Тема 2. КЛАСИЧНІ ШИФРИ ПЕРЕСТАНОВКИ

1. Загальна характеристика шифрів перестановки

Шифри перестановки відносяться до симетричних. Це означає, що один і той же алгоритм, а також один і той же ключ використовуються і для шифрування, і для дешифрування повідомлень. При цьому алгоритм та ключ шифрування з метою використання для дешифрування можуть бути шляхом певних перетворень представлені в іншій формі. Але це не означає, що вони різні.

Шифр перестановки полягає в тому, що окремі знаки або певні групи знаків за певними правилами переставляються місцями безпосередньо у відкритому тексті.

У найпростішому випадку шифр перестановки використовується як блоковий. Це означає, що в процесі шифрування знаки відкритого тексту переставляють в межах деяких блоків фіксованого розміру.

Стійкість шифру перестановки залежить від розміру блоку, а також від рівня складності порядку перестановки.

Найстародавніший приклад застосування шифру перестановки датується V-м століттям до н.е. Спартанці шифрували свої повідомлення за допомогою пристрою під назвою «скитала».

На циліндричну палицю (на скиталу) намотували спіраллю виток до витка стрічку пергамента. На ній писали вздовж осі палиці декілька рядків повідомлення. Після розмотування стрічки знаки на ній виявлялись розташованими хаотично.

	п	о	в	і	
	д	о	м	л	
	е	н	н	я	

Наприклад, відкритий текст «повідомлення», записаний в три рядки по одній літері на ширину стрічки, дає криптограму «пдеоонвмніля». Ключем такого шифру є діаметр палиці (або, що теж саме, кількість рядків тексту навколо палиці). [8]

2. Звичайна перестановка

Розглянемо блок відкритого тексту $T=(T_1,T_2,T_3,...,T_N)$ довжиною N і відповідний блок попарно різних індексів $\sigma=\sigma(K_1,K_2,K_3,...,K_N)$, де $1\leq K_i\leq N$ для всіх $1\leq i\leq N$. Тут блок індексів σ є ключем шифрування.

Звичайною перестановкою знаків даного тексту T називається його перевпорядкування таким чином, що знак з позиції $\sigma(i)=K_i$ у відкритому тексті переміщується у позицію i у криптограмі.

Виберемо ключем шифрування вектор індексів $\sigma=(2, 4, 3, 1)$ при N = 4. Він показує наступний взаємозв'язок індексів: $\sigma(1)=2$, $\sigma(2)=4$, $\sigma(3)=3$ і $\sigma(4)=1$ (знак відкритого тексту з порядковим номером 2 перетворюється у знак криптограми з порядковим номером 1, знак відкритого тексту з порядковим номером 4 перетворюється у знак криптограми з порядковим номером 2, знак відкритого тексту з порядковим номером 3 залишається знаком криптограми з тим же порядковим номером, знак відкритого тексту з порядковим номером 1 перетворюється у знак криптограми з порядковим номером 4. На підставі такого ключа текст «шифр» буде зашифровано у криптограму «ирфш». Інакше кажучи, значення i = 2, 4, 3 і 1 дають послідовність перенесення знаків із відкритого тексту у криптограму, тобто «и», «р», «ф» і «ш».

При дешифруванні можна скористуватись тим же ключем σ. При цьому треба врахувати, що індекси у складі ключа показують порядкові номери розташування послідовних знаків криптограми при перенесенні їх у відкритий текст. Наприклад, індекси у складі ключа $\sigma=(2, 4, 3, 1)$ при дешифруванні криптограми «ирфш» показують порядкові номери розташування її знаків при перенесенні їх у відкритий текст (перший знак "и" має у відкритому тексті порядковий номер 2, другий знак "р" має у відкритому тексті порядковий номер

4, третій знак "ф" має у відкритому тексті той же порядковий номер 3 і, нарешті, четвертий знак "ш" має у відкритому тексті порядковий номер 1).

Ще один приклад: відкритий текст "ШИФРУВАННЯ ПЕРЕСТАНОВКОЮ" при використанні ключа σ=(3, 8, 1, 5, 2, 7, 6, 4) для блоку довжиною N=8 перетворюється на криптограму "ФНШУИАВР_СНЕЯЕРПНЮТВАОКО".

Загальна можлива кількість перестановок заданого тексту T із N знаків рівна N!, значення якого швидко зростає зі збільшенням N. [8]

3. Звичайні рядково-стовпчикові табличні перестановки

Це перестановки, коли даний текст записується у прямокутну таблицю певного розміру по рядках, а зашифрований текст прочитується із таблиці по стовпчиках. Основний варіант шифрування полягає в тому, що спочатку отримують шифрувальну таблицю шляхом заповнення її послідовних рядків зліва направо. Після цього отримують криптограму шляхом прочитування її послідовних стовпчиків згори вниз. Наприклад, для повідомлення «перестановки» за допомогою шифрувальної таблиці розміром 3x4 (три рядки і чотири стовпчики) буде отримано криптограму «псоетвракени».

