Тема 8. ШИФРИ З ВИКОРИСТАННЯМ ГАМУВАННЯ

Однією з ознак абсолютно стійкого шифру є повна випадковість ключа. Зрозуміло, що використовуючи випадкові числа, можна побудувати будь-який випадковий ключ.

Одним із найпростіших механічних приладів для отримання випадкових чисел є рулетка. В сучасних умовах для отримання випадкових чисел застосовують різноманітні генератори, які поділяються на дві групи – апаратні та програмні. В апаратних генераторах джерелом випадкових чисел є шум в електронних приладах. Програмний генератор випадкових чисел являє собою програму, яка генерує послідовність чисел за деяким алфавітом. Завдяки алгоритму, така послідовність чисел цілком детермінована (визначена), тобто принципово не може бути випадковою. Але, оскільки така числова послідовність за своїм зовнішнім виглядом та властивостями дуже нагадує випадкову, то її називають *послідовністю псевдовипадкових чисел.*

В криптографії послідовність псевдовипадкових чисел називають *гамою шифру,* або просто *гамою.* Гама має свій період. Період гами – це така кількість псевдовипадкових чисел у послідовності, після якої вони починають повторюватись. [8]

1. Шифр звичайного накладання двійкової гами

Процес шифрування звичайним накладанням двійкової гами полягає у наступному [8]:

1. Відкритий текст подають у вигляді неперервної послідовності k-розрядних двійкових чисел. Для цього використовують перетворення порядкових номерів знаків відкритого тексту із алфавіту обсягом $m=2^k$.
2. Генерують гаму шифру у вигляді послідовності псевдовипадкових двійкових цифр.
3. На кожний черговий розряд відкритого тексту накладають відповідний розряд двійкової гами з використанням операції додавання по модулю 2 і таким шляхом отримують черговий двійковий розряд криптограми.

(Виключна диз'юнкція (також операція XOR, додавання за модулем два) – двомісна логічна операція, що приймає значення «істина» тоді і тільки тоді коли значення «істина» має рівно один з її операндів. Виключна диз'юнкція є запереченням логічної еквівалентності. Для запису операції використовуються позначення: $a \oplus b$).

4. Подають криптограму через даний алфавіт, виконавши попереднє розбиття криптограми на послідовні к-розрядні двійкові числа

Рівність $m=2^k$ є природнім обмеженням даного методу. Якщо $m>2^k$, то у вигляді k-розрядних двійкових чисел неможливо представити всі знаки алфавіту. Якщо $m<2^k$, то не кожне двійкове число може бути представлене у вигляді знаку даного алфавіту. В останньому випадку залишається тільки відмовитися від цієї операції.

Ключові дані, що входять до складу шифру, такі:

- ✓ алфавіт з порядковими номерами знаків, а також кількість розрядів двійкового їх подання;
- ✓ параметри обраного методу генерації двійкової гами шифру, в тому числі кількість розрядів двійкового подання кожного псевдовипадкового числа їх послідовності.

Розглянемо приклад шифрування відкритих текстів, побудованих в алфавіті обсягом $m=2^3=8$ знаки цього алфавіту можна представити у вигляді 3-розрядних двійкових чисел:

Номер	0	1	2	3	4	5	6	7
Знак відкритого тексту	А	Б	В	Г	Д	Ж	З	Е
Двійковий код	000	001	010	011	100	101	110	111

Двійкову гамму шифру згенеруємо лінійним конгруентним методом $x_{n+1}=(a \cdot x_n+b) \bmod m,\ n=0, 1, \ldots$ з параметрами $m=16,\ a=5,\ b=7,\ x_0=10$. Початок послідовності псевдовипадкових чисел має вигляд: 10, 9, 4, 11, 14, …. Оскільки тут $m=2^4$, то кожне десяткове число слід представляти не менше як 4-

рирозрядне двійкове. У випадку 4-х розрядного подання, початок двійкової гами такий: 1010|1001|0100|1011|1110 ….

Шифрування:

Відкритий текст «БАГАЖА»	001|000|011|000|101|000
Гамма шифру	101|010|010|100|101|111
Результат додавання по модулю 2	100|010|001|100|000|111
Криптограма	Д В Б Д А Е

При дешифрування криптограми на неї накладається та ж сама двійкова гамма.

