувальник, шифрувальник;

encryption – (за)шифрування;

encryption key – ключ шифрування;

endorsment – атестація;

end-to-end encryption – наскрізне шифрування;

essential undecidability – істотна нерозв'язність;

exposure – незахищеність (даних), відкритість (даних впливу третіх осіб);

external security – зовнішній захист;

extra key – додатковий ключ (пошуку);

factor – множник;

forger – фальсифікатор, підроблювач (підпису, докуме-нта й т.д.);

forgery – 1) підробка; 2) фальшивий документ; 3) під-роблений підпис;

generic key – загальний ключ; загальна частина ключа;

generic operation – типова операція;

generic system functional flaw – типовий функціональ-ний дефект;

hardware security – апаратний захист;

hash function – хэш-функція;

identify – 1) ідентифікувати, розпізнавати, пізнавати; 2) позначати, іменувати;

identity element – одиничний елемент;

implementation standard – стандарт реалізації;

inconsistency – порушення цілісності, суперечливість;

infinite random key – невизначений рандомізований ключ;

insecure chanel – незахищений канал;

insider – користувач (системи, у системі);

intended receiver – санкціонований одержувач;

integrity – цілісність, збереженість (даних);

intended receiver – санкціонований одержувач;

interface standard – стандарт взаємодії;

interlopers – порушник, зловмисник;

internal security – внутрішня безпека (захист);

interoperability – функціональна сумісність;

intruder (те ж саме attacker) – порушник, зловмисник;

invertible element – обернений елемент;

key – ключ;

key distribution center (KDC) – центр розподілу ключів, ЦРК;

key field – поле ключа;

key management – керування ключами;

key notarization – нотаризація (нотаріальне засвідчення) ключів;

key protection – захист по ключу;

key-sequenced data set – набір даних, упорядкований по ключу;

key-verify – контролювати (дані) повторним набором на клавіатурі;

knapsack cryptosystem – рюкзачна криптосистема;

legality checking – перевірка законності;

legitimate user – законний користувач;

link encryption – шифрування передач по лініях (кана-лам) зв'язку;

lost object problem – проблема втрати об'єктів;

major key – головний (первинний) ключ;

malicious – навмисний;

masquerade – маскуватися;

message replay attack – атака з повторною передачею повідомлення;

model validation – обґрунтування моделі;

multiple – кратне;

least common – найменше загальне;

multiple-key retrieval – вибірка (пошук) по декільком ключам;

nonrepudiation – не заперечення;

operating system penetration – подолання захисту ОС;

operator spoof – обман оператора;

opponents – зламщик;

pad – стрічка;

partition – розбивка;

pass key – ключ (для) доступу;

password autentication – ідентифікація по паролю;

password protection – захист паролем;

penetration entrament – пастка для зловмисників;

penetration work factor – об'єм роботи з подолання захисту;

physical security – фізичний захист;

piggyback – паразитування;

plaintext – відкритий текст, вихідний текст;

primary key – первинний (головний) ключ;

primality theorem – тест на простоту;

privacy – таємність, конфіденційність;

privacy problem – проблема збереження таємниці;

private key – секретний ключ;
private key encryption – шифрування по закритих ключах у криптосистемах із відкритими ключами;
privilege violation – порушення повноважень;
problem of dispute – проблема підтвердження відправника;
protection against disasters – захист від випадкових ситуацій;
protection against intruders – захист від зловмисників;
protection domain – область захисту;
protection key – ключ захисту (пам'яті);
proxy protocols – протоколи за дорученням;
private – секретний;
private exponent – секретний показник ступеня;
public key – відкритий ключ;
public key encryption – шифрування з відкритими ключами;
public – відкритий;
public exponent – відкритий показник ступеня;
public key system – криптосистема з відкритим ключем;
quotient set – фактор-множина;
recursive formula – рекурентна формула;
recursive unsolvability – рекурсивна нерозв'язність;
redundance – надлишок;
relation – відношення;
remainder – остача;
repudiate – відрікатися;
residue – відрахування;
restrict – обмежувати;
revocation of capability – скасування повноважень;
risk management – керування ризиком;
running key – ключовий потік;
running key generator – генератор ключового потоку;
satisfiability – здатність до виконання (вимог);
secondary key – вторинний ключ;
secrecy – таємність;
secure data storage – надійне зберігання даних;
security – безпека, захист, захищеність, стійкість;
security auditing – перевірка захисту, перевірка на стійкість;

