ЛЕКЦИЯ 3.
Классические методы шифрования (ч.1)

3.1. Моноалфавитные шифры.

3.2. Полиалфавитные шифры.

3.3. Роторные шифровальные машины.

Шифр Цезаря.

Открытый текст: meet me after the toga party.
Шифрованный текст: phhw ph diwhu wkh wrjd sdumb.

Алфавит считается **«циклическим»**, каждая буква открытого текста **p** заменяется буквой шифрованного текста **c**:

$$C = E(p) = (p+3) \bmod(26).$$

***Обобщенный алгоритм Цезаря*:**

$$C = E(p) = (p+k) \bmod(26),$$

где ***k*** принимает значения в диапазоне от 1 до 25.

Алгоритм дешифрования:

$$p = D(C) = (C - k) \bmod(26).$$

Применение ***метода последовательного перебора всех возможных вариантов*** оправдано следующими характеристиками данного шифра:

- **Известны** алгоритмы шифрования и дешифрования.
- Необходимо перебрать всего **25 вариантов**.
- Язык открытого текста **известен** и легко узнаваем.

Криптоанализ ***шифра Цезаря*** методом
перебора всех вариантов ключей

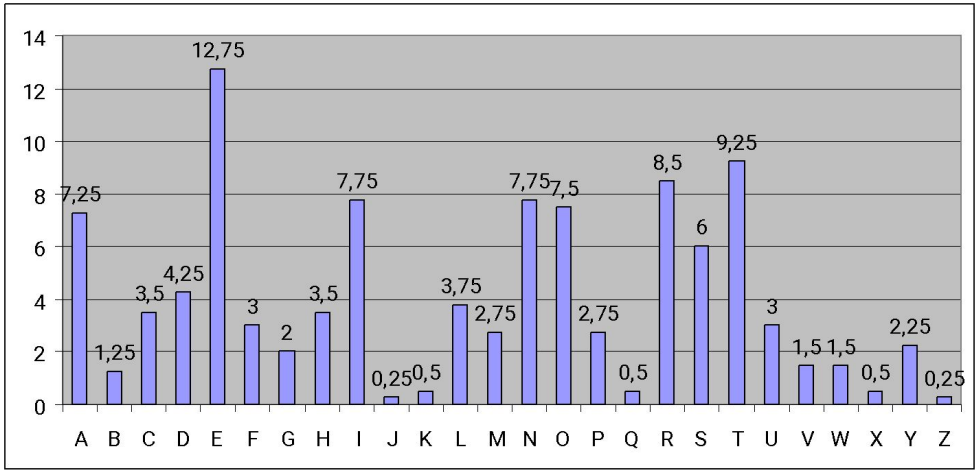
PHHW PH DIWHU WKH WRJD SDUWB

key						
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufc	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxopv
7	iaap	ia	wbpan	pda	pksw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Использование известной информации о характерных признаках, присущих текстам на соответствующем языке.

На первом этапе

- определяется **относительная частота** появления в тексте различных букв,
- сравнивается со ***среднестатистическими данными*** для букв английского алфавита.



Относительная частота появления букв в английском тексте

На втором этапе

продолжается поиск в тексте новых характерных **закономерностей**:

- может быть известно, что в рассматриваемом тексте обязательно должны присутствовать некоторые слова,

- можно искать *повторяющиеся последовательности* букв шифрованного текста и пытаться определить их эквиваленты в открытом тексте : ***один из эффективных методов заключается в подсчете частоты использования комбинаций, состоящих из двух букв.***

Такие комбинации называются **биграммами**. Для значений относительной частоты появления в тексте биграмм тоже можно построить *гистограмму.*

Шифр Плейфейера

Алгоритм Плейфейера основан на использовании **матрицы букв размерности 5×5**, созданной на основе некоторого ключевого слова.

