Захист інформації в телекомунікаційних системах

Лекція № 4

Криптографічний захист інформації: шифри простої та складної заміни

Доцент, к.т.н. Золотарьов Вадим Анатолійович

Харківський національний університет радіоелектроніки

Факультет телекомунікацій та вимірювальної техніки

Кафедра мереж зв'язку

Харків, 2016

Захист інформації в телекомунікаційних системах

Лекція № 4

Криптографічний захист інформації: шифри простої та складної заміни

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Доцент, к.т.н. Золотарьов Вадим Анатолійович

План лекції

1. Шифри простої заміни (підстановки)
2. Шифри складної заміни (підстановки)
3. Комбіновані шифри

Питання 1

ШИФРИ ПРОСТОЇ ЗАМІНИ

Шифри заміни

- Нехай шифруються повідомлення українською мовою і заміні підлягає кожна літера цих повідомлень.
- Тоді, літері **А** вихідного алфавіту співставляється деяка множина символів (шифрозамін) $\mathbf{M_А}$, **Б** – $\mathbf{M_Б}$, …, **Я** – $\mathbf{M_Я}$.
- Шифрозаміни обирають таким чином, щоб будь-які дві множини ($\mathbf{M_i}$ та $\mathbf{M_j}$, $\mathbf{i \neq j}$) не містили однакових елементів ($\mathbf{M_i \cap M_j = \varnothing}$).

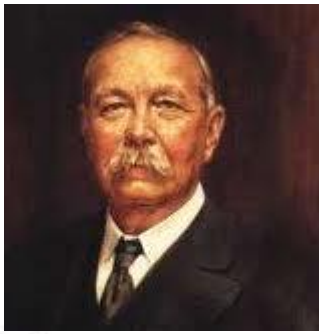
Ключ шифру заміни

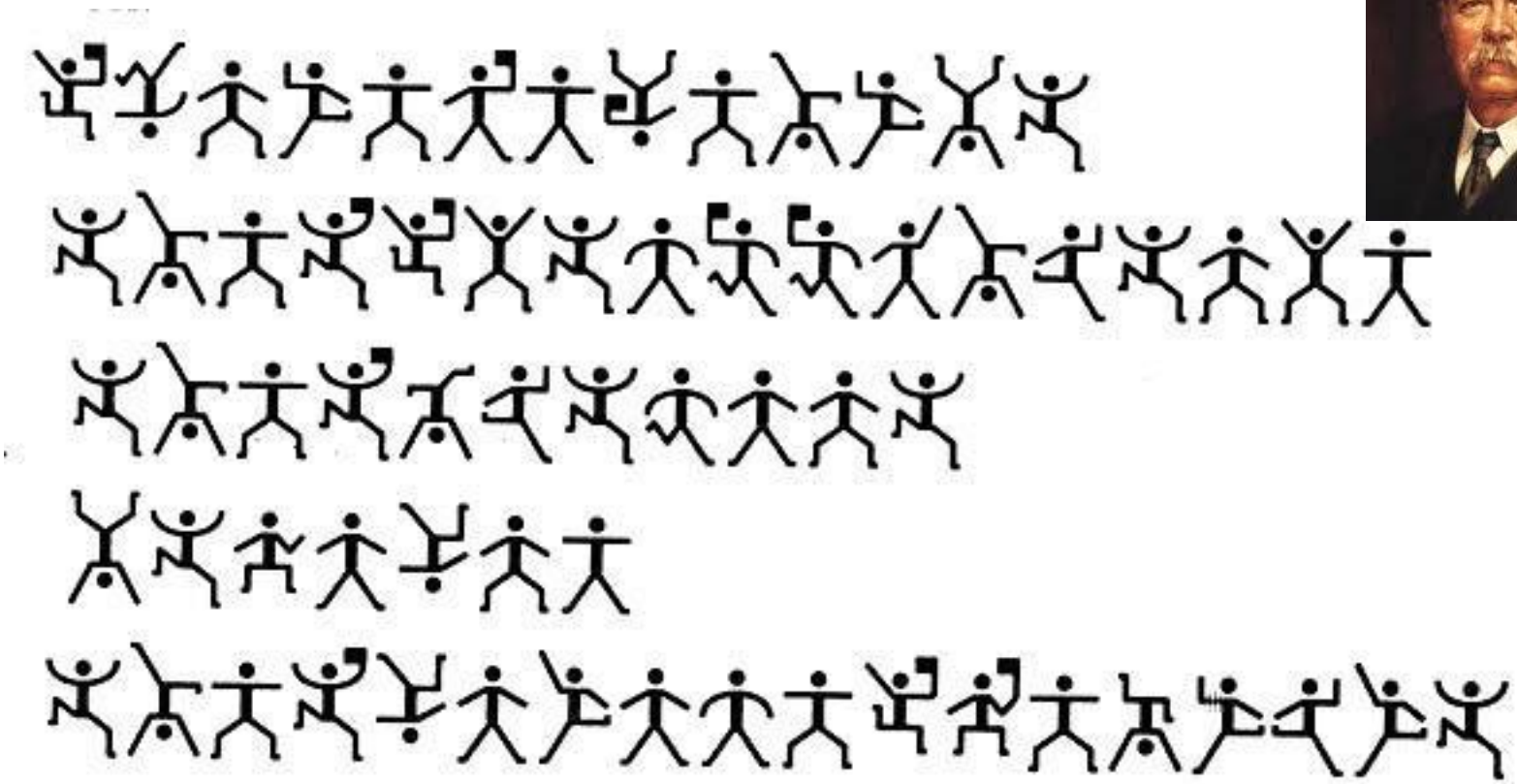
А	Б	…	Я
$М_А$	$М_Б$	…	$М_Я$

- При шифровані кожна літера **А** відкритого повідомлення замінюється будь-яким символи з множини $\mathbf{M_A}$.
- Якщо в повідомленні міститься кілька літер **А**, то кожна з них замінюється на будь-який символ з $\mathbf{M_A}$.
- За рахунок цього за допомогою одного ключа можна отримати різні варіанти шифрограми для одного і того ж відкритого повідомлення.

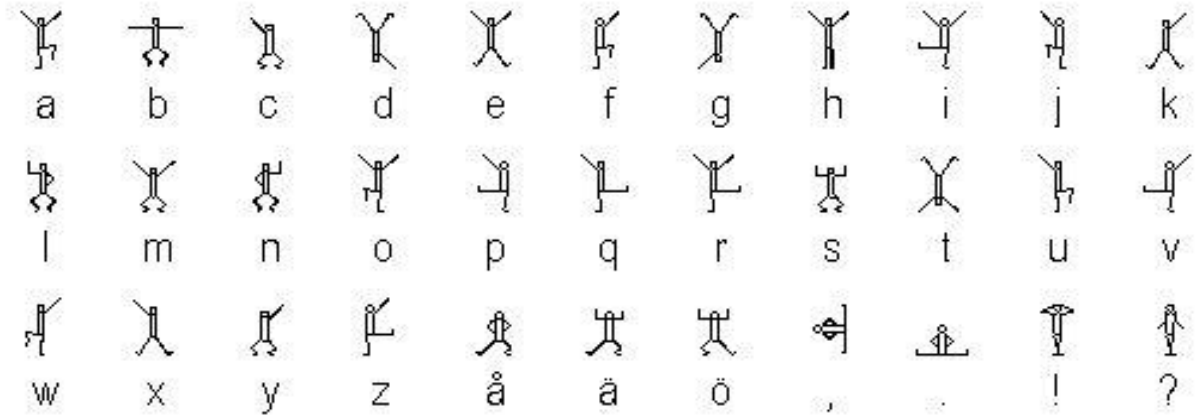
- Оскільки множини $\mathbf{M_А}$, $\mathbf{M_Б}$, ..., $\mathbf{M_Я}$ попарно не пересікаються, то за кожним символом шифрограми можна однозначно визначити, якій множині він належить і яку літеру відкритого повідомлення він замінює.
- Тому розшифрування можливо і відкрите повідомлення визначається єдиним чином.

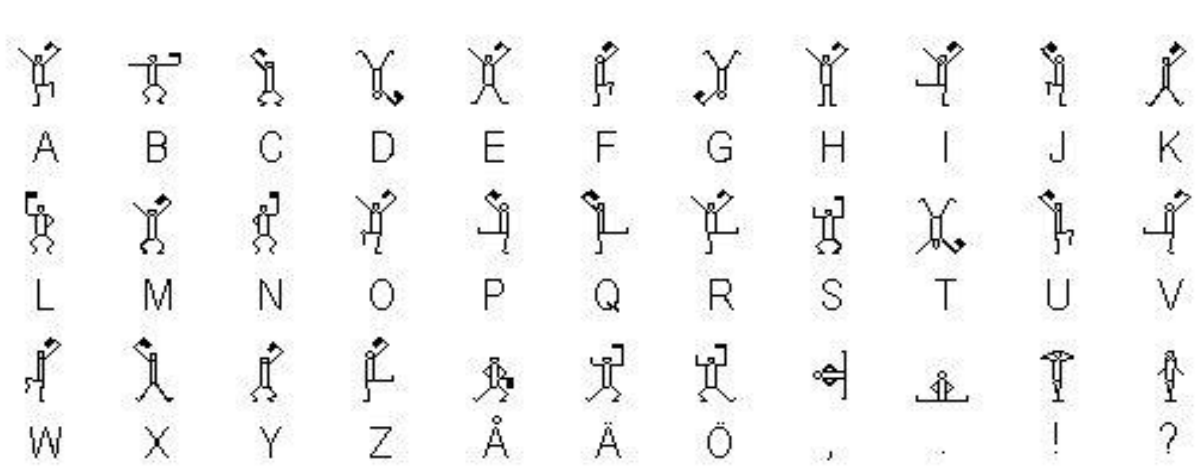
Артур Конан Дойль
«Таємниця чоловічків, що танцюють»