security requirement – вимога по безпеці;
security standard – стандарт по захисту;
sensitive – конфіденційний;
shuffle – тасувати;
sign I – ознака; позначення; знак числа; завірення (документа або даних);
sign II – підписуватися; завіряти;
signature – сигнатура, підпис;
sound protocol – надійний протокол;
space object – об'єкт пам'яті;
storage – зберігання;
storage key – 1) ключ зберігання; 2) ключ захисту пам'яті;
storage protection – захист пам'яті;
stream encryption – потокове шифрування;
strong cryptoalgoritm – стійкий крипто алгоритм;
substitution cipher – шифр постановки;
surveilance – нагляд (за роботою системи), ревізія, ідентифікація;
surveilance program – програми контролю;
survivable system – живуча система;
symmetric encryption – симетричне шифрування;
system pointer – системний вказівник (посилання);
threat monitoring – моніторинг потоків;
transparent multiprocessing – прозора мультипроцесорна обробка;
transposition cipher – перестановочний шифр;
trap – пастка, таємний хід;
trap door – лазівка;
trapping – організація пасток (у системі);
undecipherable – той, що не піддається дешифруванню;
unauthorized – 1) несанкціонований; 2) непривілегійований;
unauthorized access – несанкціонований доступ;
uncertainty – невизначеність;
undecidability – нерозв'язність;
unsolvability – нерозв'язність;
user-defined key – ключ користувача;

user interface security – безпека інтерфейсу користувача;

user requirement – вимога користувача (ті, що установленні користувачем);

user identification – див. авторизація;

validation – перевірка правильності;

verify – перевіряти;

vital – істотний;

vulnerable – уразливий;

weak cryptoalgoritm – нестійкий криптоалгоритм;

Дуже зручний словник термінів з поясненням змісту кожного терміна за редакцією Погорєлова Б. А.

СПИСОК ЛІТЕРАТУРИ

1. Коробейников А. Г. Математичні основи криптографії. Навчальний посібник. С. Пб: ГИТМО (ТУ), 2002. - 41 с.
2. Саломаа С. Криптографія з відкритим ключем. - Мир, 1995. - 318 с.
3. R. L. Rivest, A. Shamir, L. Adleman, «A method for obtaining digital signatures and public-key cryptosystems», Comm. ACM, 21(1978) pp 120-126.
4. Diffie W., Hellman M. E. «New Directions in Cryptography», IEEE Transactions on Information Theory, v.IT-22, n.6, November 1976, pp. 644-654.5.
5. Merkle R. C. «Secure Communication Over Insecure Channels», Communications of the ACM, v.21, n.4, 1978, pp.294-299.6.
6. Simmons G. I. "Cryptology", Encyclopedia Britannica, 16th edition, 1986, pp.913-924C.
7. Анохін М. А., Варновский Н. П., Сидельников В. М., Ященко В. В. Криптографія в банківській справі, МИФИ, 1997.
8. Дориченко С. А., Ященко В. В. 25 етюдів про шиф-ри. - М.: "Теис", 1994.
9. Rivest R. L., Shamir A., Adleman L. M. «A Method for Obtaining Digital Signature and Public-Key Cryptosystems», Communications of the ACM, 21(2), February 1978, pp.120-126.
10. Feige U., Fiat A., Shamir A. «Zero-Knowledge Proofs of Identity», Journal of Cryptography, 1, 1988, pp.66-94.
11. Elgamal T. «A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms», IEEE Transactions on Information Theory, IT-31, 1985, pp.469-472.
12. Merkle R. C., Hellman M. E. «Hiding Information and Signatures in Trapdoor Knapsacks», IEEE Transactions on Information Theory, IT-24, 1978, pp.525-530.
13. Нестеренко Ю. В. Алгоритмічні проблеми теорії чисел // Математична освіта – 1997. – с. 3, В. 2.
14. Pollard J. M. «Theorems on Factorization and Primality Testing», Proc. Cambridge Philos. Soc., 76, 1974.

15. Shamira. «A Polynomial Time Algorithm for Breaking the Basis Merkle-Hellman Cryptosystem», IEEE Transactions on Information Theory, v.IT-30(5), September 1984, pp.699-704.
16. Brickell E.F. «Breaking Iterated Knapsacks», in Advances in Cryptology- CRYPTO'84, Springer-Verlag, 1985, pp.342-358.
17. Березін Б.В., Дорошкевич П. В., Цифровий підпис на основі традиційної криптографії // Захист інформації. - Москва, 1992, №2. - С. 148-167.
18. Schneier Bruce, «Applied Cryptography, Second Edition» (Protocols, Algorithms and Source Code in C), John Wiley & Sons, Inc., 1996. (Є переклад на російську мову)
19. Жельніков В. Криптографія від папіруса до комп’ютера — М.: ABF, 1996. — 335 с.
20. Петров А. А. Комп'ютерна безпека. - М.: ДМК, 2000.

Навчальне видання

Математичні основи криптографії

Конспект лекцій

для студентів спеціальностей

7.080202 „Прикладна математика”,

денної форми навчання

Відповідальний за випуск зав. кафедри прикладної та обчислювальної математики д-р. фіз.-мат. наук, проф. Л. А. Фильштинський
Редактор Н. М. Мажуга
Комп’ютерне верстання Г. О. Кладієнко

Підписано до друку 15.02.2010, поз.
Формат 60×84/16. Ум. друк. арк. 12,10. Обл.-вид. арк. 9,96. Тираж 150 пр. Зам. №
Собівартість видання грн к.

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб’єкта видавничої справи ДК № 3062 від 17.12.2007.