

Медведев Владимир Арсентьевич

E – mail: krat29@rambler.ru



Информационная безопасность организации

Лекция 11. Математическое
обеспечение ИБ. Часть 1.

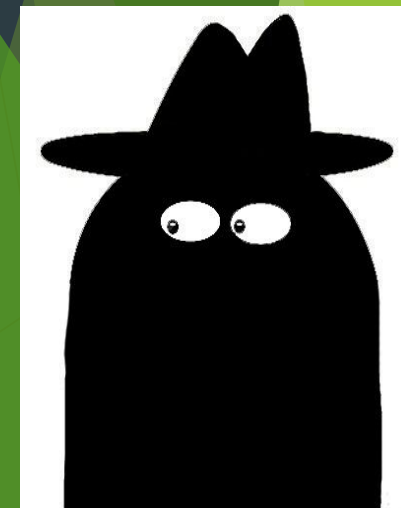
Санкт – Петербург, 2016 г.

«Люди делятся на три категории: умеющие считать и не умеющие считать» - закон Уинкорна

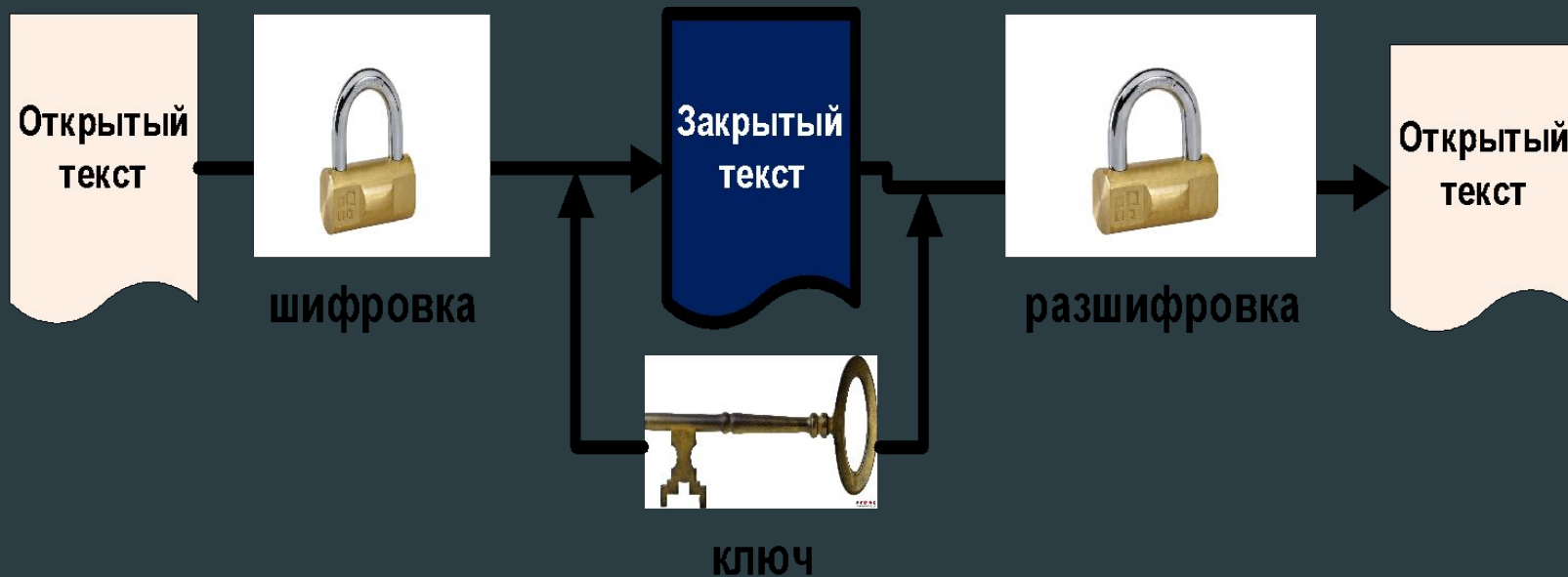
Криптография позволяет хранить важную информацию или передавать её по ненадёжным каналам связи (таким как Интернет) так, что она не может быть прочитана никем, кроме легитимного получателя.

Криптоаналитиков также называют взломщиками шифров.

Криптография бывает *стойкой* или *слабой*. Криптографическая стойкость измеряется тем, сколько понадобится времени и ресурсов, чтобы восстановить исходный открытый текст.