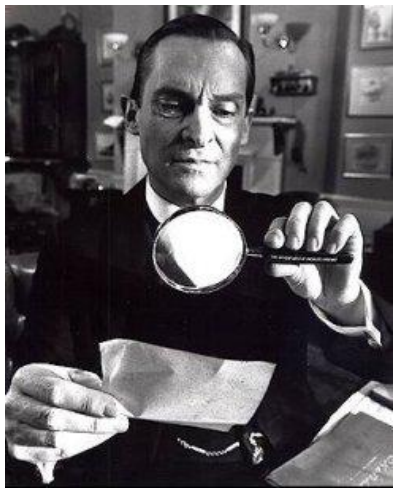




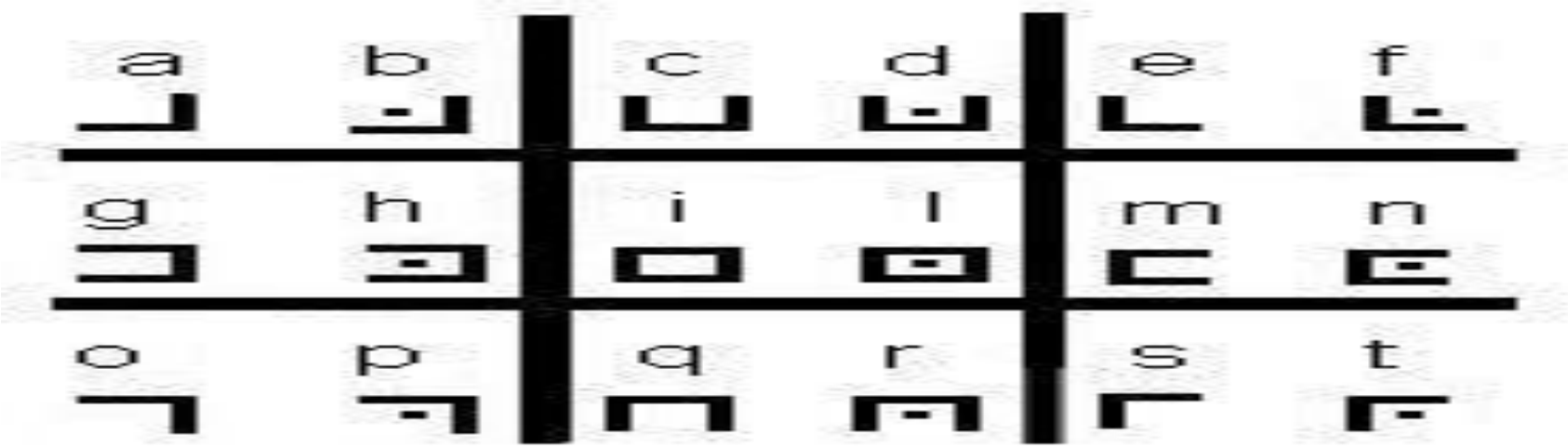
Чоловічки, що танцюють

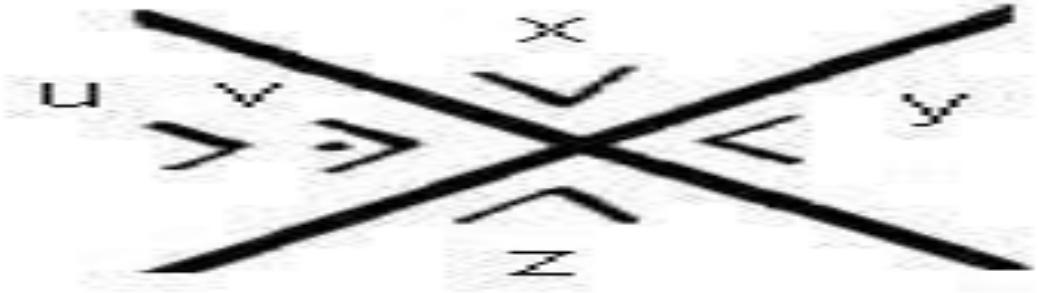






Шифр масонів





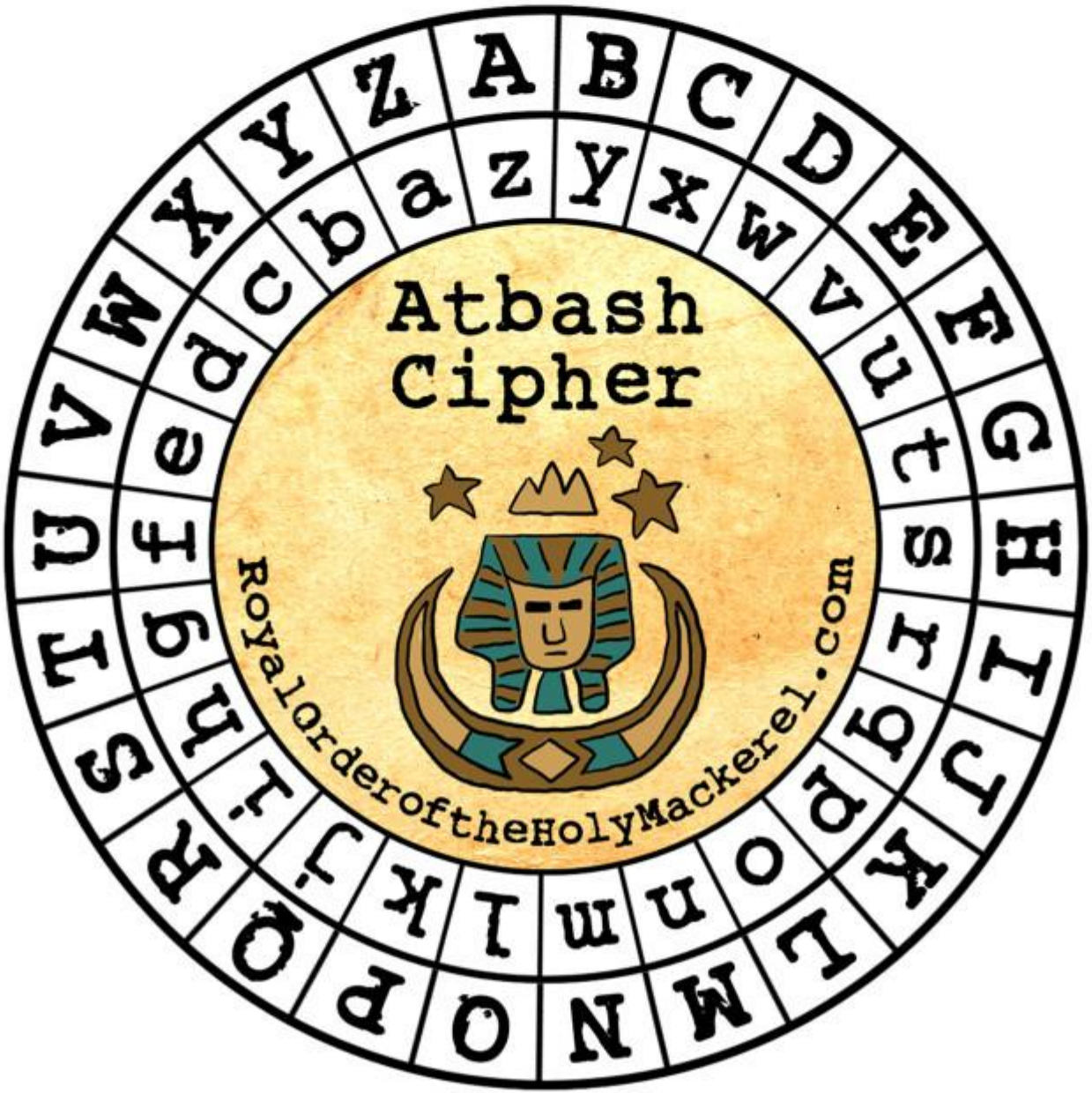
Атба́ш

- простий шифр підстановки для івриту.
- Даним алгоритмом зашифровано частину біблійних текстів.
- Правило шифрування полягає у заміні i-тої літери алфавиту літерою з номером n − i + 1, де n — кількість літер в алфавіті.
- Таким чином, перша буква алфавіту замінюється останньою, друга - передостанньою і так далі.

The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א


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

Застосування алгоритму Атбаш до українського алфавіту

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
Я	Ю	Ь	Щ	Ш	Ч	Ц	Х	Ф	Т	У
І	Ї	Й	К	Л	М	Н	О	П	Р	С
С	Р	П	О	Н	М	Л	К	Й	Ї	І
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
И	З	Ж	Є	Е	Д	Ґ	Г	В	Б	А

Шифр пар

- Ключем є фраза, яка містить половину літер абетки. В українській абетці можна змінити в текстах літеру “ї”, яка зрідка трапляється, на літеру “і”. Тоді використовується 32 літери.
- Ключова фраза повинна мати 16 різних літер (але може бути довшою, ніж 16 літер, тобто деякі літери можуть повторюватися).
- Послідовно записують різні літери, що є в ключі, у першому рядку. Під ним вписують послідовні літери абетки, пропускаючи вже наявні в ключі. Таким способом отримують відповідні пари літер.

Шифр пар з ключем “Реве та стогне Дніпр широкий”

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	Е	В	Т	А	С	О	Г	Н	Д	І	П	Ш	И	К	Й
Б	Г’	Є	Ж	З	Л	М	У	Ф	Х	Ц	Ч	Щ	Ь	Ю	Я

Шифрування за допомогою полібіанського квадрата

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	χ
χ	ν		φ	ι

Полібіанський квадрат для української мови

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

Перший метод шифрування

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

К	Р	И	П	Т	О	Г	Р	А	Ф	І	Я
Р	Ц	М	Х	Ш	Ф	З	Ц	Е	Ь	Н	В

θ	μ	β	φ	ρ
ε	ς	λ	o	δ
ψ	α	σ	ζ	υ
π		ι	ω	κ
η	ξ	χ	γ	τ

Другий метод шифрування.

