ЛЕКЦІЯ 2

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Класичні шифри та їх криптоаналіз

План

1. Шифри простої заміни
2. Шифри перестановки
3. Поліграмні шифри
4. Поліалфавітні шифри
5. Криптоаналіз класичних шифрів

Умовні позначення

M	повідомлення
P	відкритий текст
C	шифротекст
K	ключ
E	функція шифрування
D	функція дешифрування
n	кількість літер повідомлення
m	загальна кількість літер алфавіту

1. Шифри простої заміни

Шифр Цезаря

Ключ:

число К – від 1 до 25

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. Шифри простої заміни

Шифрування:

літеру тексту замінюємо на літеру алфавіту на К позицій праворуч. Зациклюємо алфавіт, ігноруємо коми та пробіли

$$C_i = E_k(M_i) = (M_i + K) \bmod m$$

Дешифрування:

літеру зашифрованого тексту замінюємо на літеру розташовану в алфавіті на К позицій ліворуч. Зациклюємо алфавіт, ігноруємо коми та пробіли

$$M_i = D_k(C_i) = (C_i - K) \bmod m$$

1. Шифри простої заміни

Приклад 1.1:

Ключ: K = 3

Повідомлення: CAESAR

Шифруємо: C=2+3=5=F A=0+3=3=D E=4+3=7=H

S=18+3=21=V A=0+3=3=D R=17+3=20=U

Шифротекст: FDHVDU

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. Шифри простої заміни

Квадрат Полібія

Ключ: розташування літер в квадраті

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

1. Шифри простої заміни

Шифрування:

літера, що зашифровується, замінюється на її координати в квадраті

Дешифрування:

пара літер однозначно визначає літеру в квадраті

1. Шифри простої заміни

Приклад 1.2:

Повідомлення: CRYPTO

Шифруємо: AC DB ED CE DD CD

Шифротекст: ACDBEDCEDDCD

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

2. Шифри перестановки

Скитала

В якості носія повідомлення застосовувалася вузька та довга стрічка пергаменту (папірусу)

Ключ: діаметр палиці

2. Шифри перестановки

Шифрування:

стрічка намотувалася на палицю у вигляді спіралі і на неї вздовж палиці наносився текст секретного повідомлення. Після цього стрічка змотувалася і посилалася адресату