Дешифрування:

Криптограма «ДВБДАЕ»	100|010|001|100|000|111
Гамма шифру	101|010|010|100|101|111
Результат додавання по модулю 2	001|000|011|000|101|000
Відкритий текст	Б А Г А Ж А

2. Шифр багаторазового накладання двійкових гам

Шифр полягає в тому, що на відкритий текст спочатку накладається перга гама, потім на результат шифрування накладається друга гама, на новий результат − третя і так далі. Використання цього шифру пов’язане з тим, що є можливість досягнути більшого періоду результуючої гами у порівнянні з періодами складових гам. Для цього, періоди складових гам мають бути різними.

При використанні такого шифру слід пам’ятати, що результат шифрування не залежить від послідовності накладання гам. Аналогічно, і результат дешифрування буде правильним не залежно від того, в якому порядку застосовувати гами. [8]

3. Комбінований шифр Френдберга

Цей шифр є комбінованим, оскільки поєднує заміну з перестановкою, яка, в свою чергу, використовує гаму шифру. Як було доведено автором шифру, даний метод дозволяє приховувати частотні характеристики алфавіту відкритого тексту, що ускладнює зламування шифру.

Основні кроки шифрування чергового знаку відкритого тексту методом Френдберга наступні:

- ✓ виконання заміни згідно шифрувальної таблиці;
- ✓ отримання чергового числа гами шифру;
- ✓ використання цього числа для виконання перестановок у шифрувальній таблиці.

Далі здійснюється перехід до шифрування наступного знаку відкритого тексту і т.д.

Як бачимо, основні складові методу традиційні – шифрувальна таблиця і гама шифру.

Але особливістю в даному випадку є те, що обсяг алфавіту повідомлень і модуль послідовності псевдовипадкових чисел мають співпадати.

Шифрування методом Френдберга найбільш доцільно розглянути на прикладі.

Розглянемо приклад шифрування відкритих текстів, побудованих в алфавіті обсягом $m = 7$. Спосіб вибору шифрувальної таблиці для виконання замін не є суттєвим і може бути довільним. У загальному випадку її початковий вигляд вважається заданим і входить до складу ключових даних. Припустимо, що шифрувальна таблиця має наступний вигляд.

Номер	0	1	2	3	4	5	6
Знак відкритого тексту	А	Б	В	Г	Д	Е	Ж
Знак криптограми	D	X	T	V	N	S	W

Спосіб отримання гами шифру для виконання перестановок теж не є суттєвим і може бути довільним. Важливо тільки, щоб якимось чином була забезпечена достатня кількість псевдовипадкових чисел у їх послідовності. Крім того, вимога співпадання обсягу алфавіту повідомлень та модуля послідовності псевдовипадкових чисел для вибраного алфавіту проявляється в тому, що псевдовипадкові числа можуть приймати значення в межах від 0 до 6 включно. Припустимо, що послідовність псевдовипадкових чисел така: 403631205314625….

Процес шифрування відкритого тексту “ВЖЕДАГЖ” представлено в таблиці. Отримуємо криптограму “TWSTTSD” . Дешифрування криптограми відбувається аналогічно. Отже, наведену таблицю можна розглядати одночасно і як таблицю дешифрування криптограми “TWSTTSD”. Звичайно, буде отримано відкритий текст “ВЖЕДАГЖ”.

Цікаво, що даний приклад дійсно показує, що даний шифр дозволяє якісно приховати частотні характеристики алфавіту повідомлень. Це підтверджується, наприклад, тим, що один і той же знак криптограми “Т” відповідає різним знакам відкритого тексту (“В”, “Д” і “А”). [8]

Таблиця процесу шифрування (дешифрування):

Крок	Видозміни шифрувальних таблиць	Знак відкритого тексту	Знак криптограми	Порядковий номер знаку криптограми в алфавіті	Псевдовипадкове число	Перестановка знаків відкритого тексту у шифрувальній таблиці
1	0123456 АБВГДЕЖ DXTVNSW	В	Т	2	4	2 ⇔ 4
2	0123456 АБДГВЕЖ DXTVNSW	Ж	W	6	0	6 ⇔ 0
3	0123456 ЖБДГВЕА DXTVNSW	Е	S	5	3	5 ⇔ 3
4	0123456 ЖБДЕВГА DXTVNSW	Д	Т	2	6	2 ⇔ 6
5	0123456 ЖБАЕВГД DXTVNSW	А	Т	2	3	2 ⇔ 3
6	0123456 ЖБЕАВГД DXTVNSW	Г	S	5	1	5 ⇔ 1
7	0123456 ЖГЕАВБД DXTVNSW	Ж	D	0	2	0 ⇔ 2
8	0123456 ЕГЖАВБД DXTVNSW					