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

Повідомлення перетворюються в координати по квадрату Полібія. Координати записуються вертикально

	З	А	Х	И	С	Т
Координати горизонтальні	2	1	5	2	4	4
Координати вертикальні	4	1	2	5	4	5

Другий метод шифрування.

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

Потім координати зчитуються за рядками

21 52 44 41 25 45

	З	А	Х	И	С	Т
Координати горизонтальні	2	1	5	2	4	4
Координати вертикальні	4	1	2	5	4	5

Другий метод шифрування.

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

Далі координати

21 52 44 41 25 45

Перетворюються в літери

Координати горизонтальні	**2**	**5**	**4**	**4**	**2**	**4**
Координати вертикальні	1	2	4	1	5	5
	Е	Х	С	О	И	Т

Третій метод шифрування по полібіанському квадрату

1. Беремо координати з 2-го методу, але записуємо їх без розбиття на пари

2152444125 45

2. Отримана послідовність циклічно зсувається на один крок праворуч

521524441254

3. Ця підгрупа знову розбивається на групи

52 15 24 44 12 54

Третій метод шифрування.

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я	`	.	_

Далі координати 12 52 44 41 25 45

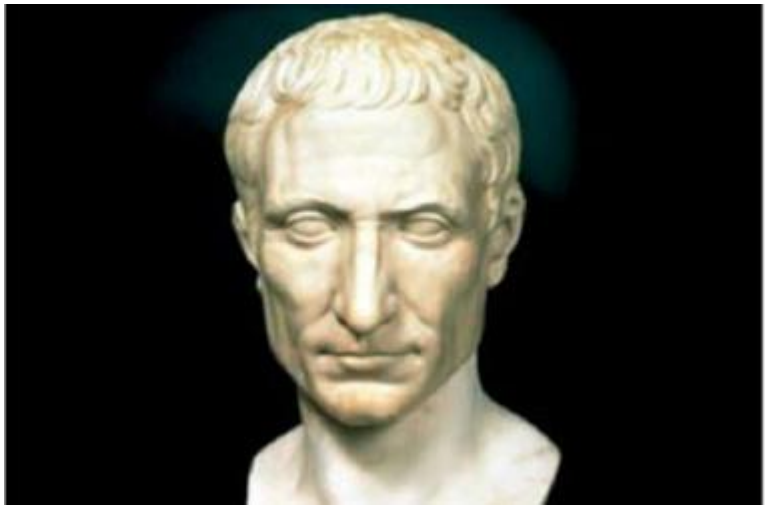
Перетворюються в літери

Координати горизонтальні	**5**	**1**	**2**	**4**	**1**	**5**
Координати вертикальні	2	5	4	4	2	4
	Х	Ґ	З	С	Б	4

Нумерація літер української абетки

L	N	L	N	L	N	L	N	L	N
А	00	Є	07	К	14	С	21	Ш	28
Б	01	Ж	08	Л	15	Т	22	Щ	29
В	02	З	09	М	16	У	23	Ь	30
Г	03	И	10	Н	17	Ф	24	Ю	31
Ґ	04	І	11	О	18	Х	25	Я	32
Д	05	Ї	12	П	19	Ц	26		
Е	06	Й	13	Р	20	Ч	27		

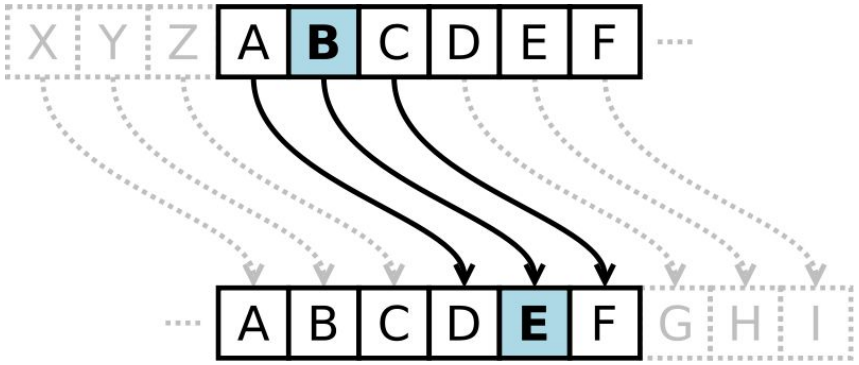
Шифрування методами Ґая Юлія Цезаря (100 – 44 до нашої ери)



Одноабеткова підстановка (K=3, m=26)

A	D	J	M	S	V
B	E	K	N	T	W
C	F	L	O	U	X
D	G	M	P	V	Y
E	H	N	Q	W	Z
F	I	O	R	X	A
G	J	P	S	Y	B
H	K	Q	T	Z	C
I	L	R	U		

- VENI VEDI VICI
- YHQL YHGL YLFL



Зашифруємо слово «ГОЛ», ключ 3

- Г -3; 3+3 =6 = Е
- О- 18; 3+18 = 21 = С
- Л – 15; 3+15 = 18 = О

- ГОЛ = ЕСО

Шифр Г’ая Юлія Цезаря (100-44 д.н.е.)

Афінний шифр Цезаря

- Шифрування відбувається за допомогою двох ключів a та b, які мають бути взаємно простими числами:

  $L = aN + b$,

  де N – номер літери відкритого тексту

  L - номер літери закритого тексту

Зашифруємо слово «ГОЛ», ключі 5,7

- Г -3; 5*3 +7 = 22 = Т
- О- 18; 5*18 + 7 = 97; 97-66 = 31 = Ю
- Л – 15; 5*15 +7 = 52; 52-33 = 19 = П

- ГОЛ = ТЮП

Шифр Цезаря з ключовим словом «БУЛЬДОЗЕРИСТ»

L	N	L	N	L	N	L	N	L	N
А	Б	Є	Е	К	Г	С	К	Ш	Ч
Б	У	Ж	Р	Л	Ґ	Т	М	Щ	Ш
В	Л	З	И	М	Є	У	Н	Ь	Щ
Г	Ь	И	С	Н	Ж	Ф	П	Ю	Ю
Ґ	Д	І	Т	О	І	Х	Ф	Я	Я
Д	О	Ї	А	П	Ї	Ц	Х		
Е	З	Й	В	Р	Й	Ч	Ц		

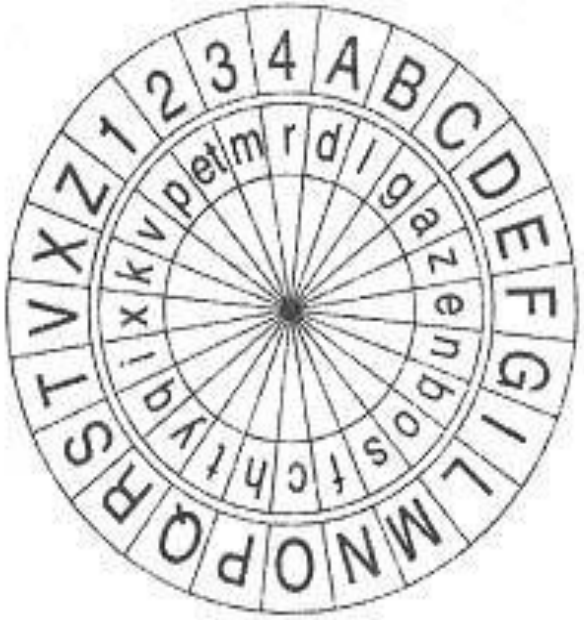
Питання 3

ШИФРИ СКЛАДНОЇ ЗАМІНИ

Шифри складної заміни (багатоабеткові шифри)

- Для шифрування кожного символу вихідного повідомлення застосовують свій шифр простої заміни
- Багатоабеткова підстановка послідовно та циклічно змінює абетку, що використовується
- При r-абетковій підстановці символ x_0 вихідного повідомлення замінюється символом y_0 з абетки B_0, символ x_1 - символом y_1 з абетки B_1, и так далі.
- Символ x_{r-1} замінюється символом y_{r-1} з абетки B_{r-1}, символ x_r замінюється символом y_r знову з абетки B_o, і т.д.

«Шифр королів» Леона Батісти Альберті (1404-1472)



Принцип дії диску Альберті

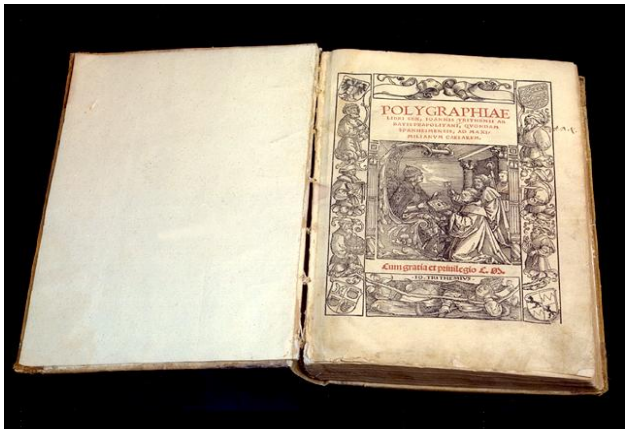
- Шифрувальний диск являв собою пару дисків різного діаметру
- Більший з них був нерухомим і мав 24 сектора, в якому були вписані 20 (з 24-х) літер латиниці за абеткою та 4 цифри – 1,2,3,4
- Менший диск був рухомим та складався з 24-х літер латиниці, записаних у довільному порядку

Шифр Альберті (XVI сторіччя)

- Процес шифрування полягав у надходженні літери відкритого тексту на зовнішньому диску та заміну цієї літери на відповідну (що стояла під нею) літеру шифрованого тексту.
- Після шифрування кількох слів зовнішній ключ зсовувався на один крок.
- Ключем цього шифру був порядок розташування літер на зовнішньому диску та його початкове розташування відносно зовнішнього диску.