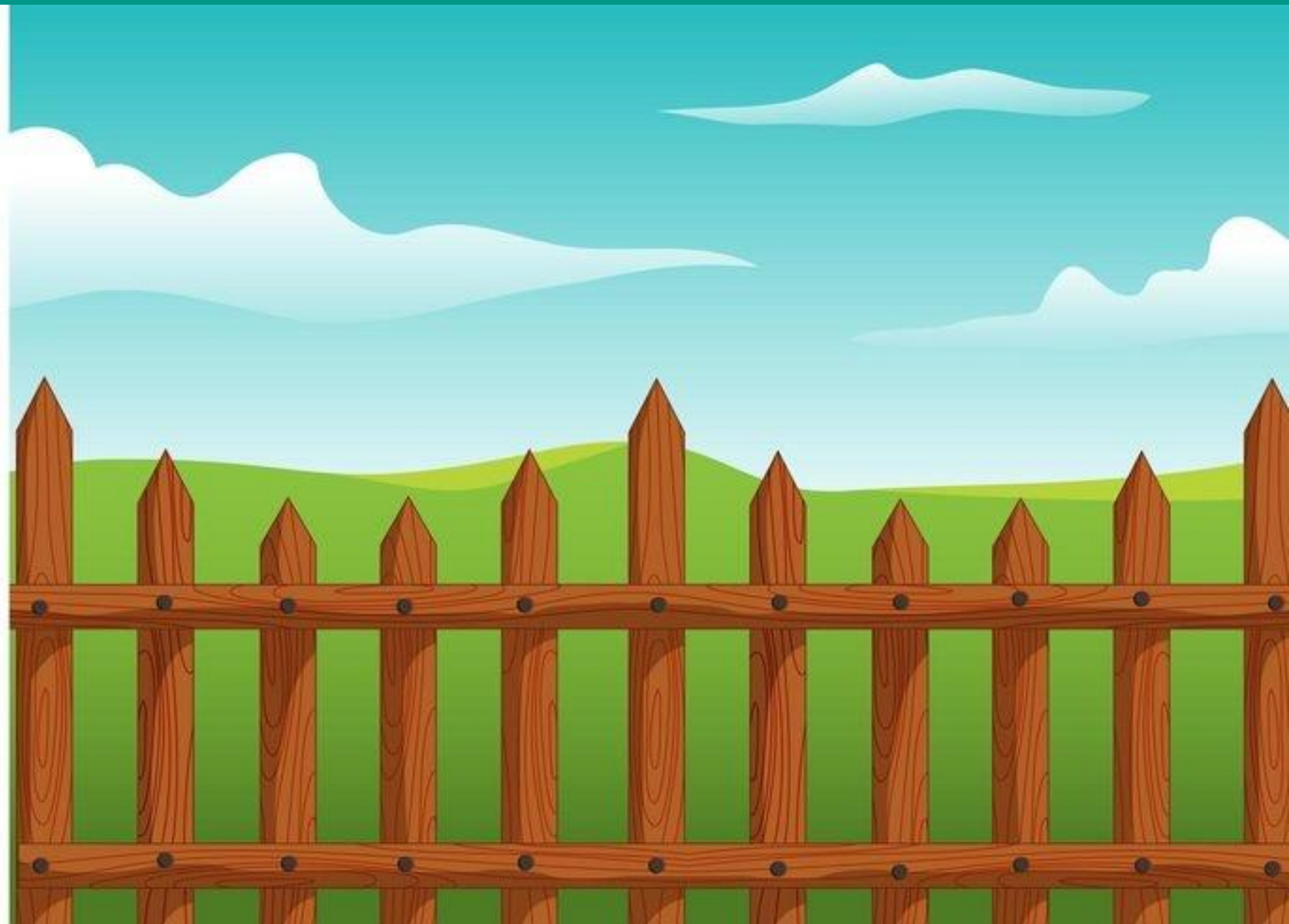
Дешифрування:

використовувалася палиця такого самого діаметру або дешифрувальний пристрій «Антискитала» (винайшов Аристотель – запропонував використовувати конусоподібний «спис»)

2. Шифри перестановки

Шифр частоколу

Ключ: ціле число К – висота частоколу



2. Шифри перестановки

Шифрування:

літери повідомлення записуємо як степені (їх кількість висота частоколу), а потім записуємо літери в степенях по рядках зверху донизу

Дешифрування:

підраховуємо літери, ділимо на ключ, записуємо літери по К штук (К - ключ) в порядку зверху донизу

2. Шифри перестановки

Приклад 2.1:

Ключ: К = 3.

Повідомлення: я отримаю іспит автоматом

Шифруємо:

	т	м	і	и	в	м	о
о	и	ю	п	а	о	т	
я	р	а	с	т	т	а	м

Шифротекст: тміивмооиюпаотярасттам

3. Поліграмні шифри

Шифр Плейфера

Шифр Плейфера є біграмним, тобто текст повідомлення розбивається на біграми (групи з двох символів)

Ключ: секретне слово та розташування літер у матриці

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

Клітинки матриці заповнюються літерами ключового слова (виключаючи літери, що повторюються), в решту комірок записуються літери алфавіту, які не зустрічаються в ключовому слові, по порядку

3. Поліграмні шифри

Шифрування:

дві літери біграми відповідають кутам прямокутника в ключовій матриці. Визначаються положення кутів цього прямокутника відносно один одного. Після чого кожну біграму зашифровують згідно правил (див. далі)

Дешифрування:

за правилами шифрування, тільки циклічно зміщуємо на крок вліво (вгору)

3. Поліграмні шифри

Правила шифрування біграм

1. Якщо дві літери біграми однакові – додаємо після першого символу «Х», зашифровуємо нову пару літер

2. Якщо літери біграми знаходяться в різних стовпцях і різних рядках – замінюємо їх на літери, що знаходяться в тих самих рядках (стовпцях), але відповідно в інших кутах прямокутника

