Тема 1. ОСНОВНІ ПОНЯТТЯ КРИПТОЛОГІЇ

Несанкціонований доступ до інформації — доступ до інформації з порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

1. Загроза інформації та можливості прихованої її передачі.

Основні ознаки інформації, що має бути захищеною:

- ✓ наявність певного кола законних власників, що мають право користуватись цією інформацією;
- ✓ наявність зловмисників, що прагнуть оволодіти цією інформацією з корисливою метою для себе та на шкоду законним власникам.

Мета, яку прагнуть досягти зловмисники, називається загрозою. Основні види загроз такі:

- ✓ загроза розголошення конфіденційної (секретної) інформації;
- ✓ загроза цілісності (автентичності, істинності) інформації;
- ✓ загроза достовірності адресних ознак інформації.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Інформація, що є державною власністю, теж вважається конфіденційною.

Цілісність інформації – це відсутність спотворених, замінених або знищених інформаційних елементів.

Достовірність адресних ознак інформації означає відсутність фальсифікації її відправника або отримувача. Це виключає можливість відмовитись від фактів передачі або отримання інформації, якщо вона дійсно передавалась або отримувалась, а також можливість підтвердити передачу або отримання інформації, якщо вона насправді не передавалась і не отримувалась.

Щоб захиститись від загроз, можна скористуватись однієї з трьох можливостей передачі прихованої інформації:

- ✓ використання абсолютно надійного, недоступного для інших каналу зв'язку між абонентами; ця можливість вважається практично нереальною, оскільки, на сучасному рівні науки і техніки неможливо створити такий канал між віддаленими абонентами для неодноразової передачі великих обсягів інформації;
- ✓ використання загальнодоступного каналу зв'язку, але при цьому приховується сам факт передачі інформації; розробкою відповідних методів та засобів займається стенографія;
- ✓ використання загальнодоступного каналу зв'язку, але при цьому до інформації, що передається, застосовується таке перетворення, що зрозуміти її може тільки адресат; розробкою відповідних методів та способів перетворення інформації займається криптології. [8]

2. Основні поняття стеганографії.

Перші застосування стеганографічних методів відомі з глибокої давнини. Наприклад, відомий такий спосіб приховування письмового повідомлення: голову раба голили, на шкірі голови писали повідомлення, чекали, поки волосся виросте, і лише тоді раба відправляли до адресата.

Відомі методи тайнопису між рядків звичайного тексту молоком або спеціальними реактивами з наступною хімічною обробкою.

Відомий метод "мікроточки", коли повідомлення за допомогою сучасної техніки записується на дуже маленький носій (мікроточку), який пересилається звичайним поштовим листом, наприклад, під маркою.

Сучасні комп'ютерні технології викликали появу комп'ютерної стеганографії. Методами комп'ютерної стеганографії здійснюється приховування повідомлень у звичайних файлах. Їх називають контейнерами.

Порожній файл-контейнер містить тільки звичайну інформацію і не містить прихованої конфіденційної інформації. Контейнер заповнюють у відповідності з ключем, який визначає порядок занесення повідомлення у

контейнер, а також його здобування із нього. Ключ може розміщуватись у контейнері разом із повідомленням або передаватись окремо.

Основні вимоги до стеганографічних методів:

- ✓ метод повинен забезпечувати збереження основних властивостей контейнера після внесення в нього конфіденційного повідомлення та ключа (розмір, дата і час створення, зовнішній вигляд даних);
- ✓ якщо про наявність прихованого повідомлення зловмиснику стало відомо, то здобування його повинно являти собою складну обчислювальну задачу.

Основна задача будь-якого стеганографічного методу – шляхом передачі ззовні звичайної інформації приховати сам факт передачі конфіденційної інформації. Засобами стеганографії можна розв’язати також додаткові спеціальні задачі:

- ✓ камуфлювання програмного забезпечення, коли його використання незареєстрованими користувачами є небажаним; наприклад, воно може бути закамуфльовано під стандартне програмне забезпечення (наприклад, текстовий редактор) або під файли мультимедіа (наприклад, під звукове супроводження комп’ютерних іграшок);
- ✓ захист авторських прав; при цьому у файл, який авторизується, вноситься спеціальна позначка, яка залишається невидимою для ока, але розпізнається спеціальним програмним забезпеченням.
- ✓ Методи комп’ютерної стеганографії розвиваються за двома основними напрямками:
- ✓ методи, що базуються на використанні властивостей комп’ютерних форматів;
- ✓ методи, що базуються на природній надмірності аудіо- та відеоінформації.