Йоґан Тритеміус (Ґайденберг) (*Iohannes Trithemius) (1462-1516)*

- 1508 р. німецький абат написав роботу “Поліграфія”



Принцип дії таблиці Тритеміуса

- Запропонував таблицю, кожний рядок якої був зсунутий циклічно відносно іншого на одну позицію праворуч
- Перша літера шифрувалася літерою з першого рядка, друга – літерою з другого; третя – з третього і т.п.

HUNC CAVETO VIRUM

HWPF GFBMCZ FUEIB

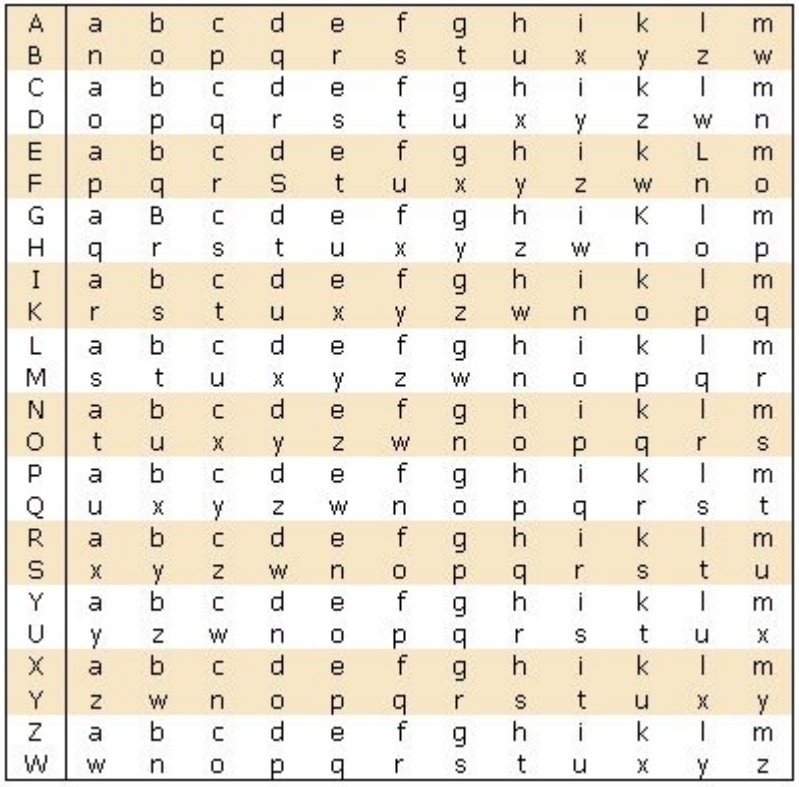
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Таблиця Джованні де ла Порта (1563 р.)

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

- Шифрування відбувається за допомогою гасла, яке пишеться над відкритим текстом
- Літера гасла визначає абетку (літери першого стовпця)

Шифрування



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

- Стережиться цієї людини
- HUNC CAVETO VIRUM
- DE LA PORTA
- XFHP YTMOGA FQEAS.

Принцип формування шифру Порти для української мови

1	А	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
	Б	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
2	В	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
	Г	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	н
3	Д	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
	Е	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	н	о
4	Є	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
	Ж	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	н	о	п

Блез де Віжінер (Blaise de Vigenère) (05.04.1523 – 19.02.1596

- $\Gamma = t_o t_1 t_2 \ldots t_{i-1} \ldots$
  $T_o = t_1 t_2 t_3 \ldots t_i \ldots$

  $T_ш = s_1 s_2 s_3 \ldots s_i \ldots$

HUNC CAVETO VIRUM…, покаткова P

YCHP ECUWZH IDAMG

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

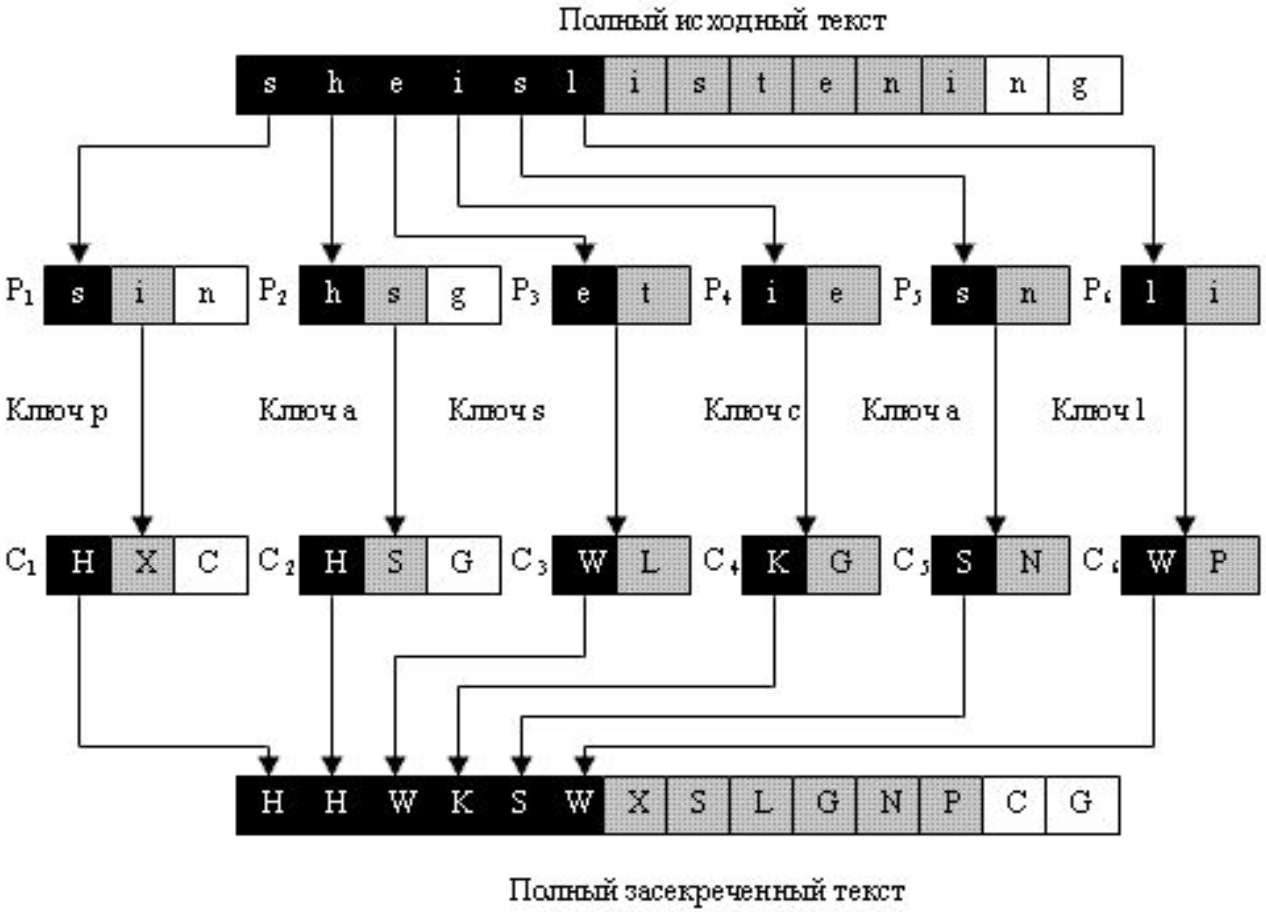
Шифр Віжінера

Ключ	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
0	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
1	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
2	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	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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