3. Якщо літери біграми зустрічаються в одному рядку – замінюємо їх на літери, розташовані в найближчих стовпцях праворуч від відповідних літер. Якщо літера остання у рядку, то вона замінюється на перший символ цього ж рядка

4. Якщо літери біграми зустрічаються в одному стовпці – перетворюємо їх в літери того ж стовпця, що знаходяться безпосередньо під ними. Якщо літера є нижньою в стовпці – вона замінюється на першу літеру цього ж стовпчика

3. Поліграмні шифри

Приклад 3.1:

Повідомлення: HIDE THE GOLD IN THE TREE STUMP

Ключ: PLAYFAIR EXAMPLE

Шифрування: HI DE TH EG OL DI NT HE TR EX ES TU MP

Шифротекст: BM ND ZB XD KY BE JV DM UI XM MN UV IF

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

3. Поліграмні шифри

Шифр Хілла

Літери алфавіту нумеруються в порядку їхнього зростання від 0 до 25. Всі операції з літерами відбуваються по модулю 26

Ключ: матриця $K(d \times d)$, елементи якої числа від 0 до 25, det $K \neq 0$, $d \geq 2$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad Mod\ 26$$

Літери повідомлення перетворюють в набір цифр, потім розбивають на d-розмірні стовпчики

3. Поліграмні шифри

Шифрування:

$$K \cdot P_i = C_i \ mod \ m,$$

де C_i – набір цифр, елементи яких числа від 0 до 25 ⇨ перетворюються на літери шифротексту

Дешифрування:

$$P = K^{-1} \cdot C_i \ mod \ m,$$

де K^{-1}– обернена матриця (алгоритм пошуку оберненої матриці)

3. Поліграмні шифри

Приклад 3.2:

Повідомлення: HELP

Ключ: $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$

Шифрування: $K \cdot P_i = C_i \ mod\ 26$

Шифротекст: HIAT

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}, \det K = 6 - 15 = 9 \neq 0$$

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \qquad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

$$K \cdot P_1 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 33 \\ 34 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = HI$$

$$K \cdot P_2 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 78 \\ 97 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} = AT$$

3. Поліграмні шифри

Приклад 3.3:

Повідомлення: HIAT

Ключ: $K^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$

Дешифрування: $P = K^{-1} \cdot C_i \ mod\ 26$

Відкритий текст: HELP

$$K^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$$

$$K^{-1} \cdot P_1 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 241 \\ 212 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix} = HE$$

$$K^{-1} \cdot P_2 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 323 \\ 171 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 15 \end{pmatrix} = LP$$

4. Поліалфавітні шифри

Шифр Віженера

Ключ: ключове слово K, якщо воно менше за повідомлення, то воно циклічно повторюється

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

4. Поліалфавітні шифри

Шифрування:

кожна літера повідомлення замінюється на літеру, що знаходиться на перетині літер першого рядка (алфавіт повідомлення) і першого стовпчика (алфавіт ключа) в таблиці Віженера

Дешифрування:

потрібно відшукати у першому стовпчику літеру ключа і за літерами шифротексту визначити, в якому стовпчику зверху знаходиться літера відкритого тексту

4. Поліалфавітні шифри

Приклад 4.1:

Повідомлення: PURPLE

Ключ: SMART

Шифротекст: HGRGEW

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

4. Поліалфавітні шифри

Якщо літерам поставити у відповідність їх номери у алфавіті, то шифр Віженера можна записати у вигляді формул:

Шифрування:

$$C_i = E_k(M_i) = (M_i + K_i) \bmod m$$

Дешифрування:

$$M_i = D_k(C_i) = (C_i - K_i) \bmod m$$

4. Поліалфавітні шифри

Приклад 4.2:

Повідомлення: ATTACKATDAWN

Ключ: LEMON

Шифротекст: LXFOPVEFRNHR

A	T	T	A	C	K	A	T	D	A	W	N
L	E	M	O	N	L	E	M	O	N	L	E
0	19	19	0	2	10	0	19	3	0	22	13
11	4	12	14	13	11	4	12	14	13	11	4
11	23	5	14	15	21	4	5	17	13	7	17
L	X	F	O	P	V	E	F	R	N	H	R