У свою чергу методи, що базуються на використанні властивостей комп’ютерних форматів є такі:

- ✓ комп’ютерні мультимедійні формати мають резервні поля. Звичайно вони заповнюються нульовими даними і не враховуються програмою;

- ✓ врахування особливостей форматування текстових файлів. Наприклад, у текст можуть бути внесені додаткові пропуски між словами, можуть бути змінені положення рядків, розміщення слів у реченнях, параметри абзаців, тощо;
- ✓ використання прихованих полів, не відображуваних на екрані. Наприклад, використання кольору шрифту, що співпадає з кольором фону;
- ✓ приховування даних у не використовуваних місцях дисків., наприклад, в нульовій доріжці;
- ✓ використання імітації, яка базується на побудові спеціального змістовного тексту, що приховує в собі повідомлення. При цьому, наприклад, для знаків повідомлення можуть вибиратися певні позиції. Окремий випадок цього методу – акростих, наприклад:

У червоному намисті
Коло річки в зелен-листі
Розпишалася калина,
А із нею й тополина.
Їде візник, тихо стане,
На калину ніжно гляне,
А в уяві щось постане.

Методи, що базуються на природній надмірності аудіо- та відеоінформації, використовують надмірність цифрових фотографій, цифрового звуку та цифрового відео. Відомо, що молодші розряди цифрових відліків містять мало корисної інформації. Їх заміна іншою інформацією практично не впливає на якість відтворення.

В літературі наведено такі приклади з використанням указаної надмірності.

Приклад 1. Одна секунда цифрованого звучання з частотою дискретизації 44100 Гц та з рівнем відліку 8 біт у стерео режимі дозволяє приховати близько 10 Кбайт за рахунок заміни молодших розрядів звукових даних розрядами повідомлення. При цьому зміна значень відліків складає менше 1%. Це практично не виявляється при прослуховуванні файлу більшістю людей.

Приклад 2. Графічні кольорові файли за схемою RGB кодують кожну точку трьома байтами. Зміна кожного із трьох молодших бітів приводить до

зміни яскравості точки менш як на 1%. Це дозволяє приховувати у стандартному графічному малюнку обсягом 800 Кбайт близько 100 Кбайт повідомлення. При звичайному перегляді зображення це не помітно. [8]

3. Предмет криптологія

Криптологія – наука, що складається з двох напрямків: криптографії та криптоаналізу.

Криптографія – наука, що займається розробкою шифрів. При цьому, шифром називається такий метод або спосіб перетворення повідомлень, який забезпечує захист інформації в них від зловмисників.

Криптоаналіз – це наука про методи та способи розкриття зашифрованих повідомлень, а також про тактику та стратегію їх застосування. Внаслідок застосування криптоаналізу можливо також фальсифікувати або саме повідомлення, або його адресні ознаки (наприклад, видати підроблене повідомлення за істинне).

Шифруванням називається процес застосування шифру до повідомлення, що має бути захищеним. Внаслідок шифрування відкритий текст перетворюється у шифроване повідомлення (криптограму).

Дешифрування – процес, обернений шифруванню, який теж здійснюється за відомими правилами шифру.

Сучасна термінологія не вважає синонімами терміни “кодування” та “шифрування”. Це пояснюється тим, що термін “кодування” охоплює ті методи та способи перетворення повідомлень, які розглядаються в рамках наукового напрямку теорії інформації та кодування. Вказані методи та способи перетворення повідомлень вирішують інші задачі (наприклад, пов’язані із стисненням даних або захистом даних від випадкових спотворень у каналах зв’язку).

Особу, яка вирішує задачу перехвату повідомлень та розкриття зашифрованих повідомлень за допомогою методів криптоаналізу, називають *противником*. Розкриття зашифрованих повідомлень називають *зламуванням шифру*. Окрему спробу зламування шифру називають *атакою на шифр.*

Крім зламування шифру противник може робити спроби отримати інформацію, що захищається, іншими способами. Найбільш відомий з них – агентурний. При цьому противник певним способом схиляє до співпраці одного із законних власників, і за допомогою цього агента отримує доступ до потрібної інформації. В таких випадках криптографія безсила. [8]

4. Основні принципи криптології

Принцип рівної міцності захисту. На шляху від одного законного власника до іншого інформація може захищатись різними способами в залежності від загроз, що виникають. Так утворюється ланцюг захисту інформації з ланками різного типу. Противник прагне знайти найслабкішу ланку, щоб з найменшими витратами добратися до інформації. Законні власники повинні враховувати це в своїй стратегії захисту інформації криптографічними методами: безглуздо робити якусь ланку дуже міцною, якщо є слабкіші ланки.