Симметричное шифрование



Data Encryption Standard (DES) – пример симметричного алгоритма, широко применявшегося на Западе с 70-х годов в банковской и коммерческой сферах. В настоящее время его сменяет Advanced Encryption Standard (AES).

Достоинства и недостатки

**скорость
криптографических
операций**

**полезно для шифрования
данных, которые не
предназначены для
передачи**

**сложности передачи тайного ключа,
отправителю и получателю нужно
предварительно согласовать ключ и
держат его в тайне**

**глобальная проблема
в сложности управления
ключами без риска его
перехвата**

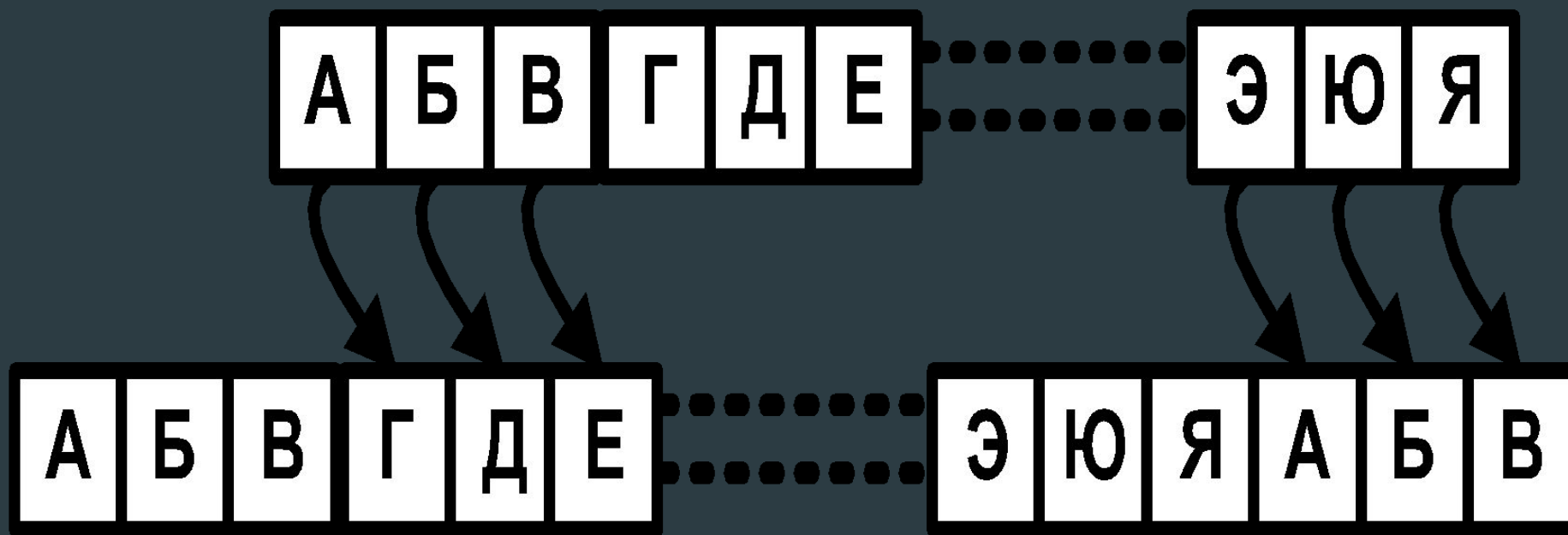


Наиболее известные виды криптозащиты

- *шифр Цезаря* (аффинный шифр), когда каждая буква исходного сообщения меняется на другую букву, сдвинутую на фиксированное число позиций;
- *шифр Альберти* (полиалфавитный шифр), когда буквы в сообщении берутся поочерёдно из двух и более алфавитов;
- *шифр Марии Стюарт* (полиалфавитный шифр), когда одни буквы заменяют другими из «параллельного алфавита» плюс некоторые «общеупортебительные» слова заменяются специальными символами;
- *шифр квадрат Виженера*, когда составляется матрица, где количество строк равно количеству столбцов, каждая строка представляет собою один и тот же алфавит, но начинается со сдвигом на один символ. В сообщении каждый знак указывает буквой позицию в первой строке и цифрой – на сколько строк нужно опуститься, чтобы найти истинную букву.

Шифр Цезаря

Шифр Цезаря — это вид шифра подстановки. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее:



Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$Y = (x + k) \bmod n,$$

$$X = (y - k + n) \bmod n,$$

где:

x — символ открытого текста, y — символ шифрованного текста,
 n — мощность алфавита, k — ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра, когда каждой букве алфавита размера ставится в соответствие число из диапазона.