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

5. Криптоаналіз класичних шифрів

Частота символу у повідомленні дорівнює кількості його появи у тексті, поділеній на загальну кількість літер тексту

Для кожної мови справедливо наступне: у досить довгих текстах кожна літера зустрічається із приблизно однаковою частотою, залежно від самої літери і незалежно від конкретного тексту

5. Криптоаналіз класичних шифрів

Літера з найбільшою частотою в шифротексті буде замінюватися на літеру з найбільшою частотою у мові. А кількість позицій між ними буде визначати довжину ключа

Українська мова						Англійська мова					
А	0,072	**Ї**	0,006	**У**	0,04	**A**	0,082	**J**	0,002	**S**	0,063
Б	0,017	**Й**	0,008	**Ф**	0,001	**B**	0,015	**K**	0,008	**T**	0,091
В	0,052	**К**	0,035	**Х**	0,012	**C**	0,028	**L**	0,040	**U**	0,028
Г, Ґ	0,016	**Л**	0,036	**Ц**	0,006	**D**	0,043	**M**	0,024	**V**	0,010
Д	0,035	**М**	0,031	**Ч**	0,018	**E**	**0,127**	**N**	0,067	**W**	0,023
Е	0,017	**Н**	0,065	**Ш**	0,012	**F**	0,022	**O**	0,075	**X**	0,001
Є	0,008	**О**	**0,094**	**Щ**	0,001	**G**	0,020	**P**	0,019	**Y**	0,020
Ж	0,009	**П**	0,029	**Ь**	0,029	**H**	0,061	**Q**	0,001	**Z**	0,001
З	0,023	**Р**	0,047	**Ю**	0,004	**I**	0,070	**R**	0,0060		
И	0,061	**С**	0,041	**Я**	0,029						
І	0,057	**Т**	0,055								

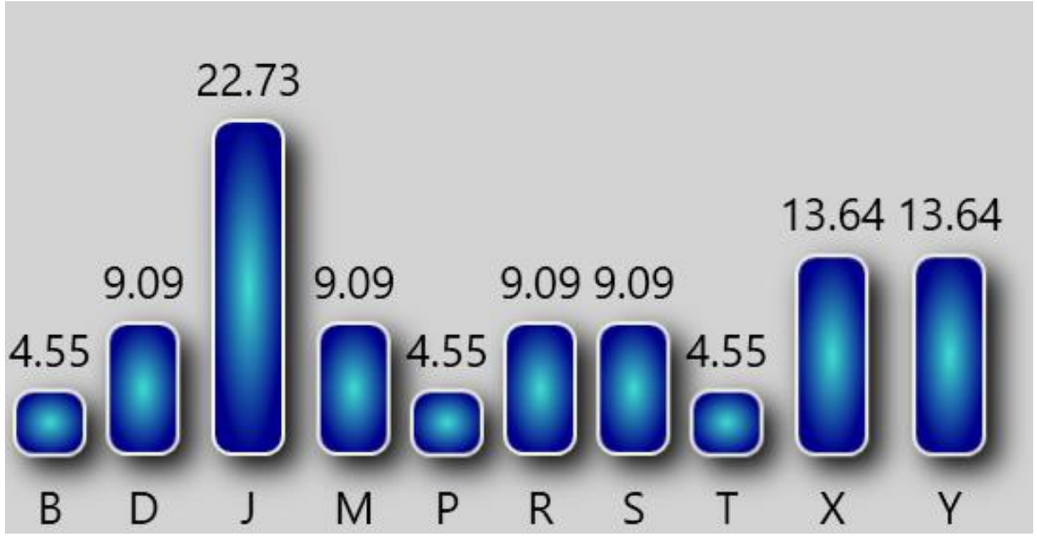
5. Криптоаналіз класичних шифрів

Приклад 5.1:

Шифротекст: YMJ JSJRD PSTBX YMJ XDXYJR

Знаючи, що текст зашифрований за допомогою шифру Цезаря, знайдемо частоту кожної літери шифротексту та визначимо літеру з найбільшою частотою – це J