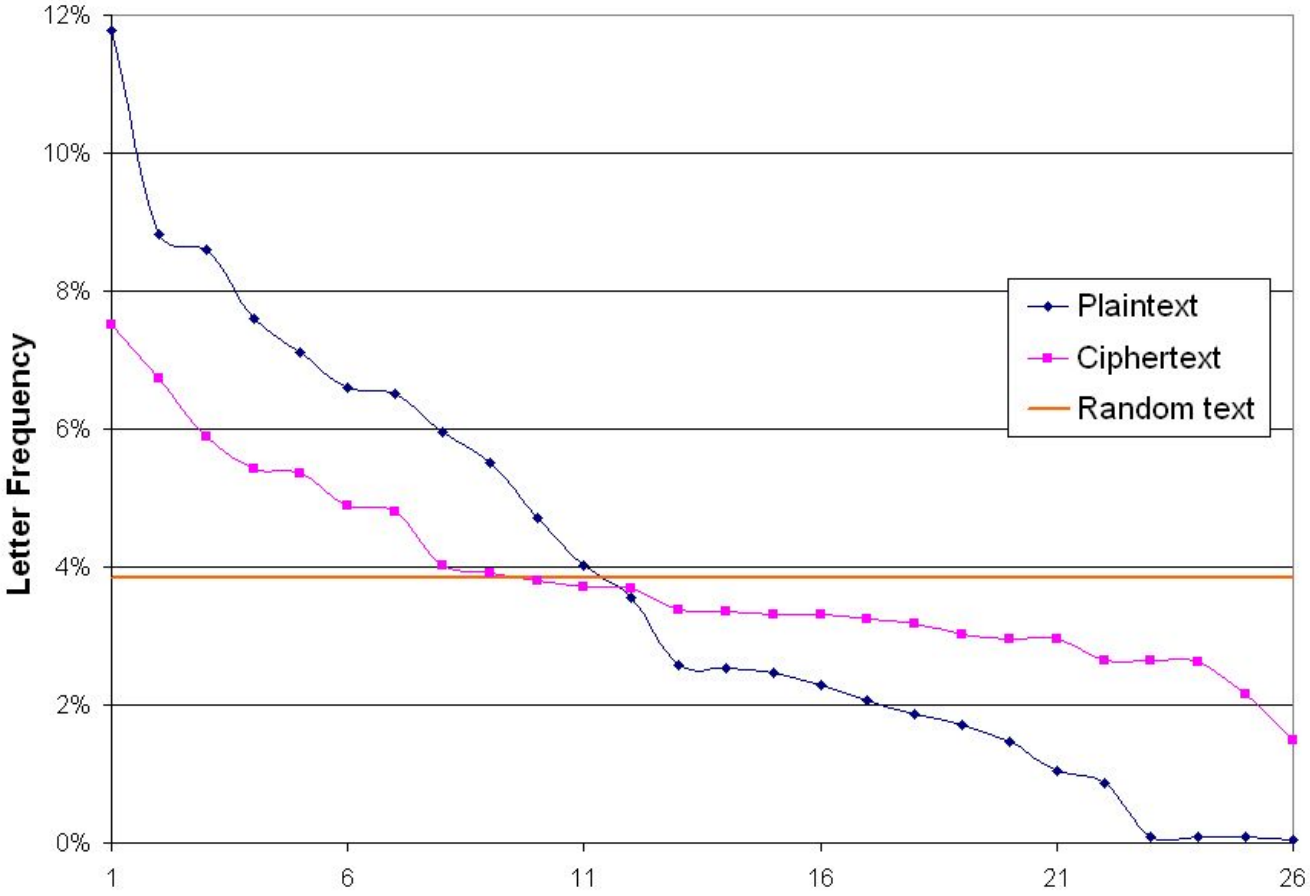
Шифрування методом Віжінера

М	і	с	т	о	Х	а	р	к	і	в
м	е	т	а	л	і	с	т	у	р	а
16	11	21	22	18	25	0	20	14	11	2
16	6	22	0	15	12	21	22	27	20	0
32	17	8	22	1	4	21	9	8	31	2
Я	н	Ж	т	б	Г`	с	з	ж	ю	в

Шифр Віжінера як комбінація адитивних шифрів



Шифр Віжінера “розмиває” частоти появи символів у тексті



Криптоаналіз шифра Віжінера

- 1. Знаходять довжину ключа

За допомогою тесту Kasiski криптоаналітик шукає повторні сегменти

- 2. Знаходять сам ключ

Шифр Бофора (гомофонічна заміна)

_	А	Е	К	Р	Т	Х
111	017	034	077	067	058	665
333	031	010	112	090	067	667
677	048	099	229	134	045	666
999	114	222	367	276	123	555
455	923	567	458	456	156	344

АТАКА ХАКЕРА ХЕКА

017058031077048111

665114112034067923

333667010229017

Шифр Хосе де Бронхорна графа де Гронсфельда

- поліалфавитний шифр заміни створений графом Гронсвельдом (керівником першої дешифровальної служби Німеччини) в XVII столітті. Шифр можна вважати удосконаленням шифру Цезаря (надійність) і Віжінера/Бофора (швидкість).

Ключ

- Довжина ключа (*K*) повинна бути рівною довжині вихідного тексту. Для цього циклічно записують ключ доти, доки його довжина не буде відповідати довжині вихідного тексту.

Шифрування

- Кожен символ M_i відкритого тексту M потрібно змістити вправо на K_i (відповідний символ ключа K) кроків.
- Або користуючись таблицею Гронсфельда ($T_{x\,y}$, де x — номер рядка, а y — номер стовпця, відлік ведеться з нуля): кожен символ C_i шифротексту C знаходиться на перетині стовпця y, перший символ якого дорівнює відповідному символу відкритого тексту M_i, і K_i-й (відповідній цифрі ключа) рядка — ($T_{Ki\,y}$)

Таблиця Гронсфельда

	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
0	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
1	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
2	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	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Дешифрування

- Кожний символ (C_i) зашифрованого тексту C потрібно змістити вліво на K_i (відповідний символ ключа K) кроків.
- Або користуючись таблицею Гронсфельда ($T_{x\,y}$, де x — номер рядка, а y — номер стовпця і відлік ведеться з нуля): потрібно в K_i (i-а цифра ключа K) рядку знайти символ, який дорівнює відповідному символу шифротексту ($T_{Ki,y} = C_i$), і перший элемент стовпця буде i-ий символ відкритого тексту.

Приклад шифрування методом Гронсфельда

- Нехай дано вихідний текст:

  C = «GRONSFELD»

і ключ:

- K = «2015»

- Довжина тексту — 9 символів, значить і довжина ключа також повинна дорівнювати 9 символам.

  K = «201520152»

Шифрування *K* = «201520152»

	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
0	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
1	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
2	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	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

- M_1 = «G».
- y = 6 (y — номер стовпця)
- $K_1 = 2$
- $C_1 = T_{26}$ = «I»
  C += «I» (C = «I»)
- M_2 = «R».
- y = 17
- $K_2 = 0$
- $C_2 = T_{06}$ = «R»
  C += «I» (C = «IR»)

Шифрування *K* = «201520152»

	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
0	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
1	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
2	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	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

- m_9 = «D»
- y = 3
- K_9 = 2
- $C_9 = T_{2\,3}$ = «F»
  C += «I» (C = «IRPSUFFQF»)
- Шифротекст (*C*) — «IRPSUFFQF»

Дешифрування

- C_1 = «I».
- x = K_1 = 2
- y = 6
- M += «G» (M = «G»)
- C_2 = «R»
- x = K_2 = 0
- y = 17
- M += «R» (M = «GR»)
- . . . . . .
- C_{10} = «H»
- x = K_9 = 2
- y = 3
- M += «F» (M = «GRONSFELD»)
- Дешифрований текст (*M*) — «GRONSFELD»

	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
0	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
1	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
2	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	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Френсіс Бекон (*Francis Bacon)* *(1561-1626)*

- Не повинні підлягати дешифруванню
- Не повинні займати багато часу для написання та читання
- Не мають викликати підозри

Автоключові шифри

- Щоб зрозуміти залежність ключа від позиції, розглянемо простий багатоалфавитний шифр, що має назву «автоключовий».
- Підключи утворюються автоматично в залежності від символів вихідного тексту в процесі шифрування
- У даному шифрі ключ – потік підключів, в якому кожний підключ використовується щоб зашифрувати відповідний символ у вихідному тексті.

Вибір підключів

- Перший підключ – визначене заздалегідь значення, таємно узгоджене відправником та отримувачем
- Другий підключ – значення першого символу вихідного тексту (між 0 та 32)
- Третій – і-те значення другого вихідного тексту і т.п.

Математичний опис автоключів

- $P = P_1\ P_2\ P_3 \ldots\ldots$
- $C = C_1\ C_2\ C_3 \ldots\ldots$
- $K = (k_1, P_1, P_2, P_3, \ldots\ldots)$
- Шифрування $C_i = (P_i + k_i) \bmod 33$
  Дешифрування $P_i = (C_i - k_i) \bmod 33$

«сьогодні іспит», початковий ключ «12»

	С	ь	о	г	о	д	н	і	і	с	п	и	т
Р	21	30	18	03	18	05	17	11	11	21	19	10	22
К	12	0	30	15	18	03	08	25	3	14	2	21	31
С	33-33=0	30	48-33=15	18	36-33=3	08	25	36-33=3	14	35-33=2	21	31	53-33=20
	а	**ь**	**л**	**0**	**г**	**ж**	**х**	**г**	**к**	**в**	**с**	**ю**	**р**

Криптоаналіз шифру «Автоключів»

ПЕРЕВАГИ

- Приховує статистику частоти окремого символу

НЕДОЛІКИ

- Перший ключ може бути лише одним з 32 значень

  (1, 2,……..31,32)

Шифр Хосе де Бронхорна графа де Гронсфельда (1734) ключ 1649

	і	н	ф	о	р	м	а	ц	і	я
№	11	17	24	18	20	16	00	26	11	32
К	01	06	04	09	01	06	04	09	01	06
№	12	23	28	27	21	22	04	35=2	12	38=5
Ш	ї	у	ш	ч	с	щ	Г’	в	ї	д

Шифр лорда Лайона Пфлейфера

- Винайдений 1854 року
- Використовується одночасне шифрування

  відразу двох літер відкритого тексту – “біграм”

Метод Плейфера – по_лк_ов_ни_кІ_ва_нБ_ог_ун

Ф	У	Т	Б	О	Л	Ь	Н
И	Й	А	В	Г	Д	Е	Є
Ж	З	І	Ї	К	М	П	Р
С	Х	Ц	Ч	Ш	Щ	Ю	Я

П	О	Л	К	О	В
К	Ь	О	М	Б	Г
Н	И	К	І	В	А
Ф	Є	М	Ї	Г	В
Н	Б	О	Г	У	Н
Ф	О	Г	К	Т	Ф

Сер **Чарльз Вітстон** (Sir Charles Wheatstone)

(1802 – 1875)

- Удосконалив шифр Плейфера, запропонувавши використовувати не один, а два квадрати

Подвійний квадрат Вітстона:

пр ил ет аю _ш ес то го

пе ов щн фм еш рф жб дц

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Механічний пристрій Вітстона

- Стрілки пов`язані між собою шестирінкою
- Спочатку велика та мала стрілки встановлювалися на 12.00
- Відкритий текст великою стрілкою, закритий – маленькою
- Подвійних літер не повинно бути

Jean Guillaume Auguste Victor François Hubert Kerckhoff (19.01.1835 – 09.08.1903)

1883 року у роботі «Військова криптографія» сформулював «принципи Керкхоффса»

Принципи Керкхоффса

1. Система шифрування має бути такою, щоб її було неможливо фізично, якщо не математично розкрити
2. Систему шифрування не потрібно тримати в таємниці: потрапляння системи до рук ворога не має спричинити незручностей
3. Зберігання та передача ключа мають здійснюватися без паперових записів, кореспонденти повинні мати змогу змінювати ключ на власний розсуд
4. Система має бути придатною для передачі телеграфом
5. Система має бути мобільною; робота з нею не повинна потребувати участі кількох осіб одночасно
6. Система має бути простою у використанні, не вимагала значного навантаження розуму або дотримання великої кількості правил

