Розглянемо приклади шифрування, які ґрунтуються на техніці підстановок.

а) **Шифр Цезаря**. Цей шифр відомий з давніх часів і приписують його авторство Юлію Цезарю – римському імператору. Цей шифр базується на заміні кожної літери алфавіту новою літерою цього ж алфавіту, яка знаходиться на три позиції правіше.

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P
n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Дано *відкритий текст:* "meeting will in twelve"
криптограма: PHHWLQJ ZLOO LQ WZHOYH

Зауважимо, що алфавіт "закручений" так, що після літери Z наступною буде йти літера A.

Якщо кожній літері припишемо числовий відповідник ($n(a) = 0, n(b) = 1, \ldots$), то цей шифр можна подати у такому вигляді. Кожна літера відкритого тексту p замінюється літерою тексту зашифрованого q на підставі правила:

$$q = f(p) = n(p) + 3 \ (mod\ 26).$$

Зсув літер в алфавіті може мати довільну величину, а це означає, що загальний вигляд алгоритму є таким:

$$q = f(p) = n(p) + k \ (mod\ 26),$$

де $k \in \{1, 2, \ldots, 26\}$. Алгоритм дешифрації досить простий:

$$p = g(q) = n(q) - k \ (mod\ 26).$$

Якщо відомо, що даний текст зашифрований шифром Цезаря, то його криптоаналіз не складає труднощів. Цей криптоаналіз можна виконати як методом частотного аналізу, так і методом простого перебору, випробовуючи 25 можливих ключів.

Нижче на рисунку показані результати застосування методу перебору до зашифрованого тексту. В даному випадку відкритий текст дістаємо на третьому кроці перебору.

Ключ	PHHWLQJ	ZLOO	LQ	WZHOYH
1	oggvkpi	yknn	kp	vygnxg
2	nffujog	xjmm	jo	uxfmwf
3	meeting	will	in	twelve
4	lddshmc	vhkk	hm	svdkud
⋮	⋮	⋮	⋮	⋮
25	...	...	...	...

Рис. 2.6. Криптоаналіз шифру Цезаря методом перебору

Застосування методу перебору стало можливим, оскільки:

1) відомий алгоритм шифрування і дешифрування;

2) існує тільки 25 можливих ключів;

3) мова відкритого тексту відома і легко розпізнається.

Метод підстановки стає практичним, якщо існує великий простір для вибору ключів. Наприклад, американський стандартний алгоритм DES використовує 56-бітовий ключ, що дає простір вибору 2^{56}, або більше $7 \cdot 10^{16}$ можливих ключів.

Істотним є також третя риса. Якщо не відома мова відкритого тексту, то можемо не розпізнати результати розшифрування. Більше того, криптограма може бути яким-небудь способом скорочена або стиснена, а це додаткові перешкоди на шляху розшифрування. Якщо стиснемо файл, а потім його зашифруємо простим шифром підстановки, то ВТ може бути не розпізнаний цим методом.

Криптоаналіз шифру Цезаря можна ускладнити, якщо поміняти звичний порядок літер в алфавіті. Наприклад, нехай порядок літер змінений таким чином:

a	*b*	*c*	**d**	*e*	*f*	**g**	*h*	*i*	**j**	*k*	*l*	**m**	*n*	*o*	**p**	*q*	*r*	**s**	*t*	*u*	**v**	*w*	*x*	**y**	*z*
a	d	g	j	m	p	s	v	y	b	e	h	k	n	q	t	w	z	c	f	i	l	o	r	u	x

.

Тоді шифрограма буде такою: KMMFYUS OYHH YU FOMHLM і її криптоаналіз стає складнішим.

б) **Блоковий спосіб шифрування** з використанням техніки підстановок. Шифрування слова $p = y_1 y_2 \dots y_m$ у алфавіті зі звичним порядком літер виконується таким чином:

– слово p розбивається на блоки по t символів в кожному блоці;

– кожний символ в блоці перетворюється за допомогою підстановок $\alpha_1, \alpha_2, \dots, \alpha_t$, кожна з яких має вигляд:

$$\alpha_i(k) = k + j_i \ (mod\ 26),$$

де k – номер літери в алфавіті X, а $k + j_i \ (mod\ 26)$ – її відповідник в алфавіті X при підстановці α_i, $i = 1, 2, \dots, t$.

Тоді, коли $t = 3$, $\alpha_1(k) = k + 3$, $\alpha_2(k) = k + 7$, $\alpha_3(k) = k + 10$, слово $p = thi\ sci\ phe\ ris\ sec\ ure$ перетворюється до слова

$$q = wos\ vjs\ soo\ upc\ vlm\ xyo.$$

Дійсно, літера t має номер $k = 19$ і $\alpha_1(k) = 19 + 3 = 22$, а це номер літери w в алфавіті X, літера h має номер $k = 7$ і $\alpha_2(k) = 7 + 7 = 14$, а це номер літери o в алфавіті X, літера i має номер $k = 8$ і $\alpha_3(k) = 8 + 10 = 18$, а це номер літери s в алфавіті X, літера s має номер $k = 18$ і $\alpha_1(k) = 18 + 3 = 21$, а це номер літери v в алфавіті X і т. д.

Дешифрація виконується очевидним чином:

$$\alpha^{-1}(k) = \begin{cases} k - j_i, & \text{якщо } k - j_i \geq 0, \\ k - j_i + 26, & \text{якщо } k - j_i < 0. \end{cases}$$

Наприклад, літери o і c мають таких відповідників:

$\alpha_3^{-1}(14) = 14 - 10 = 4$, а це літера e, $\alpha_3^{-1}(2) = 2 - 10 + 26 = 18$, а це літера s.

Перевагою такого способу шифрування є те, що частота входження літер в текст шифрограми скрита, а це значно ускладнює криптоаналіз такого тексту. ♠.