Матрица создается путём:

- размещения букв, использованных в ключевом слове, *слева направо* и *сверху вниз* (повторяющиеся буквы отбрасываются);
- оставшиеся буквы алфавита размещаются в *естественном* порядке в оставшихся строках и столбцах матрицы;
- буквы **I** и **J** считаются одной и той же буквой.

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

Открытый текст шифруется ***порциями по две буквы*** по следующим правилам:

1. Если оказывается, что повторяющиеся буквы открытого текста образуют одну пару для шифрования, то между этими буквами вставляется специальная *буква-заполнитель*, например, ***x***.

В частности, такое слово как **balloon** будет преобразовано к ***ba lx lo on***.

2. Если буквы открытого текста попадают в одну и ту же **строку** матрицы, каждая из них заменяется буквой, следующей за ней в той же строке ***справа*** – с тем условием, что для замены последнего элемента строки матрицы служит первый элемент той же строки.

Например, ***ar*** шифруется как **RM**.

3. Если буквы открытого текста попадают в один и тот же **столбец** матрицы, каждая из них заменяется буквой, стоящей в том же столбце ***сразу под ней***, с тем условием, что для замены самого нижнего элемента столбца матрицы берется самый верхний элемент того же столбца.

Например, ***mu*** шифруется как **CM**.

4. Если не выполняется ни одно из приведенных выше условий, каждая буква из пары букв открытого текста заменяется буквой, находящейся на **пересечении** содержащей эту букву **строки матрицы и столбца**, в котором находится вторая буква открытого текста.

Например, ***hs*** шифруется как **BP**, а ***ea*** – как **IM** (или **JM**, по желанию шифровальщика).

Шифр Хилла.

Алгоритм **заменяет** каждые **m** последовательных букв открытого текста **m** буквами шифрованного текста.

Подстановка определяется **m** ***линейными уравнениями***, в которых каждому символу присваивается численное значение **(a = 0, b = 1, …, z = 25).**

Например, при **m = 3** получаем следующую систему уравнений:

$$C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \pmod{26},$$
$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \pmod{26},$$
$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \pmod{26}.$$

Или в виде произведения вектора и матрицы :

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{23} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

или :

$$C = KP,$$

где **C** и **P** – векторы длины 3, представляющие соответственно **шифрованный** и *открытый* тексты, **K** – матрица размерности 3 × 3, представляющая ***ключ шифрования***.

Операции выполняются *по модулю 26*.

Для **расшифровки** нужно воспользоваться матрицей, ***обратной* K**.

Обратной по отношению к матрице **K** называется такая матрица K^{-1}, для которой выполняется равенство $KK^{-1} = K^{-1}K = I$, где **I** – ***единичная*** матрица.

Общий вид системы *Хилла* :

$$C = E_K(P) = KP,$$
$$P = D_K(C) = K^{-1}C = K^{-1}KP = P.$$

Взлом шифра Хилла
для шифра с матрицей ***m* × *m*.**

Известны **m** пар отрывков **открытого** и соответствующего ***шифрованного*** текстов, каждый длины **m**.

1.Выбираются такие пары

$$\mathbf{P_j = (p_{1j}, p_{2j}, \ldots, p_{mj})} \quad \text{и} \quad \mathbf{C_j = (C_{1j}, C_{2j}, \ldots, C_{mj}),}$$

чтобы выполнялось условие $\mathbf{C_j = KP_j}$ для всех $\mathbf{1 \le j \le m}$ и некоторой известной *ключевой матрицы* **K**.

2. Определяются две такие матрицы

$$\mathbf{X = (p_{ij})} \quad \text{и} \quad \mathbf{Y = (C_{ij})}$$ размера **m×m,**

что $\mathbf{Y = X\,K}$.

3. При условии, что для матрицы **X** существует обратная матрица, ***матрицу − ключ*** **K** можно определить по формуле

$$\mathbf{K = X^{-1}\,Y}.$$

4. Если получить матрицу, обратную матрице **X**, невозможно, необходимо сформировать ***другую*** матрицу **X** с дополнительными парами соответствия открытого и шифрованного текстов, до тех пор, пока не будет найдена обратная матрица.

