Системи безпеки програм і даних

Контрольна робота №2

Жилінков Іван ІК-91

ABCD – цифри заліковки відсортовані за зростанням. A<=B<=C<=D.

Залікова книжка No9222 A = 2; B = 2; C = 2; D = 9.

1. Принцип Керкгоффза. Шифр Вернама. Переваги і недоліки. Дайте визначення своїми словами.

Принцип Керкгоффса *– правило розробки систем шифрування.*

Основний принцип даного правила, залишати в секретності лише ключ шифрування, коли алгоритм роботи системи може бути розсекреченим та доступним. Це робить систему простою та гнучкою одночасно безпечною, оскільки можна легко змінювати ключі і не хвилюватись про розкритість алгоритму шифрування.

Недоліки :

- *До ключа окрім секретності ставиться ше 6 вимог (*лаконічність, динамічність, простота для запамятовування для використання у телеграмі).*
- *Обмеження в довжині ключа, оскільки великий ключ перенавантажує систему передачі інформації*

Шифр Вернама *– система симетричного шифрування. Це єдина система з абсолютною криптографічною стійкістю, яку забезпечує шифрування за допомогою XOR операції з ключем. Таким чином ключ має таку ж довжину як і вихідне повідомлення, але складається з випадкових символів.*

Недоліки :

- *Для великих даних, громізткість ключа через особливості алгоритму*
- *Генерація одноразового ключа для кожного повідомлення*
- *Кожен ключ складається з послідовності бітів, в якій кожен біт залежить від попереднього. А це обмежує вибір ключ для шифрування*
- *Складність конфіденційної передачі ключа для обох сторін шифрування, та викоанння усіх умовах алгоритму в реальних умовах*

2. ***Синтез відмовостійкої топології. Синтезуйте топологію на основі зсувів – кодових перетворень (граф Де Бруйна).***

- *Кількість вузлів 10-16. Коди вузлів в системі зчислення з основою B+1.*
- *Побудуйте маршрут (на основі зсувів) від узла A до вузла з номером (16-B) через вузол (A+B+C+D)mod6. Знайдіть альтернативні маршрути в умовах відмови одного з проміжних вузлів.*
- *Розрахуйте показники топології:*
  - *діаметр системи (D);*
  - *середній діаметр системи (Ds);*
  - *ступінь системи (S);*
  - *кількість ребер системи (R);*

Коди вузлів в системі зчислення з основою B+1 = 2+1 = 3.

Побудуйте маршрут (на основі зсувів) від узла A=2 до вузла з номером (16-B = 16-2 = 14) через вузол (A+B+C+D=2+2+2+9=15)mod6 = 15mod6 = 3.

В результаті маємо таку топологію:

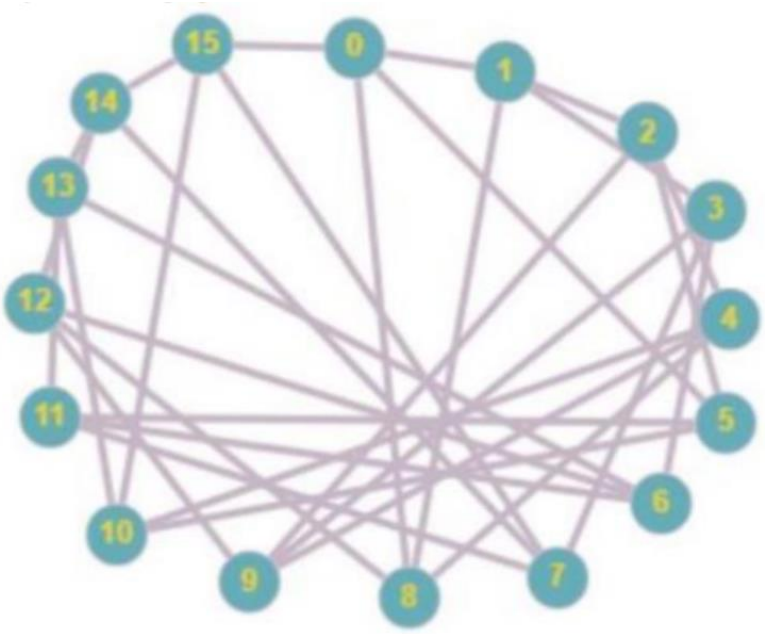
- *14 вузлів*
- *Система числення – 3*
- *Потрібно побудувати маршрут: 2 => 3 =>14*

Топологія

0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**
0000	0010	0010	1001	1000	1010	1100	1110
0001	0011	0101	0111	1001	1011	1101	1111
0000	0000	0001	0001	0010	0010	0011	0011
1000	1000	1001	1001	1010	1010	1011	1011

1000	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
0000	0010	0010	0100	1000	1010	1100	1110
0001	0011	0101	01111	1001	1011	1101	1111
0100	0100	0001	0101	0110	0110	0111	0111
1100	1100	1101	1101	1110	1110	1011	1011

Граф



Маршрут із 2 у 14 через 3:

2(0010) => 3(0011) => 4(0100) => 7(0111) => 14(1110)

Нехай сталася відмова вузла 7:

2(0010) => 3(0011) => 4(0100)=> 6(0110) => 12(1100) => 14(1110)

D=3

Ds ≈ 2.77

S=4 так як кожен вузол з'єднаний з 4 іншими

R=32

3. ***Мережа Фейстеля. Генератори псевдовипадкових чисел****. Наведіть перші 3 числа для лінійного конгруентного генератора для чисел B, C, D, W0=0,5.*

