МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Методичні вказівки

до виконання лабораторних робіт з дисципліні «Основи криптології »

для студентів напряму підготовки

«Комп'ютерні науки »

**Лабораторна робота № 1   
Режими шифрування блокових шифрів. Мережа Фейстеля.**

|  |  |
| --- | --- |
| Мета лабораторної роботи: | 1. Ознайомитись з основними операціями, що застосовуються у блокових шифрах. 2. Ознайомитись з режимами шифрування блокових алгоритмів шифрування. 3. Ознайомитись блоковими шифрами, заснованих на структурі мережі Фейстеля. 4. Ознайомитись з алгоритмом шифрування DES . 5. Виконати програмну реалізацію та чисельний експеримент з алгоритмом шифрування DES . |
| Час для виконання: | 4 академічні години. |

**Зміст роботи.**

**I. Теоретичні відомості.**

Введення в блокові шифри

Блоковий алгоритм перетворює n-бітний блок незашифрованого тексту на n-бітний блок зашифрованого тексту. Число блоків довжини n дорівнює 2 n . Щоб перетворення було оборотним, кожен із таких блоків повинен перетворюватися на свій унікальний блок зашифрованого тексту. При невеликій довжині блоку така підстановка погано приховує статистичні особливості незашифрованого тексту. Якщо блок має довжину 64 біта, він вже добре приховує статистичні особливості вихідного тексту. Але в даному випадку перетворення тексту не може бути довільним через те, що ключем буде саме перетворення, що виключає ефективну як програмну, так і апаратну реалізації.

У блокових шифрах зазвичай блок тексту сприймається як неотрицательное ціле число, чи кілька незалежних неотрицательных цілих чисел. Довжина блоку завжди вибирається рівною мірою двійки. У більшості блокових алгоритмів симетричного шифрування використовуються такі типи операцій:

* Таблична підстановка, коли група бітів відображається в іншу групу бітів. Це звані S-блоки.
* Переміщення, за допомогою якого перезапорядковуються біти повідомлення.
* Операція додавання за модулем 2, що позначається XOR або .
* Операція додавання за модулем 2 32 або модулем 2 16 .
* Циклічний зсув на кілька бітів.

Ці операції циклічно повторюються алгоритмі, утворюючи звані раунди. Вхід кожного раунду є вихід попереднього раунду і ключ, який отриманий за певним алгоритмом з ключа шифрування K. Ключ раунду називається підключом. Кожен алгоритм шифрування може бути представлений так, як показано на рис.

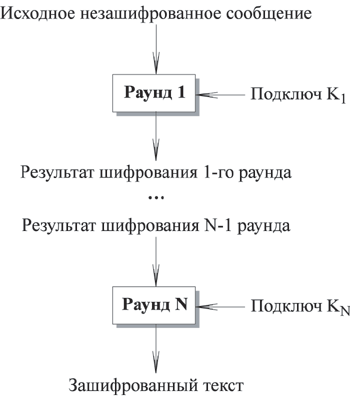


Рис.1

**ІІІ. Завдання**

**Завдання 1.**

Виконати програмну реалізацію алгоритму DES для шифрування та розшифрування тестового файлу.

**Завдання 2**

# Виконати чисельний експеримент. Число дати свого народження перевести в двійковий код, використовуючи спрощений алгоритм шифрування DES (S-DES)

**IV. Звіт**

Має містити програмну реалізацію з коментарями, результат виконання чисельного експерименту з вихідними та отриманими значеннями, процес обчислень при "ручній" перевірці вихідних даних.

# Лабораторна робота № 2 Підстановочно-перестановні мережі. Системи типу "квадрат". Алгоритм шифрування Rijndael (стандарт AES)

|  |  |
| --- | --- |
| Мета лабораторної роботи: | 1. Ознайомитись блоковими шифрами, заснованих на структурі SP-мереж та структури типу Square. 2. Ознайомитись з алгоритмом шифрування Rijndael. 3. Виконати програмну реалізацію та чисельний експеримент із алгоритмом шифрування Rijndael. |
| Час для виконання: | 4 академічні години. |

**Зміст роботи.**

**I. Теоретичні відомості. Алгоритм Rijndael**

Американський стандарт шифрування AES є підмножиною алгоритму Rijndael з довжиною ключа 128 біт. Сам стандарт був прийнятий урядом США у вигляді FIPS у вигляді документа FIPS-197 (його ЛЮБИЦЬКИЙ переклад можна прочитати тут). Однак, ці документи, як і будь-які інші стандарти, містять формальний опис алгоритму, який мало придатний для навчання та розуміння роботи алгоритму непідготовленими користувачами.

Досить докладний опис алгоритму Rijndael в академічному стилі представлено у лекції 4

Однак, для розуміння процесу реалізації алгоритму непогано уявляти собі процес його роботи загалом. Допомогти цьому може анімаційний ролик, який демонструє роботу Rijndael. Даний ролик (Flash) було створено на факультеті інформаційних технологій Бостонського коледжу (якому належать права на нього). Ролик можна знайти в 1 розділі цієї дисципліни в Moodle .

**ІІ. Завдання**

**Завдання 1.**

Виконати програмну реалізацію алгоритму Rijndael із зазначеною довжиною блоку та ключа згідно з варіантом.