Принцип доцільності захисту. На сучасному рівні технічного розвитку засоби зв'язку, засоби перехоплення повідомлень, а також засоби захисту інформації вимагають занадто багато витрат. Тому існує проблема співвідношення вартості інформації, витрат на її захист та витрат на її здобування. Перш ніж захищати інформацію криптографічними методами, треба вирішити два питання:

1) Чи отримає противник внаслідок атаки інформацію, що буде більш цінною, ніж вартість самої атаки?
2) Чи є інформація, яку захищає її власник, більш цінною, ніж вартість захисту?

Відповідь на ці два питання визначає доцільність захисту та вибір підходящих засобів криптографічного захисту.

Принцип використання ключа. Розробка хорошого шифру – справа надзвичайно трудомістка. Тому бажано збільшити термін цього шифру і використовувати його для шифрування якнайбільшої кількості повідомлень. Але при цьому виникає небезпека, що противник вже зламав шифр і вільно

читає шифровані повідомлення. Саме тому в сучасних шифрах використовують ключі.

Ключем в криптографії називають змінюваний елемент шифру, який застосовується до шифрування конкретного повідомлення. При цьому вважають, що сам шифр (крім ключа) є відомим противнику і доступним для вивчення. Оригінальність подання повідомлення забезпечується тільки періодично змінюваним ключем. Знання ключа дозволяє швидко та просто відновити початковий текст. Без знання ключа дешифрування тексту має бути практично недосяжним.

Принцип стійкості шифру. Здатність шифру протидіяти різноманітним атакам на нього називається *стійкістю шифру.* З математичної точки зору проблема отримання строго доведених оцінок стійкості для будь-якого шифру ще не вирішена. Ця проблема відноситься до проблем нижніх оцінок обчислювальної складності задачі, ще нерозв'язаних математично. Тому стійкість конкретного шифру оцінюється шляхом різноманітних спроб його зламування, а отримані результати оцінюють в залежності від кваліфікації криптоаналітиків, що атакують цей шифр. Таку процедуру називають *перевіркою стійкості.*

Принцип Керкхоффа. Стійкість сучасного шифру має визначатися, в першу чергу, ключем. Зміст цього принципу полягає в тому, що захищеність інформації не повинна залежати від таких факторів, які важко змінити при появі загрози. При використанні ключів законним власникам інформації легше перешкоджати противнику, оскільки міняти їх можна досить часто. Але, тепер законним власникам виникає інша задача – як таємно обмінятись ключами перед тим, як обмінюватися шифрованими повідомленнями.

Принцип використання різноманітних шифрів. Не існує єдиного шифру, що підходить до всіх випадків. Вибір шифру залежить від особливостей інформації (може мати різний характер, тобто бути документальною, телефонною, телевізійною, комп'ютерною тощо), від цінності інформації, від обсягів інформації, від потрібної швидкості її передачі, від тривалості захисту (державні та військові таємниці зберігаються десятками років, біржеві –

декілька годин), від можливостей противника (можна протидіяти окремій особі, можна протидіяти потужній державній структурі), а також від можливостей власників із захисту своєї інформації. [8]

5. Класифікація шифрів

До основних характеристик сучасних методів шифрування можна віднести:

- ✓ довжину ключа;
- ✓ складність алгоритму перетворення даних;
- ✓ розмір даних, що обробляються;
- ✓ спосіб роботи з ключами і т. д.

Існують різні підходи до класифікації шифрів:

- ✓ за методом шифрування – шифри заміни та шифри перестановки;
- ✓ за технологією шифрування – блокові шифри та потокові шифри;
- ✓ за особливостями ключів – симетричні шифри та асиметричні.

У своїй роботі “Теорія зв’язку у відкритих системах” (1949) Клод Шеннон розглядав класифікацію шифрів за методом шифрування.

Шифр *заміни* здійснює перетворення, при якому літери або якісь інші фрагменти відкритого тексту замінюються відповідними фрагментами шифрованого тексту.

Шифр *перестановки* здійснює перетворення, при якому літери або якісь інші фрагменти переставляються місцями безпосередньо у відкритому тексті.