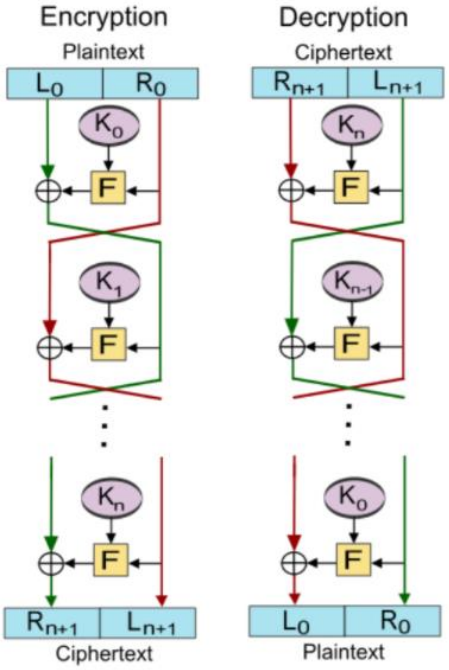
Мережа Фейстеля *– різновид блочного шифру з певною ітеративною*

Структурою, що означає дана мережа являє собою багаторазову повторювану структуру. В такій блочній структурі при переході від одного блока до іншого змінюється ключ, причем він залежить від попередніх блоків.

*Основні принципи **алгоритму шифрування** мережі Фейстеля :*

- *Вся інформація розбивається на блоки фіксованої довжини, якщо довжина вхідного блоку менше, ніж розмір, який шифрується заданим алгоритмом, то блок подовжується. Як правило довжина блоку є ступенем двійки (*64 біта, 128 біт). З усіма блоками виконуються однакові операції, тому розглянемо на прикладі одного блока.*

- *Обраний блок ділиться на два рівних підблоки - "лівий" (L0) І "правий" (R0).*



- *Лівий підблок L0 видозмінюється функцією f(Д0,K0) в залежності від ключа K0, Після цього він складається по модулю 2 з правим підблоком R0.*

- *Результат складання привласнюється новому лівому підблоку L1, який буде половиною вхідних даних для наступного раунду, а лівий підблок L0 присвоюється без змін новому правому підблоку R0, який буде іншою половиною*

- *Після чого операція повторюється N-1 разів, при цьому при переході від одного етапу до іншого змінюються раундові ключі (K0 на K1 і т. д.), де N - кількість раундів в заданому алгоритмі.*

***Алгоритм розшифровки** по суті такий же, як і шифрування, проте ключі в ньому ідуть у зворотному порядку, від останнього (N-го) до першого.*

Для лінійного конгруентного генератора використовується формула:

$$Wi+1 = (B * Wi + C) mod D$$

Тому :

$B = 2; C = 2; D = 9; W0 = 0.5$

$$W1 = (2 * W0 + 2) mod 9 = (2 * 0.5 + 2) mod 9 = 3$$

$$W2 = (2 * W1 + 2) mod 9 = (2 * 3 + 2) mod 9 = 8$$

$$W3 = (2 * W2 + 2) mod 9 = (2 * 8 + 2) mod 9 = 0$$

***Відповідь:** 3, 8, 0;*

4. Пошук простих чисел в заданому діапазоні. *Знайдіть за допомогою тесту Рабіна, просте число, яке буде більше за 60+(A+B+C)*D.*

Знайдемо просте число $P > P_{max} = 60 + (2 + 2 + 9) * 9 = 177$

За тестом Рабіна:

Нехай a = 3;

$$k = log_3 \frac{177}{2} = 4.08 \qquad k \approx 5$$

$$P_{1,2} = 2 * 3^5 \pm 1 = 2 * 243 \pm 1 = 486 \pm 1$$

$$P_1 = 485 \qquad P_2 = 487$$

Перевірка на простоту:

$3^{484} mod 485 = 81$ не підходить

$3^{486} mod 487 = 1$ підходить

Отже 487 це просте число та більше ніж P_{max}*;*

Відповідь: *487;*

5. Виконайте шифрування за алгоритмом RSA.

- *p=7, q=13. Згенеруйте відкритий і секретні ключі. Зашифруйте і розшифруйте повідомлення, яке містить три цифри ABC.*

$P = p * q = 7 * 13 = 91$

$F_e = (p - 1)*(q - 1) = (7 - 1) * (13 - 1) = 6 * 12 = 72$

72 mod 2 = 0 => не підходить

72 mod 3 = 0 => не підходить

72 mod 5 = 2 => підходить

Тоді e => 5

*K * Φ(N) + 1mod e = 0, k = 2*

*d = (k * Φ(N) + 1)/e = 29*

Зашифруємо повідомлення 222:

Ключ: <5, 91>

$$222^5 mod 91 = 66$$

Розшифруємо повідомлення 222:

Ключ: <29,91>

$$66^{29} mod 91 = 222$$

Отже ключі знайдено правильно, так як ми отримали те ж повідомлення, що зашифрували.

- ***Завдання з coursera (quantum computing).*** *Відкритий ключ RSA: (e, N) = (53, 299). Повідомлення (число) m зашифровано цим відкритим ключовим словом: e (m)= 171. Розшифруйте повідомлення.*

Маємо відкритий ключ <53;299> та одне повідомлення «171», що закодоване цим ключем. Потрібно знайти початкове повідомлення m.

*N = 299, тому p * q = 13 * 23*

Φ(N) = (p-1)(q-1) = 264*

k =1

*d = (k * Φ(N) + 1)/e = 5*

Розшифруємо повідомлення:

$171^5 \ mod 299 = 19$

Отже, зашифрували повідомлення «19»

Відповідь: *19;*