Принцип Керкхоффса

Інформаційна безпека та сталість методу шифрування базується саме на таємності ключа для шифрування, але не на таємності обраного криптометоду

Gilbert Sandford Vernam

Г`ілберт Сендфорд Вернам

(03.04.1890 – 07.02.1960)

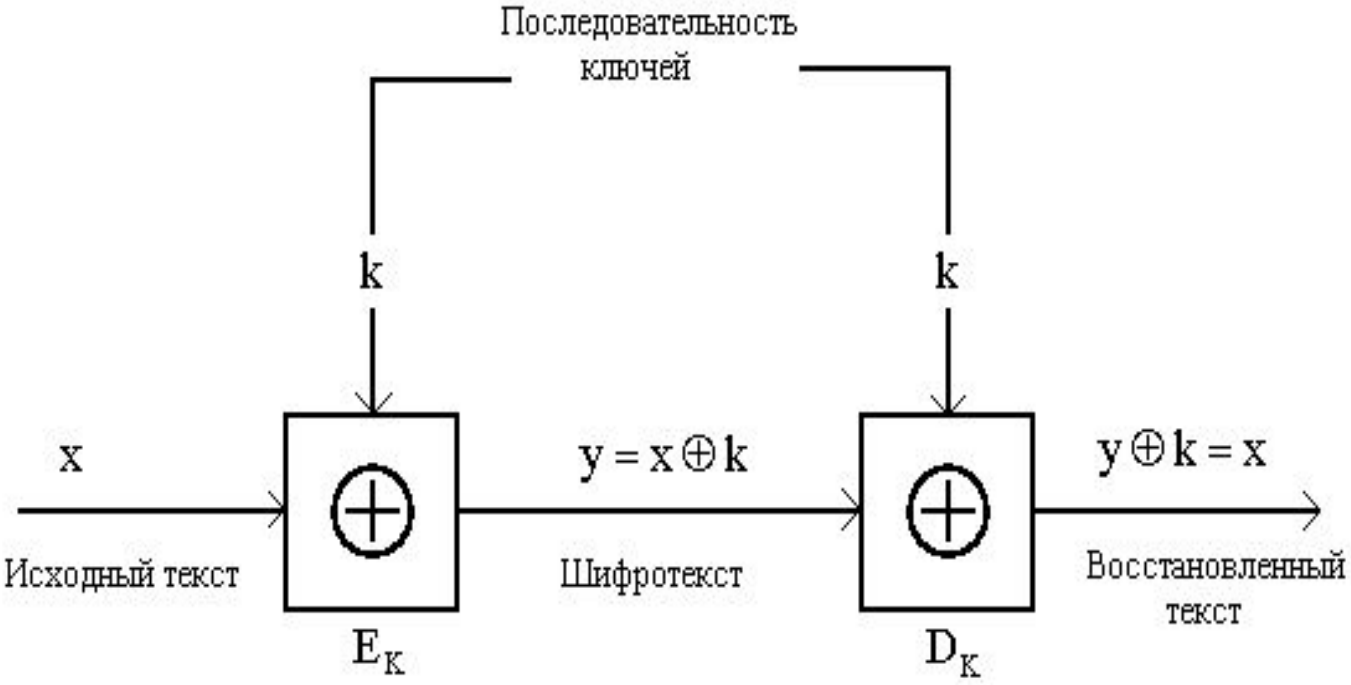
Vrrnam Cipher у 1918 р.

Шифр Г`ільберта Вернама (одноразового блокноту)

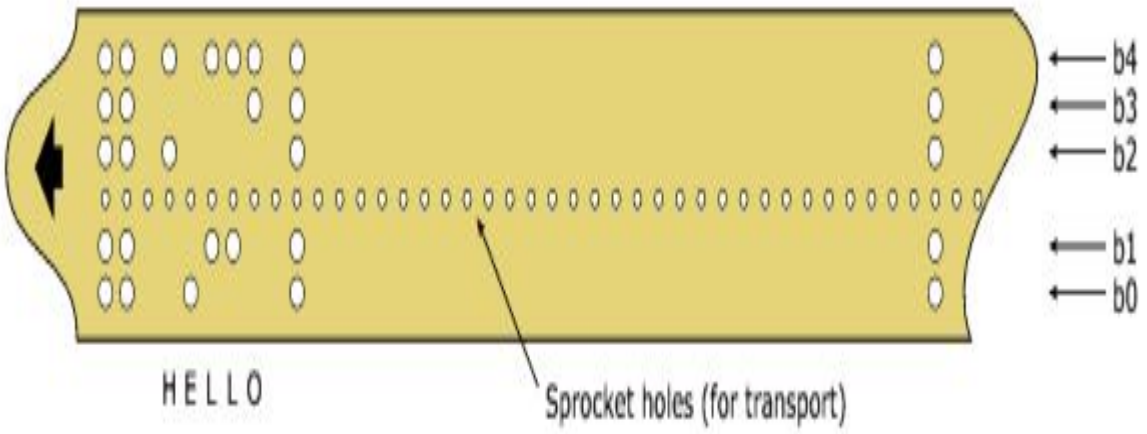
- Для утворення шифртексту повідомлення об'єднується операцією XOR з ключем (названим одноразовим блокнотом або шифроблокнотом). При цьому ключ повинен володіти трьома критично важливими властивостями:

- Бути справді випадковим;
- Збігатися з розміром з заданим відкритим текстом;
- Застосовуватися тільки один раз.

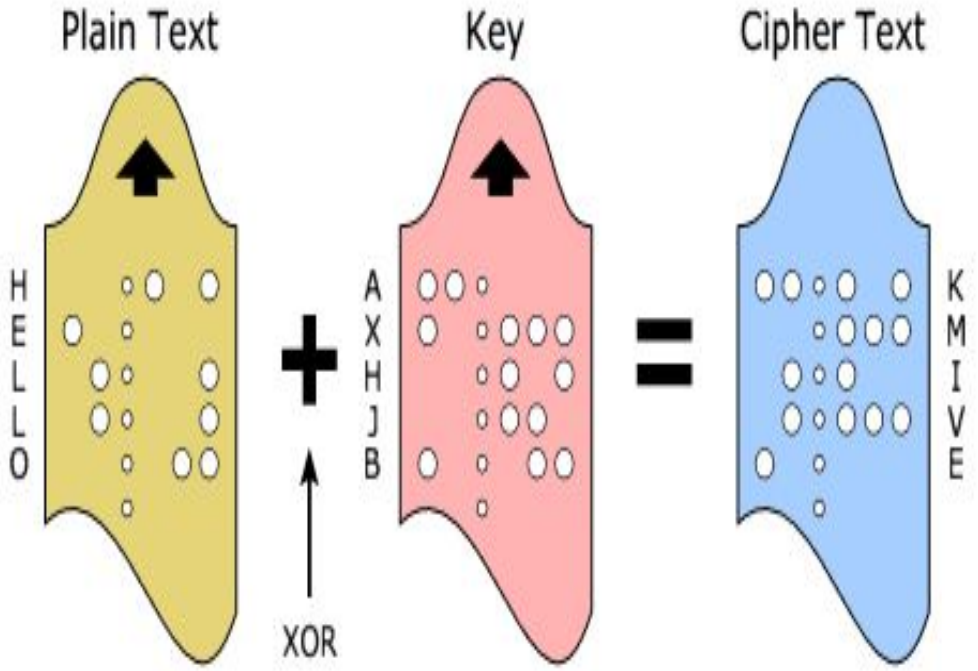
Шифрування та розшифрування методом Вернама



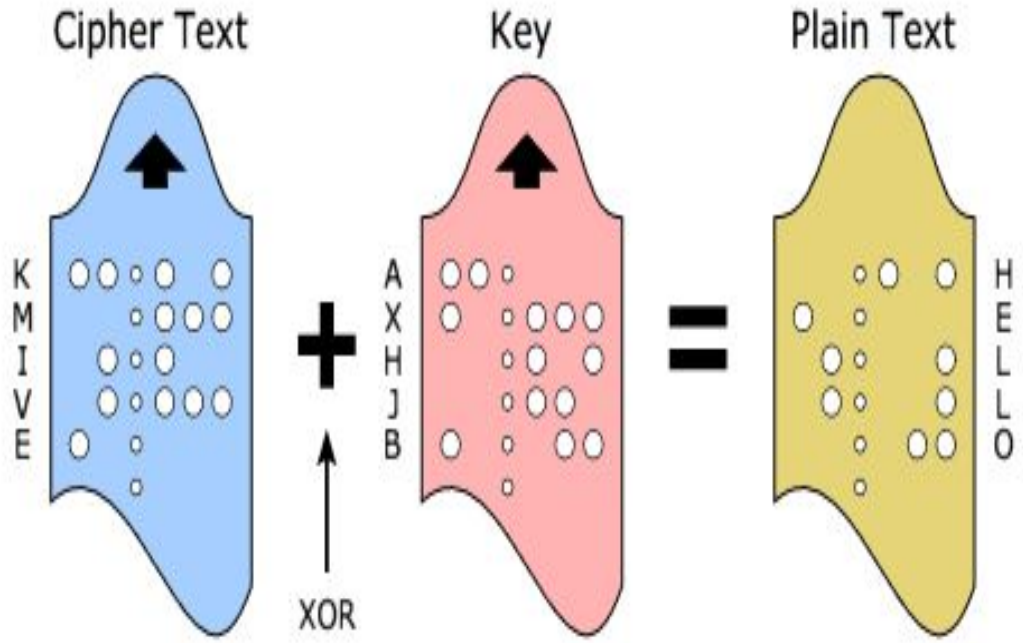
Приклад слова «HELLO» в одноразовому блокноті



Vernam Cipher зашифрування



Vernam Cipher розшифрування



Багатосимвольні підстановки зі стисненням

- Маємо проіндексований словниковий вектор розмірності N, кожний елемент якого – текстовий рядок довжиною від 1 до К символів (зазвичай N = 1024, К= 3)
- Елементами вектора є: літери (від А до Я), цифри (від 0 до 9), розділові знаки (,.’:?), словосполучення з 2-х та 3-х літер, що зустрічаються найчастіше.