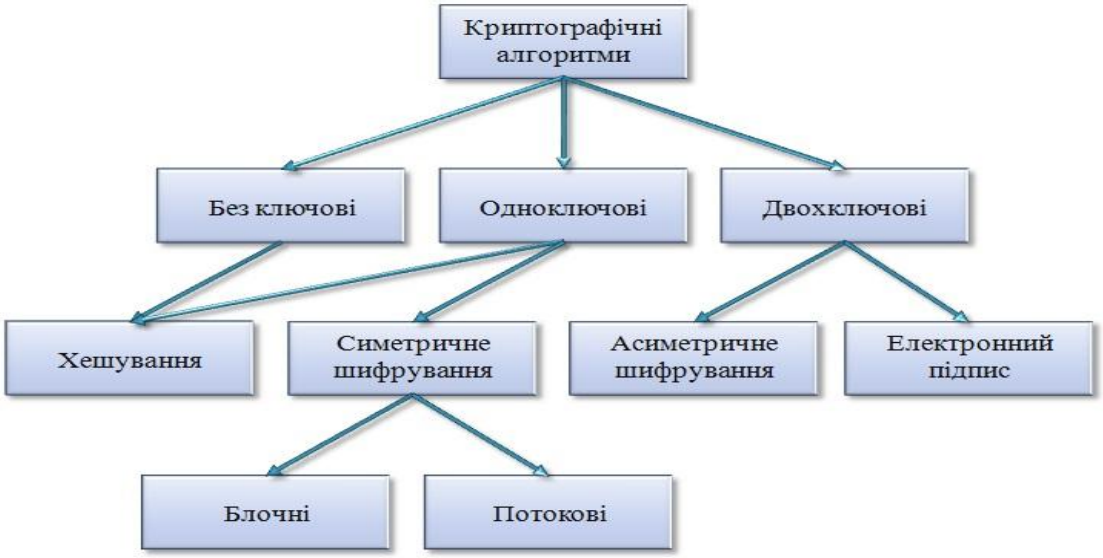
В *блокових* шифрах метод шифрування застосовують до блоку відкритого тексту, який має певні розміри (кількість знаків). В *потокових* шифрах метод шифрування застосовують до кожного знаку відкритого тексту окремо.

Якщо один і той же алгоритм, а також один і той же ключ використовується і для шифрування, і для дешифрування повідомлень, то такий метод шифрування називається *симетричним*. Зрозуміло, що цей єдиний ключ має бути секретним і відомим тільки відправнику та отримувачу повідомлення. Тому ці методи також називаються одно ключовими шифрами або *шифрами з секретним ключем*. Для симетричних шифрів є характерною нерозв’язувана

проблема, яка полягає в ускладненнях з передачею абоненту секретного ключа, а також в неможливості переконатись в аутентичності отриманого абонентом ключа.

Якщо алгоритми шифрування та дешифрування різні, і якщо використовуються два ключі – один для шифрування, а другий – для дешифрування повідомлення, то такий метод шифрування називається *асиметричним***.** Один з цих ключів є секретним, інший – відкритим. Тому асиметричні методи шифрування називаються двохключовими шифрами або шифрами з відкритим ключем.

В загальному всі криптографічні алгоритми поділяються так як на малюнку:



Ефективність використання симетричних шифрів визначається високою швидкодією при обробці великих обсягів інформації.

Ефективність використання асиметричних шифрів визначається відсутністю необхідності пересилання секретних ключів.

Вся сукупність засобів (шифри, ключі, програмно-апаратні засоби), яка забезпечує криптографічний захист інформації від загроз противника, називається *криптографічною системою.* Особливістю криптографічної системи є те, що два учасники секретного зв’язку повністю довіряють один одному.