п	е	р	е
с	т	а	н
о	в	к	и

Зрозуміло, що ключем шифру є розмір таблиці (для наведеного прикладу 3x4). І для того, щоб отримати відкритий текст повідомлення, слід вписати криптограму в таблицю того ж самого розміру по стовпчиках, а прочитати по рядках.

Шифр звичайних рядково-стовпчикових табличних перестановок є блоковим. Розмір блоку співпадає із загальною кількістю клітинок таблиці (для наведеного прикладу розмір блоку становить 3x4=12 знаків).

В літературі вказується, що можливе також заповнення таблиці по стовпчиках, а прочитування по рядках. І таку перестановку називають

звичайною стовпчиково-рядковою. Але елементарний аналіз показує, що це еквівалентно звичайному транспонуванню розмірів таблиці. Отже, говорити про такий варіант немає ніякого сенсу, а застосовувати – недоцільно. Дійсно, шифрувальна таблиця розміром 4x3 стовпчиково-рядкової перестановки дає для наведеного прикладу ту ж саму криптограму «псоетвракени».

п	с	о
е	т	в
р	а	к
е	н	и

Інші варіанти заповнення приводять до значного збільшення обсягу ключової інформації (треба указувати порядок заповнення) і тому теж не доцільні для застосування.

Суттєво кращий ефект підвищення криптографічної стійкості дає метод, коли даний текст шифрують, послідовно застосовуючи дві таблиці різного розміру. Таку перестановку називають *подвійною звичайною рядково-стовпчиковою табличною перестановкою.* Наприклад, шифрування повідомлення «стовпчик» за допомогою таблиць 2x4 і 3x3 дає криптограму «счвпоктиб» (останній знак – довільний). [8]

4. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків

Такі перестановки мають більший рівень стійкості.

При такому способі шифрування обумовлюється не тільки розмір таблиці, але й ключове слово. Ключове слово має вигляд вектора індексів перестановок стовпчиків.

Процес шифрування полягає в тому, що над верхнім рядком таблиці записують ключ, довжина якого співпадає з кількістю її стовпчиків. Після цього здійснюють вписування відкритого тексту у таблицю по рядках звичайним способом. Наприклад, повідомлення

4	1	3	2
п	е	р	е
с	т	а	н
о	в	к	и

Криптограма утворюється шляхом прочитування по стовпчиках, але тепер стовпчики беруться не підряд, а у порядку, визначеному ключем. Таким чином отримуємо криптограму «етвениракпсо».

Для підвищення криптографічної стійкості методу даний текст шифрують, послідовно застосовуючи дві таблиці різного розміру та два ключа стовпчиків. Таку перестановку називають подвійною рядково-стовпчиковою табличною перестановкою із застосуванням ключів стовпчиків. [8]

5. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків

Шифр рядково-стовпчикових табличних перестановок із застосуванням ключа рядків принципово нічим не відрізняється від аналогічного шифру, який використовує ключ стовпчиків.

При такому способі шифрування ключове слово має вигляд вектора індексів перестановок рядків.

Процес шифрування полягає в тому, що зліва від першого стовпчика таблиці записують ключ, довжина якого співпадає з кількістю її рядків. Після цього здійснюють вписування відкритого тексту у таблицю по рядках, але не підряд, а у відповідності з ключем. Наприклад, повідомлення «перестановки» з ключем «3, 1, 2» дає наступну шифрувальну таблицю розміром 3х4.

3	о	в	к	и
1	п	е	р	е
2	с	т	а	н

Криптограма утворюється шляхом послідовного прочитування її стовпчиків згори вниз. Таким чином отримуємо криптограму «опсветкраиен».

Для підвищення криптографічної стійкості методу даний текст шифрують, послідовно застосовуючи дві таблиці різного розміру та два ключа рядків. Таку перестановку називають *подвійною рядково-стовпчиковою* табличною перестановкою із застосуванням ключів рядків. [8]

6. Рядково-стовпчикові табличні перестановки з двома ключами

При такому способі шифрування обумовлюються розмір таблиці, а також два ключових слова у вигляді векторів індексів, перше з яких діє на рядки, а друге – на стовпчики.

Процес шифрування полягає в тому, що зліва від першого стовпчика таблиці записують перший ключ, довжина якого співпадає з кількістю її рядків, а над верхнім рядком таблиці записують другий ключ, довжина якого співпадає з кількістю її стовпчиків. Після цього здійснюють вписування відкритого тексту у таблицю по рядках, але не підряд, а у відповідності з першим ключем, який діє на рядки. Наприклад, повідомлення «перестановки» з ключами «3, 1, 2» і «4, 1, 3, 2» дає наступну шифрувальну таблицю розміром 3x4.