Оскільки в англійській мові найчастіше зустрічається літера E, то припускаємо, що її було замінено на J



5. Криптоаналіз класичних шифрів

Ключ: Обчислимо ключ як відстань між E та J: 9 – 4 = 5

Спробуємо відновити відкритий текст з ключем 5.
Відкритий текст: THE ENEMY KNOWS THE SYSTEM

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

5. Криптоаналіз класичних шифрів

Метод Казіскі

Повторення літер в ключі разом з повторенням літер у відкритому тексті дає повторення літер у шифротексті

Відстань між повтореннями в шифротексту будуть рівні або кратні довжині (періоду) ключа

5. Криптоаналіз класичних шифрів

Визначення довжини ключа методом Казіскі

1. Знайдемо у шифротексті однакові відрізки довжиною не менше трьох символів (зауважимо, що такі однакові відрізки можуть з’явитися в тексті з досить малою ймовірністю)

2. Визначимо відстань між стартовими позиціями відрізків у шифротексті

3. Візьмемо один із спільних дільників цих відстаней в якості довжини ключа

5. Криптоаналіз класичних шифрів

Приклад 5.2:

Шифротекст:

QPWK ALVRXC QZIKGRB PFAEOMFL JMSD ZVDHXC XJ YEBIMTRQW NMEAI ZRVKC VKVLXN EIC FZPZCZZH KM LVZV ZIZR RQWDKECH OS NYXXL SPMYKV QXJT DCIOMEE XDQV SRXLRLKZH OV

	Дільники
Відстань між RQW 40	2, 4, 5, 8, 10
Відстань між IZR 30	2, 3, 5, 6, 10

Ймовірна довжина ключа: 5

5. Криптоаналіз класичних шифрів

Запишемо шифротекст у таблицю з 5 стовпців.

В кожному стовпці знайдемо літери, що найчастіше зустрічаються

Кожен стовпець шифрувався своєю величиною зсуву, яку можна знайти, використовуючи частотний аналіз

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

5. Криптоаналіз класичних шифрів

2-ий стовпець	Z	25 – 4 mod 26 = 21	V
4-ий стовпець	V	21 – 4 mod 26 = 17	R
5-ий стовпець	C	2 – 4 mod 26 = 24	Y
1-ий стовпець	X I	23 – 4 mod 26 = 19 8 – 4 mod 26 = 4	T E
3-ий стовпець	Очевидно, що третя літера E		

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

5. Криптоаналіз класичних шифрів

Ключ: EVERY

Відновимо переше слово:

Q = 16, E = 4:

16 – 4 mod 26 = 12 ⇨ M

P = 15, V = 21:

15 – 21 mod 26 = 20 ⇨ U

W = 22, E = 4:

22 – 4 mod 26 = 18 ⇨ S

K = 10, R = 17:

10 – 17 mod 26 = 19 ⇨ T

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

5. Криптоаналіз класичних шифрів

Відкритий текст:

MUST CHANGE MEETING LOCATION FROM BRIDGE TO UNDERPASS SINCE ENEMY AGENTS BELIEVED TO HAVE BEEN ASSIGNED TO WATCH BRIDGE STOP MEETING TIME UNCHANGED XX

	M	U	S	T	C
	H	A	N	G	E
	M	E	E	T	I
	N	G	L	O	C
	A	T	I	O	N
	F	R	O	M	B
	R	I	D	G	E
	T	O	U	N	D
	E	R	P	A	S
	S	S	I	N	C
	E	E	N	E	M
	Y	A	G	E	N
	T	S	A	R	E
	B	E	L	I	E
	V	E	D	T	O
	H	A	V	E	B
	E	E	N	A	S
	S	I	G	N	E
	D	T	O	W	A
	T	C	H	B	R
	I	D	G	E	S
	T	O	P	M	E
	E	T	I	N	G
	T	I	M	E	U
	N	C	H	A	N
	G	E	D	X	X
Ключ:	**E**	**V**	**E**	**R**	**Y**