Приклад словарного вектора

1	2	3	….	254	255	256	…
?	К	ПОМ	…	Я	ЧИ	КО	…
367	368	369	370	….	512	513	514
Б	‘	ЗО	ВІД	….	КА	КУ	9
…	880	881	882	883	…	920	921
…	ПРИ	МУ	ТЬ	П	….	ТУ	Г’
922	923	….	1020	1021	1022	1023	1024
ЛЕ	ЩО	-	ТІР	ПІД	1	НАД	АБ

Процедура шифрування

- З вихідного тексту виділяється лексема розміром в K символів.
- Якщо така лексема є в словарному векторі, то індекс цієї лексеми записується до тексту шифровки.
- Якщо такої лексеми немає в словарному векторі, то розмір лексеми зменшується на 1 та відбувається вже пошук нової, скороченої, лексеми.
- Ця дія повторюється доти, доки не знайдеться потрібна лексема, або поки довжина лексеми не дорівнюватиме 1.

Приклад застосування багатосимвольної підстановки зі стисненням

Вихідний текст: Кому п`ятірку?

Шифрування: ко- 256; му-881; п – 883;

‘ – 368; я – 254; тір – 1020; ку – 513; ? – 1

Шифротекст:

256.881.883.368.254.1020.513.1

Питання 4

КОМБІНОВАНІ ШИФРИ

Шифр ADFGVX (шифр першої світової війни)

- У шифру використано комбінацію двох способів шифрування: підстановку та перестановку.
- Спочатку кожну літеру латинської абетки або цифру від 0 до 9 шифровано блоками довжини 2, які складаються з літер A, D, F, G, V, X на підставі таблиці розміру 6 x 6.
- Потім до отриманого криптотексту застосовують шифр перестановки – матричний шифр з ключем.

Шифр ADFGVX

Таблиця підстановки

	A	D	F	G	V	X
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	0	J	D
G	5	S	I	Y	H	U
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

Шифрування фрази

- One day - (якось)
- ADFAXAFXDGGG

FDFAXAFXDGGG

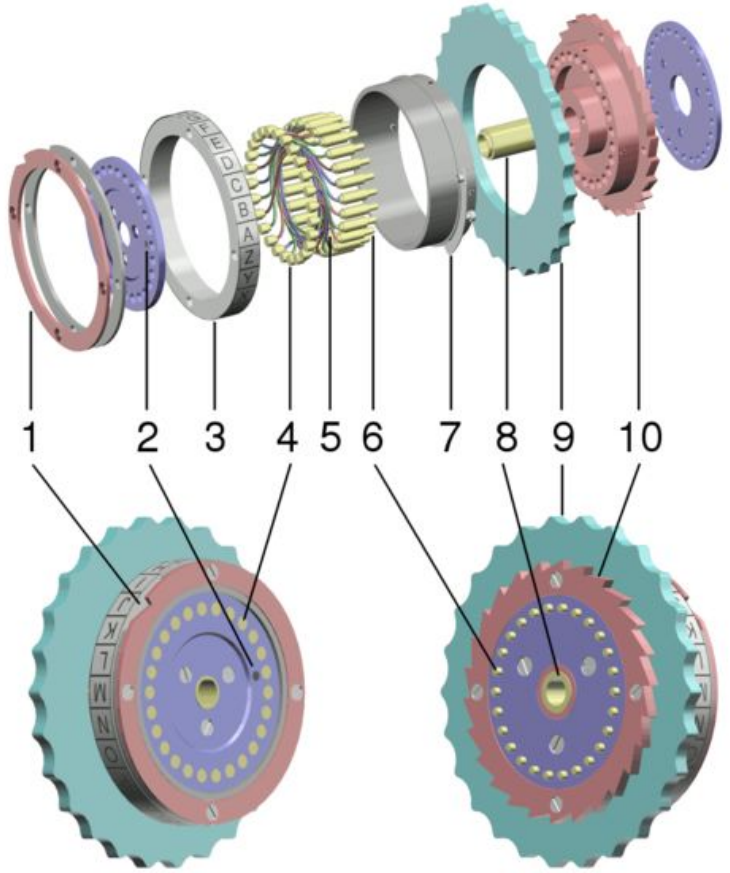
Матричний шифр з ключем GARDEN					
G	**A**	**R**	**D**	**E**	**N**
4	1	6	2	3	5
F	D	F	A	X	A
F	X	D	G	G	G

КРИПТОГРАМА

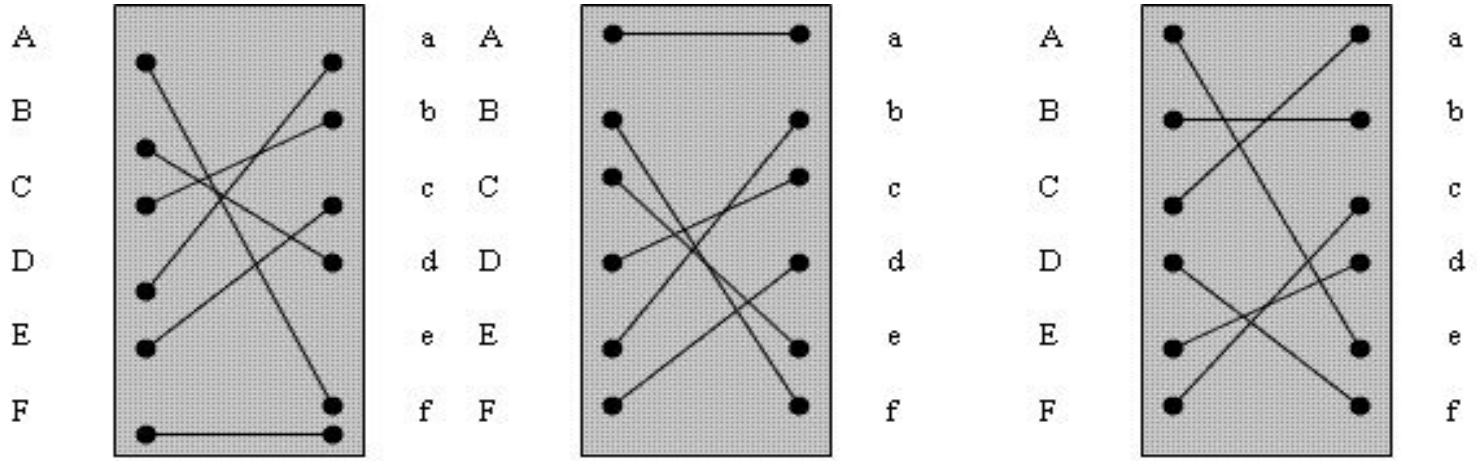
- DXAGXGFFAGFD

Жорж-Жан Панвєн у 1918 р., під час німецького наступу на Париж , втративши 15 кг ваги, за кілька днів розкрив шифр **ADFGVX**