Варіанти завдання:

|  |  |  |
| --- | --- | --- |
|  | Довжина блоку | Довжина ключа |
| 1 | 128 | 128 |
| 2 | 128 | 192 |
| 3 | 128 | 256 |
| 4 | 192 | 128 |
| 5 | 192 | 192 |
| 6 | 192 | 256 |
| 7 | 256 | 128 |
| 8 | 256 | 192 |
| 9 | 256 | 256 |
| 10 | 128 | 128 |
| 11 | 128 | 192 |
| 12 | 128 | 256 |
| 13 | 192 | 128 |
| 14 | 192 | 192 |
| 15 | 192 | 256 |
| 16 | 256 | 128 |
| 17 | 256 | 192 |
| 18 | 256 | 256 |

**Завдання 2**

Виконати чисельний експеримент.

**Завдання 3**

Використовуючи виконану у Завданні 1 реалізацію алгоритму шифрування Rijndael, виконати програмну реалізацію утиліти шифрування/дешифрування файлу за допомогою Rijndael. Ключ та вихідний текст знаходяться у зовнішніх файлах. Імена файлів та назва операції (шифрування, дешифрування) задаються як параметри програми у командному рядку.

**IV. Звіт**

Має містити програмну реалізацію з коментарями, результат виконання чисельного експерименту з вихідними та отриманими значеннями, процес обчислень при "ручній" перевірці вихідних даних.

**Лабораторна робота №3   
Системи шифрування з відкритим ключем . RSA**

|  |  |
| --- | --- |
| ***Мета лабораторної роботи :*** | **1) Ознайомитись із системами шифрування з відкритим ключем на прикладі RSA .  2 ) Провести дослідницький експеримент з використанням алгоритму RSA .** |
| ***Час для виконання:*** | **4 академічні години.** |

**I. Теоретичні відомості** :

 Опис алгоритму \_ RSA можна знайти в лекції 2 розділу цієї дисципліни системи Moodle .

**ІІ. Завдання \_**

**1.       Виконати програмну реалізацію алгоритму RSA . При цьому вважати, що всі змінні та структури даних, що використовуються в програмі для зберігання числових даних, поміщаються в розрядну сітку стандартних типів даних ЕОМ (У С++ рекомендується використовувати long long). Звичайно, що така реалізація не може претендувати на практичне використання в реальних системах (у зв'язку з недостатньою розрядністю обчислень), проте дозволяє зрозуміти роботу самого алгоритму.**

**2.       Провести обчислювальний експеримент - як тестовий приклад простих чисел p і q взяти прості числа розрядністю від 100000000 до 1000000000000. Генерувати відкритий і закритий ключі. Зашифрувати за допомогою відкритого та розшифрувати за допомогою закритого ключа повідомлення, що є конкатенацією Вашого прізвища, імені та по батькові, кожен символ яких представлений у вигляді кодів ASCII (866 кодова сторінка, тобто кодування DOS ) .**

**Лабораторна робота №5**

**Теоретичні відомості:**

**Алгоритм формування схеми Ель-Гамалю**

1. Вибираємо просте число p.

2. Вибираємо два випадкові числа

g<p та x<p.

3. Обчислюємо

y≡g x modp.

Відкритим ключем схеми Ель-Гамалю є числа y, g і p. Закритим ключем – число x.

**Алгоритм формування цифрового підпису**

1. Дано повідомлення M, яке треба підписати.

2. Вибираємо випадкове число

k< p

взаємно просте з p-1

3. Обчислюємо

a≡g k modp.

4. З рівняння

M = (xa + kb) mod (p-1)

визначаємо

b = (M-xa) k -1 mod (p-1)

5. Формуємо підпис. Підписом є пара чисел (a, b). Число k є секретним ключем.

**Зауваження.**

Під час формування цифрового підпису на кроці 4 замість значення M можна використовувати значення μ= H(M) , де H– деяка хеш-функція.

**Перевірка підпису**

1. Дано повідомлення M та підпис ( a , b ).

2. Обчислюємо

y a a b modp≡

≡ [g x ] a a b ≡g xa g kb ≡

≡g xa +kb ≡g M modp .

3. Обчислюємо g M modp.

4. Якщо значення y a a b modp збіглося з g M modp, то підпис є вірним.

**Завдання:**

1. Розробте програмну реалізацію алгоритму обміну ключами ( алгоритму Деффі-Хеллмана ). Ключі повинні автоматично формуватися у файли . Повинна бути забезпечена наочність виконання алгоритму . Для створеного програмного забезпечення проведіть тестування не менше ніж на 10 різних наборах даних .
2. Реалізувати ЕЦП на базі алгоритму Ель-Гамалю . Підготувати звіт , до якого включити алгоритм формування системи Ель-Гамаля , опис функцій з яких складається програма . Підготувати для демонстрації контрольний приклад. При формуванні цифровий підписи передбачити схему ЕЦП із використанням хеш-функцій .
3. Провести обчислювальний експеримент , що демонструє роботу алгоритму Ель-Гамалю . Зашифрувати за допомогою відкритого та розшифрувати за допомогою закритого ключа повідомлення \_ \_ собою конкатенацію Вашою прізвища , імені та по батькові , кожен символ яких представлений у вигляді кодів ASCII (866 кодова) сторінка , тобто . кодування DOS ).