Полиалфавитные шифры

Шифры, основанные на применении ***нескольких моноалфавитных*** подстановок, называются **полиалфавитными** и обладают следующими особенностями:

1. Используется набор *связанных моноалфавитных* подстановок.
2. Имеется некоторый *ключ*, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Шифр Виженера

1. Шифр базируется на наборе правил моноалфавитной подстановки, представленных 26 шифрами ***Цезаря*** со сдвигом от **0 до 25**.

2. Каждый из таких шифров обозначается **ключевой буквой**, являющейся буквой шифрованного текста, соответствующей букве открытого текста.

*Например, шифр **Цезаря**, для которого смещение равно **3**, обозначается ключевой буквой **d**.*

3. Все 26 шифров располагаются по **горизонтали**, и каждому из шифров соответствует ***своя*** ключевая буква, представленная в крайнем столбце слева.

4. Алфавит, соответствующий буквам открытого текста, находится в **первой сверху строке таблицы.**

5. **Процесс шифрования** – необходимо по ключевой букве ***x*** и букве открытого текста ***y*** найти букву шифрованного текста, которая находится на **пересечении** строки ***x*** и столбца ***y***.

Для шифрования нужен **ключ**, *имеющий ту же длину*, что и само сообщение.

Например, если ключевым является слово

deceptive,

сообщение **«we are discovered save yourself»** шифруется следующим образом.

Ключ: ***d e c e p t i v e d e c e p t i v e d e c e p t i v e***
Открытый текст: w e a r e d i s c o v e r e d s a v e y o u r s e l f
Шифрованный текст: Z I CVTWQNGR ZGVT WAV ZHC Q YGLMGJ

6. Расшифровка текста – ***буква ключа*** определяет *строку*, **буква шифрованного текста**, находящаяся в этой *строке*, определяет **столбец**, и в этом столбце в первой строке таблицы будет находиться соответствующая буква **открытого текста**.

ТАБЛО ВИЖЕНЕРА

	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

Лучшей защитой от криптоанализа является выбор ключевого слова, ***по длине равного длине открытого текста, но отличающегося от открытого текста по статистическим показателям***.

Шифр Вернама

Система ***Вернама*** оперирует двоичными числами:

$$\mathbf{C_i = p_i \oplus k_i},$$

где
$\mathbf{p_i}$ – i-ая двоичная цифра открытого текста,
$\mathbf{k_i}$ – i-ая двоичная цифра ключа,
$\mathbf{C_i}$ – i-ая двоичная цифра шифрованного текста,
$\oplus$- операция **XOR** (исключающее «ИЛИ»).

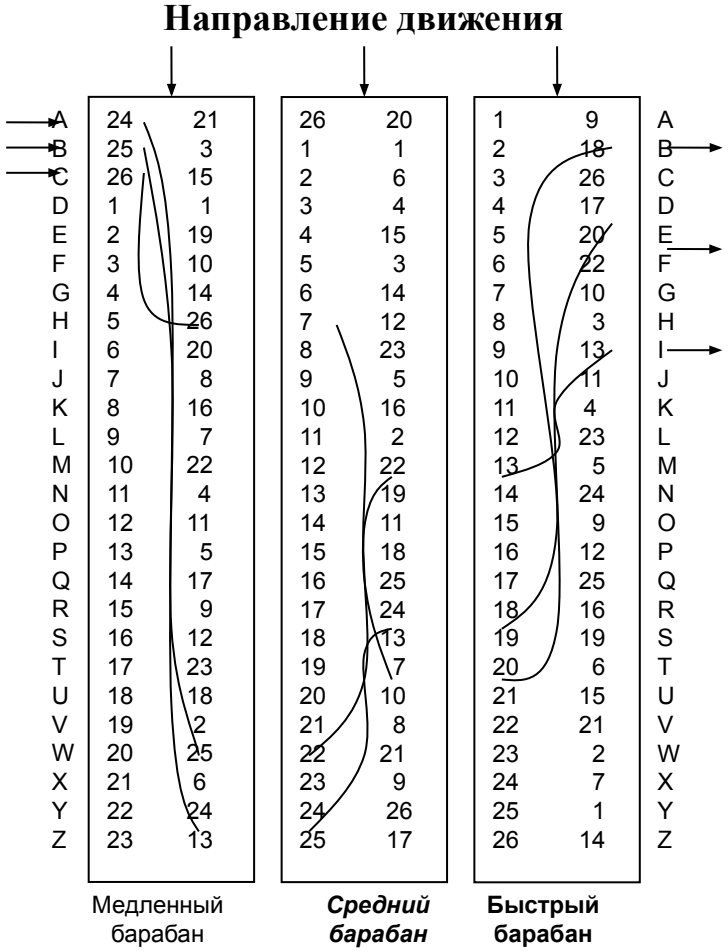
Расшифровка (достаточно выполнить ***эту же*** операцию):