5. Криптоаналіз класичних шифрів

Приклад 5.3:

Шифротекст:

WERXEHJVYSOSPKMUVCOGSIXFUFLTHTVYCBTWPTMCLHTRGCMGQEAG
RDVFEGTDJPFPWPGVLIASCSGABHAFDIASEFBTVZGIIIHDGIDDKAVYCCXQG
JQPKMVIYCLTQIKPMWQEQDYHGEMCTPCKRAXTKVJSPWVYJXMHNVCFN
WRDCCMVQNCKXFVYCSTBIVPDYOEFBTVZGIIQXWPXAPIHWICSUMVYCTG
SOPFPLACUCXMSUJCCMWCCRDUSCSJTMCEYYCZSVYCRKMRKMVKOJZAB

У шифротексті триграма VYC зустрічається 5 разів

5. Криптоаналіз класичних шифрів

Відстань між появами VYC	
між 1-ою та 2-ою	72
між 1-ою та 3-ою	144
між 1-ою та 4-ою	180
між 1-ою та 5-ою	222

НСД (72, 144, 180, 222) = 6, тому можна припустити, що довжина ключового слова рівна 6

5. Криптоаналіз класичних шифрів

Метод Фрідмана

Для уточнення довжини ключа будемо використовувати метод Фрідмана

Цей метод базується на обчислені індексу збігу (ІЗ), який дозволяє визначити для деякої послідовності $x = (x_1 x_2 \dots x_n)$ з літер алфавіту $A = \{a_1, a_2, \dots, a_m\}$ ймовірність того, що два випадкових елемента цієї послідовності збігаються

5. Криптоаналіз класичних шифрів

Метод Фрідмана

$$I_c(x) = \frac{\sum_{i=0}^{m-1} n_i(n_i - 1)}{n(n-1)},$$

де n_i – кількість появи літери a_i в послідовності x, n – загальна кількість літер в x

Відомо, що І3 рядків осмисленого тексту для різних природніх мов такий:

0,058 – українська мова

0,053 – російська мова

0,065 – англійська мова

5. Криптоаналіз класичних шифрів

i	n_i	n_i-1	$n_i(n_i$-1)
A	10	9	90
B	7	6	42
C	27	26	702
D	11	10	110
E	10	9	90
F	11	10	110
G	15	14	210
H	9	8	72
I	15	14	210
J	9	8	72
K	11	10	110
L	7	6	42
M	15	14	210
N	3	2	6
O	5	4	20
P	14	13	182
Q	8	7	56
R	10	9	90
S	14	13	182
T	15	14	210
U	6	5	30
V	20	19	380
W	10	9	90
X	12	11	132
Y	12	11	132
Z	4	3	12
	290		**3592**

Обчислимо ІЗ для шифротексту з прикладу 5.3:

$$I_c(x) = \frac{\sum_{i=0}^{m-1} n_i(n_i - 1)}{n(n-1)},$$

$$I_c(x) = \frac{3592}{290(290-1)} \approx 0{,}0429$$

5. Криптоаналіз класичних шифрів

Для текстів англійською мовою довжину ключа можна визначити за формулою або таблицею:

$$l \approx \frac{k_p - k_r}{I_c(x) - k_r + \frac{k_p - I_c(x)}{n}},$$

де $k_r = \frac{1}{m} = \frac{1}{26} = 0{,}0385$, $k_p = \sum_{i=0}^{m-1} p_i^2 = 0{,}065$

l	1	2	3	4	5	6	7	8	9	10	∞
$I_c(x)$	0,0660	0,0520	0,0470	0,0449	0,0435	0,0426	0,0419	0,0414	0,0410	0,0407	0,0388

5. Криптоаналіз класичних шифрів

Визначимо довжину ключа для прикладу 5.3:

$$l \approx \frac{k_p - k_r}{I_c(x) - k_r + \frac{k_p - I_c(x)}{n}}$$

$$l \approx \frac{0{,}065 - 0{,}0385}{0{,}0429 - 0{,}0385 + \frac{0{,}065 - 0{,}0429}{290}} \approx 6{,}06369$$