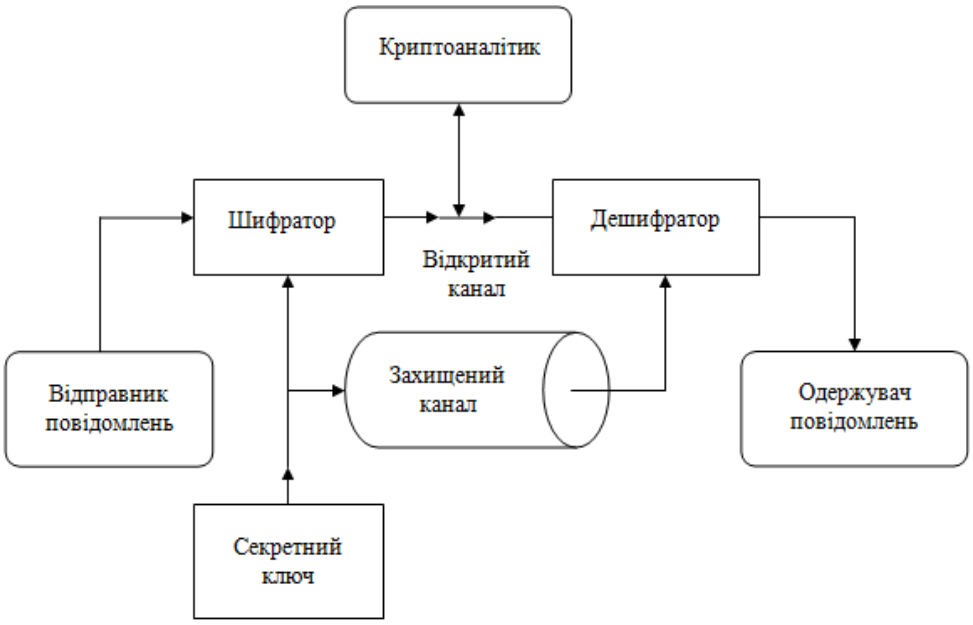


Рис. 1.1 Схема криптосистеми з таємним ключем (симетрична)

Криптосистема з рисунка може діяти у 2-х варіантах:

1) повна система, тобто в якій і відправник і одержувач можуть переходити з однієї ролі в іншу, при цьому система шифрування та дешифрування повинні бути і у відправника і у одержувача;
2) криптосистема односторонньої дії, у якій відправник може тільки відправляти, а одержувач тільки приймати з відповідними засобами шифрування і дешифрування у кожної з сторін.

6. Поняття абсолютно стійкого шифру

Одним з найважливіших результатів Клода Шеннона був висновок про існування та єдність абсолютно стійкого шифру. Абсолютно стійкий шифр має три ознаки:

- ✓ одноразовість використання;
- ✓ повна випадковість ключа;
- ✓ рівність довжин відкритого тексту та ключа або ключ більший від тексту.

У разі відсутності хоча б однієї з цих ознак шифр втрачає властивість абсолютної стійкості і з’являються принципові умови його зламування (хоча їх, можливо, буде важко реалізувати).

Теоретично противник з необмеженими ресурсами може зламати будь-який неабсолютно стійкий шифр.

Приклад. У 1999 році автор твору “Книга коду” Саймон Сінгх запропонував 25 тис. доларів тому, хто зможе зламати неабсолютно стійкий шифр, найскладніший за всю історію криптографії. Саймон Сінгх, доктор фізичних наук Кембріджського університету, разом з доктором Полом Лейландом, що працює в Кембріджі на компанію Microsoft, на протязі двох років в умовах повної секретності створили 10 криптограм зі зростаючою складністю. Але всього через рік, восени 2000 року, команда шведських комп’ютерщиків, очолюваних фахівцем із захисту інформації Фредриком Алмгреном, зламали всі 10 шифрів. Вони випередили конкурентів з усього світу і отримали винагороду. На це їм знадобилося 70 років комп’ютерного часу.

Указані ознаки роблять абсолютно стійкий шифр занадто дорогим. Тут виникають проблеми, пов’язані із значним збільшенням обсягу шифрованих даних (повідомлення плюс ключі), із забезпеченням всіх абонентів достатнім запасом секретних випадкових ключів, а також із виключенням їх повторного застосування (при кількості абонентів, більшій двох).

З цих причин абсолютно стійкі шифри застосовують тільки у випадках передачі невеликих обсягів особливо важливої державної інформації. Звичайні користувачі вимушені застосовувати неабсолютно стійкі шифри.

Прикладом реалізації абсолютно стійкого шифру є шифр Вернама. Цей шифр здійснює побітове додавання (по модулю 2) n-бітового відкритого тексту та n-бітового ключа: $y_i = x_i \oplus k_i$, $i=1, \ldots n$. Тут $x_1, x_2, \ldots, x_n$ – відкритий текст, $k_1, k_2, \ldots, k_n$ – ключ, $y_1, y_2, \ldots, y_n$ – криптограма. Різновид шифру Вернама для десяткових чисел в наш час знаходить застосування у системах військового зв’язку у вигляді, так званих, шифрувальних блокнотів.