# Лабораторна робота 6. Алгоритм шифрування ГОСТ 28147-89.

Міждержавний стандарт шифрування ГОСТ 28147-89 передбачає 4 режими роботи:

* режим простої заміни;
* режим гамування;
* режим гамування із зворотним зв'язком;
* режим вироблення имитовставки.

**Проста заміна**

Режим простої заміни є основою для решти всіх режимів. Довжина блоку - 64 біта, довжина ключа – 256 біт, кількість підключів – 32, довжина підключа - 32 біта, число циклів –32.

Відкриті дані, належні шифруванню, розбиваються на 64-бітові блоки, які обробляються незалежно один від одного. (Оскільки блоки даних шифруються незалежно один від одного, при шифруванні двох однакових блоків відкритого тексту виходять однакові блоки шифротекста і навпаки.). Схема обробки 64-бітового блоку показана на Рис.Д1-2. Процедура шифрування 64-бітового блоку включає 32 цикли. У кожному циклі використовується свій підключ, який виробляється з основного ключа. Розмір масиву відкритих або зашифрованих даних, що піддається відповідно шифруванню або дешифруванню, повинен бути кратний 64 бітам, після виконання операції розмір отриманого масиву даних не змінюється.

Режим простої заміни застосовується для шифрування короткої, ключової інформації.

У **режимах гамування** виробляється гама- шифр блоками по 64 біта із застосуванням ГОСТ в режимі простої заміни. У першому режимі гама не залежить від шифрованих даних, в другому – залежить від шифроблоків.

Режим вироблення **імитовставки** призначений для виявлення випадкових або умисних спотворень даних. Імітовставка виробляється (за допомогою перших 16 циклів ГОСТ в режимі простій заміни) з відкритих даних і ключа і додається при передачі по каналу зв'язку до блоків зашифрованих даних.

 

де ⊕ - складання по модулю 2

Рис. Д1- Алгоритм шифрування ГОСТ 28147-89 (режим простої заміни)



Рис.Д2- Функція перетворення *f(R,X)* в алгоритмі ГОСТ 28147-89

# Хай 32-бітова послідовність має вигляд

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1001 | 1011 | 1100 | 0101 | 1110 | 0100 | 0000 | 1001 |

Розіб'ємо вхідну послідовність на 8 блоків по 4 біта. Шостий блок 1100 пропускаємо через 6-ий вузол підстановки за наступним правилом: перетворимо двійкове число 1100 до десяткового вигляду – 12. Заповнення 12-го рядка для 6-го вузла підстановки рівне 9, що в двійковому вигляді є 1001. Таким чином, 4-бітовий блок 1100 замінюється на 1001. Решта блоків замінюється аналогічно.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | номер вузла |
| 1001 | 1011 | 1100 | 0101 | 1110 | 0100 | 0000 | 1001 | вхід |
| 9 | 11 | 12 | 5 | 14 | 4 | 0 | 9 | адреса  |
| 2 | 7 | 9 | 15 | 5 | 10 | 14 | 11 | заповнення |
| 0010 | 0111 | 1001 | 1111 | 0101 | 1010 | 1110 | 1011 | результат |

Вихідна послідовність має вигляд

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0010 | 0111 | 1001 | 1111 | 0101 | 1010 | 1110 | 1011 |

Виконайте перший цикл алгоритму шифрування ГОСТ 28147-89 в режимі простої заміни. Для отримання 64 біт початкового тексту використовуйте 8 перших літер зі своїх даних: Прізвища Імені по Батькові. Для отримання ключа (256 біт) використовують текст, що складається з 32 літер. Перший підключ містить перші 4 букви.

Початкові дані для шифрування: КОЗИНА Г

Для ключа візьмемо послідовність що складається з 32 букв:

*Алина пошла в лес собирать грибы*

Для першого підключа Х використовуємо перші 4 букви ключа: АЛИН.

Перекладаємо початковий текст і перший підключ в двійкову послідовність (см.Д2):

початковий текст

|  |  |
| --- | --- |
| К | 11001010 |
| О | 11001110 |
| З | 11000111 |
| И | 11001000 |
| Н | 11001101 |
| А | 11000000 |
| пропуск | 00100000 |
| Г | 11000011 |

перший підключ X0

|  |  |
| --- | --- |
| А | 11000000 |
| Л | 11001011 |
| И | 11001000 |
| Н | 11001101 |

Таким чином, перші 64 біта визначають вхідну послідовність

L0: 11001010 11001110 11000111 11001000

R0: 11001101 11000000 00100000 11000011

наступні 32 біта визначають перший підключ

Х0: 11000000 11001011 11001000 11001101

I. Знайдемо значення функції перетворення f(R0,X0) (див. Д1)

1). Обчислення суми R0 і X0 по mod 232

R0: 1100 1101 1100 0000 0010 0000 1100 0011

Х0: 1100 0000 1100 1011 1100 1000 1100 1101

 1000 1110 1000 1011 1110 1001 1001 0000

2). Перетворення в блоці підстановки

Результат підсумовування R0+X0 по mod 232

1000 1110 1000 1011 1110 1001 1001 0000

перетворимо в блоці підстановки (див. Д2). Для кожного 4-бітового блоку обчислимо його адресу в таблиці підстановки. Номер блоку відповідає номеру стовпця, десяткове значення блоку відповідає номеру рядка в таблиці. Таким чином, 5-тий блок (1011) замінюється заповненням 11-го рядка і п'ятого стовпця в таблиці підстановки (1110).

номери блоків

 8 7 6 5 4 3 2 1

1000 1110 1000 1011 1110 1001 1001 0000

відповідні номери рядків в таблиці підстановки

 8 14 8 11 14 9 9 0

заповнення

 9 2 3 14 5 15 3 4

результат

1001 0010 0011 1110 0101 1111 0011 0100

3). Циклічне зрушення результату п.2 на 11 біт вліво

1111 0010 1111 1001 1010 0100 1001 0001

Таким чином, знайшли значення функції f (R0,X0):

1111 0010 1111 1001 1010 0100 1001 0001

 II. Обчислюємо R1= f(R0,X0) ⊕L0.

Результат перетворення функції f(R0,X0) складаємо з L0 по mod2:

L0: 1100 1010 1100 1110 1100 0111 1100 1000

f(R0,X0): 1111 0010 1111 1001 1010 0100 1001 0001

R1: 0011 1000 0011 0111 0110 0011 0101 1001