Тема 7. ШИФРИ, ЩО ВИКОРИСТОВУЮТЬ АНАЛІТИЧНІ ПЕРЕТВОРЕННЯ

В загальному випадку будь-який шифр аналітичних перетворень $y=f(x)$ за даним елементом x відкритого тексту обчислює відповідний елемент криптограми y. Тому ці шифри належать до шифрів заміни. Кожному з них відповідає певне правило обчислення f. Правила обчислень базуються на різноманітних математичних методах.

1. Афінна система моноалфавітної заміни

Афінна система моноалфавітної системи (АФМЗ) відрізняється від замін Цезаря. Вона дає суттєву відмінність у порядку слідування знаків вторинного алфавіту у порівнянні з первинним. Афінна система моноалфавітної заміни використовує модулярну арифметику. Її загальна формула має вигляд: $j_y=(a\cdot j_x+b) \bmod m$, де

j_x – *порядковий номер знака відкритого тексту в алфавіті,*

j_y – *порядковий номер знака криптограми в алфавіті,*

m - *обсяг алфавіту,*

a, b – *ключ заміни, який являє собою пару цілих чисел* $0 \le a < m$, $0 \le b < m$

Для побудови шифрувальної таблиці цю формулу застосовують послідовно до кожного знаку алфавіту, при цьому вказане криптографічне перетворення є взаємно однозначним на даному алфавіті тільки при умові, що числа a і m взаємно прості. $(НСД(a,m)=1)$.

Побудуємо, наприклад, шифрувальну таблицю для алфавіту «АБВГДЕЖЗИК» обсягом $m=10$, використовуючи ключ $(a,b)=(7,3)$. При цьому всі вказані вище умови виконуються, в тому числі $НСД(7,10)=1$.

Порядковий номер знака алфавіту	Знак первинного алфавіту (відкритого тексту)	Результат обчислення за формулою $j_y=(a\cdot j_x+b) \bmod m$	Знак вторинного алфавіту (криптограма)
0	А	$(7\cdot 0 + 3) \bmod 10 = 3$	Г
1	Б	$(7\cdot 1 + 3) \bmod 10 = 0$	А

2	В	(7·2 + 3) mod 10 = 7	З
3	Г	(7·3 + 3) mod 10 = 4	Д
4	Д	(7·4 + 3) mod 10 = 1	Б
5	Е	(7·5 + 3) mod 10 = 8	И
6	Ж	(7·6 + 3) mod 10 = 5	Е
7	З	(7·7 + 3) mod 10 = 2	В
8	И	(7·8 + 3) mod 10 = 9	К
9	К	(7·9 + 3) mod 10 = 6	Ж

Шифрувальна таблиця набуває наступного вигляду:

Номер	0	1	2	3	4	5	6	7	8	9
Знак відкритого тексту	А	Б	В	Г	Д	Е	Ж	З	И	К
Знак криптограми	Г	А	З	Д	Б	И	Е	В	К	Ж

У відповідності з наведеним прикладом відкритий текст «ЖИВЕ» → «ЕКЗИ». Дешифрування криптограми здійснюється за цією ж шифрувальною таблицею.

Для АСМЗ характерний недолік пов’язаний з відсутністю маскування частот появи різних знаків відкритого тексту. Перевагою методу є те, що вторинний алфавіт є суттєво перевпорядкованим і водночас існує проста можливість його обчислення через первинний.

Відмітимо, що вимога *НСД(a,m)=1* є надзвичайно суттєвою, оскільки саме вона забезпечує повний набір знаків вторинного алфавіту. [8]

2. Шифр Віженера

Шифр Віженера також використовує модулярну арифметику.

У загальному випадку застосування шифру Віженера полягає у наступному:

Розглянемо алфавіт відкритого тексту $A = (a_0, a_1, \dots, a_{m-1})$, що містить m знаків, ключ $K = (k_1, k_2, \dots, k_{n-1})$, знаки якого вибрано випадковим способом алфавіту A. Довжина ключа n рівна довжині відкритого тексту $X = (x_1, x_2, \dots, x_{n-}$

$_1$). Накладемо ключ на відкритий текст. Розглянемо деякий знак x_p, $p=0,1,2,\ldots,n-1$ відкритого тексту X. Він має порядковий номер i в алфавіті A. Розглянемо також відповідний знак ключа k_p. Він має в алфавіті A порядковий номер j. Тоді знак x_p відкритого тексту перетворюється у знак криптограми y_p у відповідності з правилом $y_p=a_{(i+j) \bmod m}$.