Гай Юлий Цезарь (12 или 13 июля 100 года до н. э. — 15 марта 44 года до н. э.) — древнеримский государственный деятель, полководец, писатель, великий понтифик с 63 года до н. э.

«Пришёл, увидел, победил» - так в 47 году до н. э. Цезарь уведомил своего друга Аминция о быстрой победе при Зеле.



Задание № 1.

- Запишите свою фамилию используя шифр Цезаря.
- За первую позицию нового алфавита надо взять первую букву Вашего имени + 3 позиции

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	

Например:

Ваша фамилия и имя **Араков Илья**, тогда получим:

Ньнцъп



Полиалфавитные шифры Марии Стюарт и Л. Альберти

Предположим, что имеется некоторое сообщение:

$x_1, x_2, x_3, \dots, x_n, \dots, x_{2n}, \dots$,

которое необходимо зашифровать, а также для использования полиалфавитного шифра используется n моноалфавитных шифров.

В данном случае к первой букве применяется первый моноалфавитный шифр, ко второй букве — второй, к третьей — третий, ..., к n -ой букве — n -ый, а к $(n+1)$ -ой вновь **первый**, и так далее, пока все сообщение не будет зашифровано.

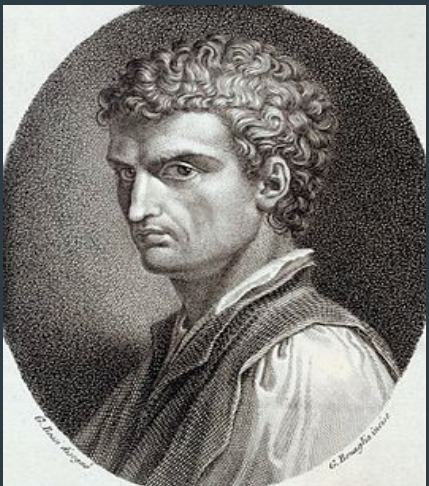
Используя метод Альберти, в качестве примера, можно рассмотреть вариант использования трёх алфавитов: 1 – стандартный алфавит, 2 – первый шифроалфавит, 3 – второй шифроалфавит:

1 – /а/б/в/г/д/е/ж/з/и/к/л/м/н/о/п/р/с/т/у/ф/х/ц/ч/ш/щ/ъ/ы/ь/э/ю/я/а/б/;

2 - /д/е/ж/з/и/к/л/м/н/о/п/р/с/т/у/ф/х/ц/ч/ш/щ/ъ/ы/ь/э/ю/я/а/б/в/г/д/;

3 – /ц/у/к/е/н/г/ш/щ/з/х/ъ/ф/ы/в/а/п/р/о/л/д/ж/э/я/ч/с/м/и/т/ь/б/ю/.

Теперь каждую нечётную букву в шифруемом сообщении заменим буквой стоящей на той же позиции во втором алфавите, а каждую чётную букву аналогично заменим из третьего алфавита. Тогда фамилия автора шифра **Альберти** будет зашифрована как: **Дъаукпцз**.



Леон Баттиста Альберти (18.02.1404, Генуя — 25.04.1472, Рим) — итальянский ученый, гуманист, писатель, один из зачинателей новой европейской архитектуры и ведущий теоретик искусства эпохи Возрождения. Предложил в книге «Трактат о шифрах» идею многоалфавитного шифра.

При таком способе шифрования одна и та же буква будет кодироваться не одинаково, в зависимости от того какую позицию она занимает. Частотный анализ, таким способом, значительно теряет свою силу.



Задание № 2.

- ▶ Запишите свою фамилию используя шифр Альберти.
- ▶ Для шифрования придумайте сами 4 новых шрифта и меняя шрифты по очереди замените буквы на новые