Ені́гма (*Enigma*) — шифрувальна машина часів 2-ї світової війни



Роторні шифри



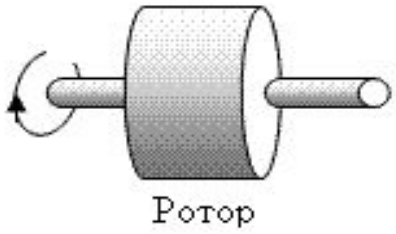
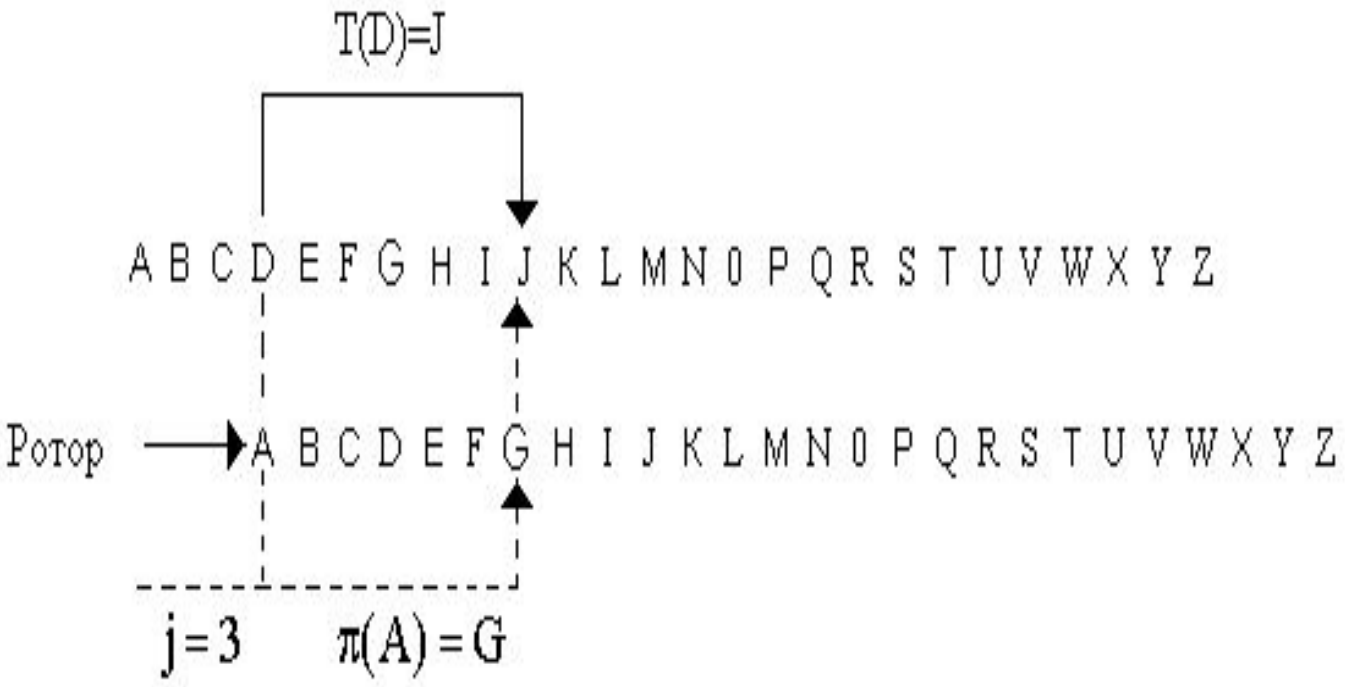
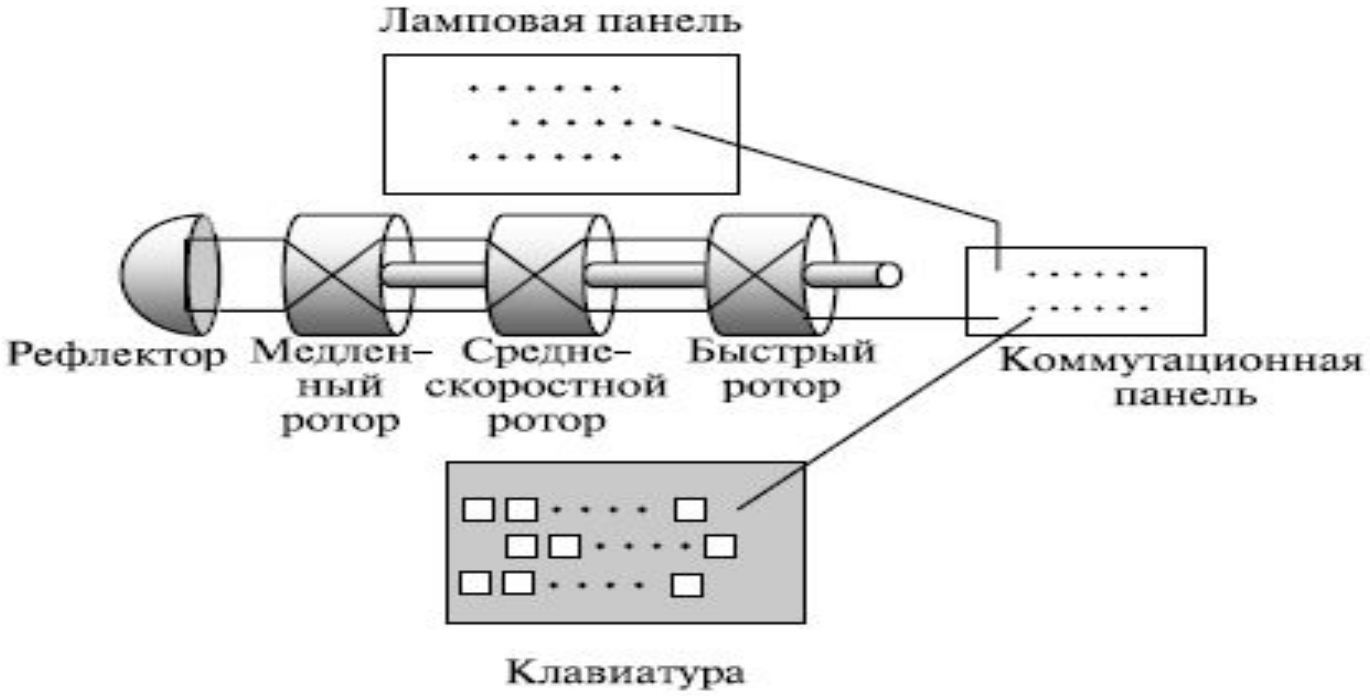


Схема формування підстановки при зсуві ротора J =3

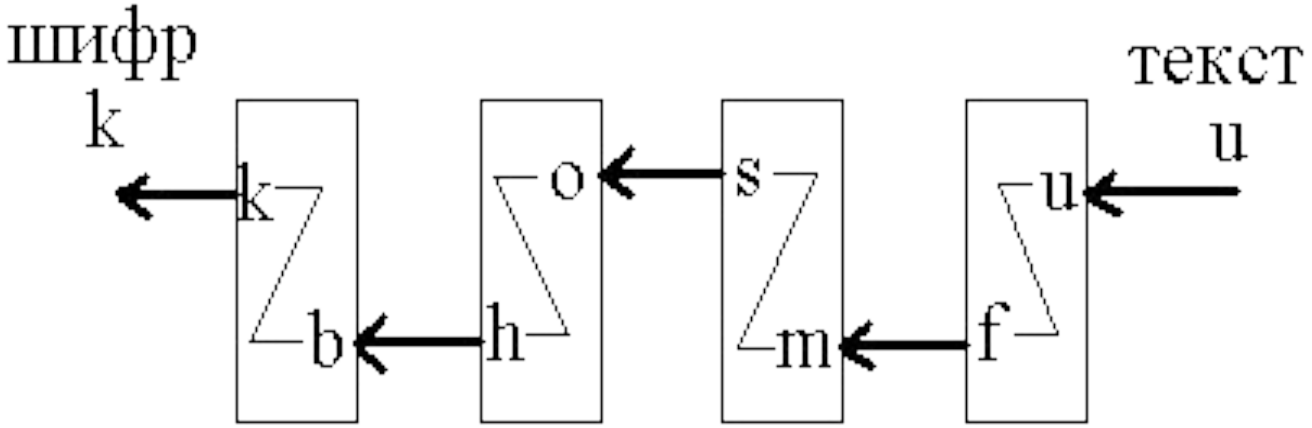


$T\,(D) = C^{3}pC^{-3}\,(D) = C^{3}\,p\,(A) = C^{3}\,(G) =$ J.

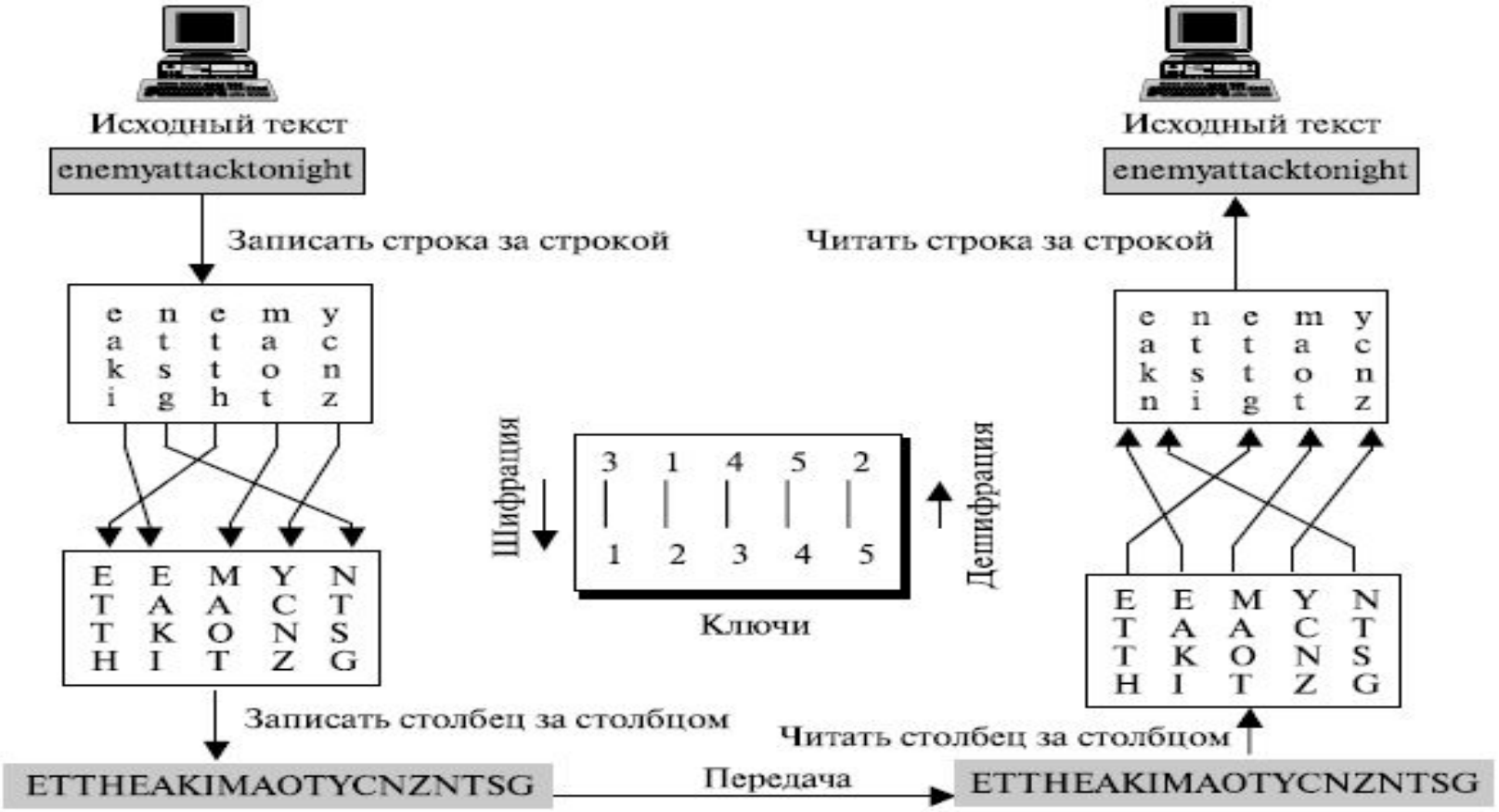
Структурна схема Енігми



Принцип дії Енігма



Ворожа атака сьогодні ввечері



Enemy attacks to nightz