Наприклад, для алфавіту «абвгдеж» обсягом $m=7$ таблиця порядкових номерів знаків відкритого тексту має наступний вигляд:

Номер	0	1	2	3	4	5	6
Знак відкритого тексту	а	б	в	г	д	е	ж

Зашифруємо відкритий текст «вежагад» за допомогою ключа «бгбдеиг» тієї самої довжини. Ще раз підкреслимо що знаки відкритого тексту і знаки ключа вибрано із одного й того ж алфавіту. Процес застосування шифру Віженера можна представити у вигляді наступної таблиці

Знак відкритого тексту	Порядковий номер знака відкритого тексту в алфавіті *(i)*	Знак ключа шифрування	Порядковий номер знака ключа шифрування в алфавіті *(j)*	Обчислення номера знака криптограми в алфавіті	Знак криптограми
в	2	б	1	(2+1) mod 7 = 3	г
е	5	г	3	(5+3) mod 7 = 1	б
ж	6	б	1	(6+1) mod 7 = 0	а
а	0	д	4	(0+4) mod 7 = 4	д
г	3	е	5	(3+5) mod 7 = 1	б
а	0	в	2	(0+2) mod 7 = 2	в
д	4	г	3	(4+3) mod 7 = 0	а

Таким чином отримуємо криптограму «гбадбва».

Для дешифрування криптограм потрібно спочатку отриманий відповідний ключ. Тут застосовується дуже просте правило: якщо деякий знак ключа шифрування має деякий номер j в алфавіті A, то відповідний знак ключа дешифрування знаходиться в тому ж алфавіті під номером $(m-j) \bmod m$.

Для прикладу, ключ шифрування «бгбдевг» перетворимо у відповідний ключ дешифрування при умові, що використовується той же самий алфавіт.

Знак ключа	Порядковий	Обчислення	Знак ключа

шифрування	номер знака ключа шифрування в алфавіті	порядкового номеру знака ключа дешифрування	дешифрування
б	1	(7-1) mod 7 = 6	ж
г	3	(7-3) mod 7 = 4	д
б	1	(7-1) mod 7 = 6	ж
д	4	(7-4) mod 7 = 3	г
е	5	(7-5) mod 7 = 2	в
в	2	(7-2) mod 7 = 5	е
г	3	(7-3) mod 7 = 4	д

Таким чином, отримуємо ключ дешифрування «жджгвед».

Тепер дешифрування криптограми можна здійснити точно таким же способом, як і шифрування відкритого тексту.

Знак криптограми	Порядковий номер знака криптограми в алфавіті	Знак ключа дешифрування	Порядковий номер знака ключа дешифрування в алфавіті *(j)*	Обчислення номера знака криптограми в алфавіті	Знак відкритого тексту
г	3	ж	6	(3+6) mod 7 = 2	в
б	1	д	4	(1+4) mod 7 = 5	е
а	0	ж	6	(0+6) mod 7 = 6	ж
д	4	г	3	(4+3) mod 7 = 0	а
б	1	в	2	(1+2) mod 7 = 3	г
в	2	е	5	(2+5) mod 7 = 0	а
а	0	д	4	(0+4) mod 7 = 4	д

Таким чином, отримуємо відкритий текст «вежагад».

При такому підході маємо абсолютно стійкий шифр, подібний до шифру Вернама. Щоб позбутися незручності такого шифру пов’язаним з великий обсягом ключа *K*, Віженер запропонував використовувати коротший ключ *K**, який шляхом свого періодичного повторення може бути перетворений у ключ *K*, довжина якого співпадає з довжиною відкритого тексту *X*.

Наприклад, алфавіт «0123456789» довжиною *m=10*, ключ шифрування «738» відкритий текст «5742906». Тоді криптограма має вигляд «2029283», а люч дешифрування буде «372». [8]

3. Шифр з автоключем

Умови існування абсолютно стійкого шифру кажуть, властивості шифру Вернама підтверджують те, що чим більша довжина ключа, тим вища стійкість шифру. Але, з іншої сторони, як показує шифр Віженера, користуватися короткими ключами значно зручніше.

Шифр з авто ключем, не позбавляючи зручностей, пов’язаних з коротким ключем, дозволяє подовжувати ключ автоматично.

Короткий ключ, як і у шифрі Віженера, вибирається звичайним способом з букв використовуваного алфавіту.

Автоматичне подовження ключа можливе за двома схемами:

- ✓ шляхом приєднання до короткого ключа того ж самого відкритого тексту;
- ✓ шляхом поступового приєднання до короткого ключа утворюваної криптограми.

У всьому іншому *(шифрування/дешифрування)* використання шифру з автоключем повністю співпадає з шифром Віженера. [8]