$$\mathbf{p_i = C_i \oplus k_i}.$$

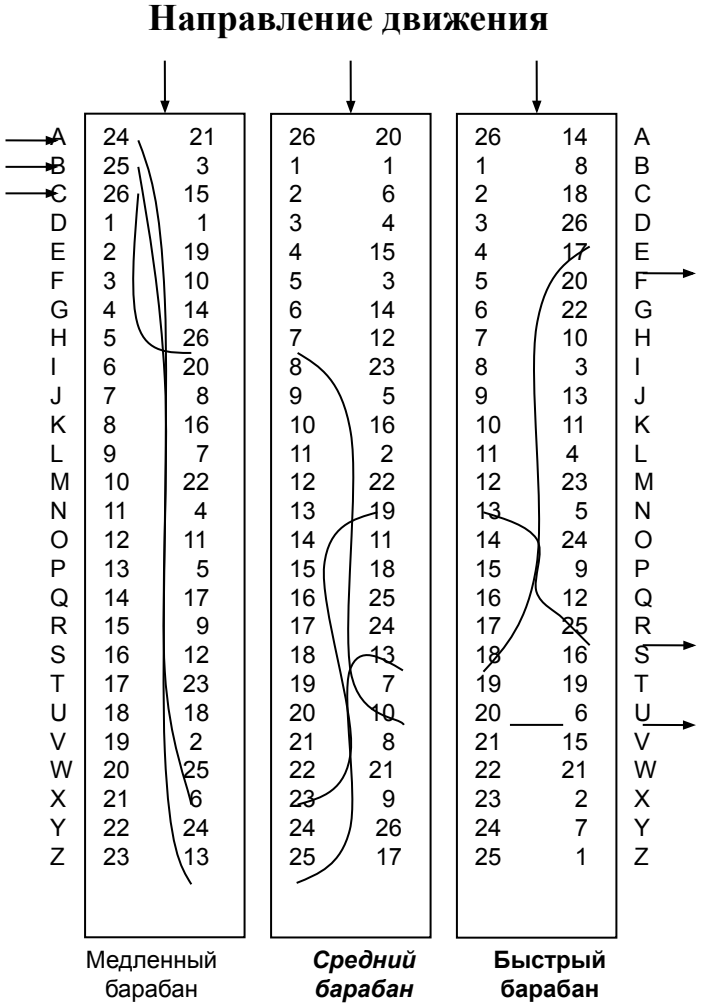
Лента однократного использования (или **схема с одноразовым блокнотом**) - *случайным образом* генерируется ключ, по длине **равный длине сообщения**.
Взлому не поддается.

Роторные шифровальные машины

Трехбарабанная **шифровальная машина с системой электропроводки, представленной соответствующей нумерацией контактов**



(а) Исходное состояние



(б) Состояние после ввода одной буквы