	4	1	3	2
3	о	в	к	и

1	п	е	р	е
2	с	т	а	н

Криптограма утворюється шляхом прочитування по стовпчиках, причому стовпчики беруться не підряд, а у порядку, визначеному другим ключем, який діє на стовпчики. Таким чином отримуємо криптограму «ветиенкраопс». [8]

7. Табличні перестановки з використанням трафарету

Квадратним трафаретом називають нанесену на планшет квадратну матрицю з прорізаними віконцями. Планшет, як маску, накладають на папір того ж розміру, і у віконця вписують знаки повідомлення по порядку слідування рядків зліва направо. Після першого заповнення планшет

повертають на 90° за годинниковою стрілкою і процедуру вписування повторюють. Таким способом вписування знаків повідомлення у віконця може бути здійснене чотири рази.

Квадратний трафарет цікавий тим, що після кожного повороту віконця опиняються над незаповненими клітинками паперу. З цією метою розташування віконець на трафареті підбирають спеціально. Кількість віконець не повинна перевищувати четвертої частини від загальної кількості клітинок трафарету. Щоб описати трафарет, застосовують позначення: нуль – віконце відсутнє, одиниця – віконце є. Таким чином, весь трафарет можна представити у вигляді сукупності двійкових чисел, кожне з яких відповідає його рядку. Ці числа доцільно представити у десятковій системі числення. Зрозуміло, що сукупність цих чисел являє собою ключ шифру.

Якщо кількість віконець трафарету виявиться більшою кількості знаків повідомлення, то порожні віконця заповнюються випадковими знаками.

Наприклад, повідомлення «перестановки» при застосуванні квадратного трафарета розміром 4х4, що має чотири віконця, може бути перетворено у криптограму «сапобтвекрваеинг». Цікаво, що на останньому четвертому повороті трафарету знаки повідомлення вже вичерпались, і тому порожні віконця були заповнені додатковими випадковими знаками «абвг». Таким чином, в наведеному прикладі після останнього, отримаємо

		п		**с**							**о**		**а**		
			е		**т**					**в**		**б**			
	р						**а**	**к**						**в**	
Е						**н**			**и**						**г**

0° 90° 180° 270°

с	**а**	**п**	**о**
б	**т**	**в**	**е**
к	**р**	**в**	**а**
е	**и**	**н**	**г**

результат

Ключем цього шифру є розмір квадратного трафарету 4х4 та послідовність двійкових чисел "0010, 0001, 0100, 1000" або, що те ж саме, десяткових чисел "2, 1, 4, 8", які цей квадратний трафарет описують.

Для дешифрування криптограми потрібний такий же самий квадратний трафарет.

В наведеному вище прикладі трафарет має чотири віконця, що дорівнює четвертій частині від загальної кількості клітинок 4х4=16.

Слід відмітити, що для підвищення криптографічної стійкості кількість віконець трафарету можна зробити меншою. Розглянемо відповідній приклад, в якому квадратний трафарет розміром 4х4 має три віконця і описується послідовністю "0, 5, 0, 8".

				е							**а**		**в**		
	п		**е**			**с**									
								н		**о**			**к**		
Р						**т**									**и**

0° 90° 180° 270°

е	**в**		**а**
	п	**с**	**е**
н	**к**	**о**	
р		**т**	**и**

результат

За рахунок зменшення кількості віконець при шифруванні повідомлення «перестановки» після внесення знаків на останньому четвертому повороті залишаються вільними ще чотири клітинки "ев_а_псенко_р_ти". їх слід заповнити додатковими випадковими знаками «абвг» вже без трафарету. Таким чином, отримуємо криптограму "еваабпсенковргти".

Шифр табличних перестановок з використанням квадратного трафарету є блоковим. Розмір блоку можна визначити, якщо кількість віконець трафарету помножити на чотири (для першого прикладу розмір блоку становить 4х4=16 знаків, для другого прикладу – 3х4=12 знаків).

Кількість можливих квадратних трафаретів різко зростає зі збільшенням їх розміру: один для 2x2, 256 для 4x4, більше 100 тисяч – для 6x6. Ця кількість суттєво збільшується за рахунок використання зменшеної кількості віконець.

Крім квадратних трафаретів існують також прямокутні трафарети. Для них застосовують повороти на 180°, а також перекладання на зворотну сторону. Розглянемо відповідній приклад, в якому прямокутний трафарет розміром 4x3 має два віконця. Цей трафарет описується послідовністю “4, 1, 0, 0”.

т											**т**	**т**		**т**
		р							**е**			**е**		**р**
			а					**р**				**а**		**р**
					ф	**а**						**а**		**ф**

0° 90° звор. сторона 180° результат

За рахунок недостатньої кількості віконець при шифруванні повідомлення «трафарет» після внесення знаків на останньому четвертому положенні трафарету залишаються вільними ще чотири клітинки "т_те_ра_ра_ф". їх слід заповнити додатковими випадковими знаками «абвг» вже без трафарету. Таким чином, отримуємо криптограму "татебраврагф". [8]