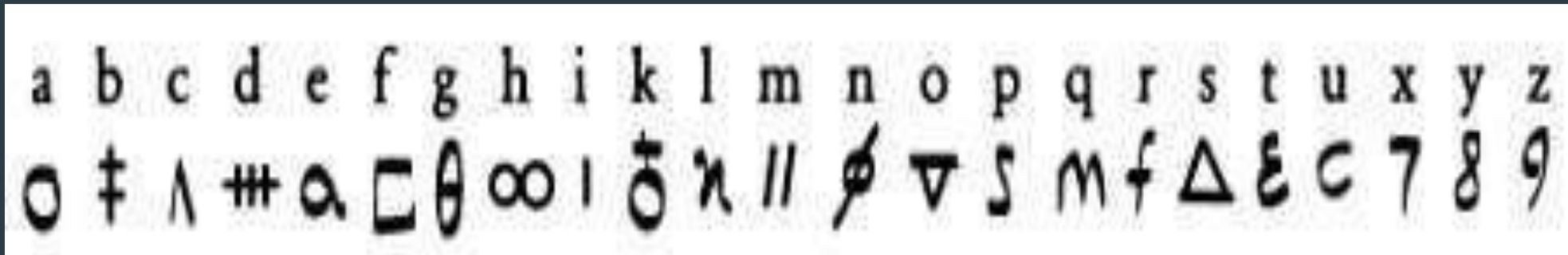
№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
2	Г	Д	Е	С	Т	В	Б	А	Ч	Ю	Ш	К	Щ	Л	Я	М
3	Л	З	А	Б	В	К	Ц	Я	Э	Ю	Ы	Ь	Ъ	У	Т	С

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ц	Х	Ф	Н	О	П	Р	Ъ	Ь	Ы	Э	У	З	Ж	И
И	Ж	Ш	Ч	Щ	Д	Е	Г	Ф	Х	Р	П	О	М	Н





Мари I (урожденная Мария Стюарт, 8.12.1542 — 8. 02.1587) — королева Шотландии с младенчества до низложения в 1567 г., а также королева Франции в 1559—1560 г. и претендентка на английский престол.



Королева считала, что шифр сверхнадёжный, но лучший криптоаналитик того времени Томас Фелиппес, был экспертом в частотном анализе...



Задание № 3.

- Запишите свою фамилию используя шифр М. Стюарт.
- Для шифрования придумайте сами новых шрифт с использованием новых знаков и замените буквы на новые

Например: Ваша фамилия **Араков**. Тогда, придумав свой алфавит, получим: ♥♥§♥♥**†¥

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
	♥♥	U	¥	Ψ	\$	%	@	?	^^	**	#	&	≈	†	Ξ	§

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
÷	ω	σ	ℵ	ћ	є	Ж	я	ѐ	↔	▼	▣	Д	♪	+



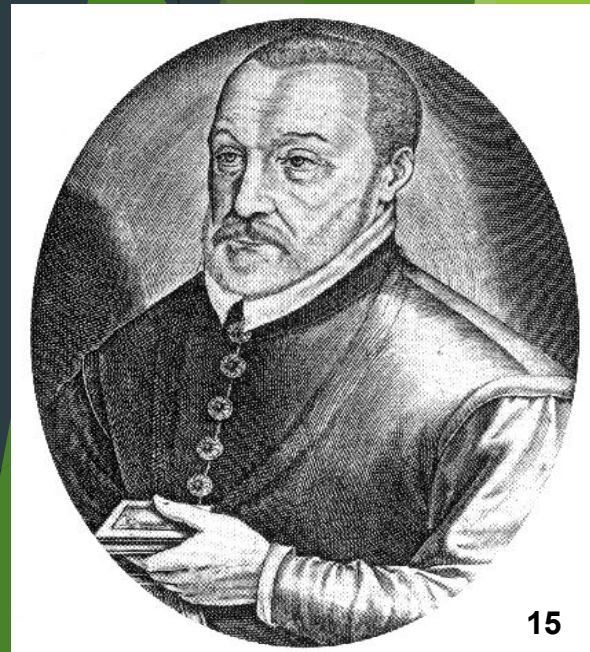
Квадрат Виженера - система полиалфавитного шифрования

- шифр является недоступным для простых методов криптоанализа.

- состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига.

На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Блез де Виженер (5.04.1523, Сен-Пурсен-сюр-Сиуль — 19.02.1596, Париж) — французский дипломат, криптограф и алхимик. Изобретение шифра в XIX веке было ошибочно приписано именно ему.



Квадрат 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

Таким образом, в таблице получается 26 различных шифров Цезаря

	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

Например, предположим, что исходный текст имеет вид:

Blaise-de-Vigenre – 15 букв.

А в качестве ключевого будет выбрано слово: ***cifra*** («шифр»), которое необходимо циклически повторять до тех пор, пока его длина не будет соответствовать длине исходного текста (15 букв):

Cifracifracifra

... и получим:

Dtfzsg-lj-Miimsie

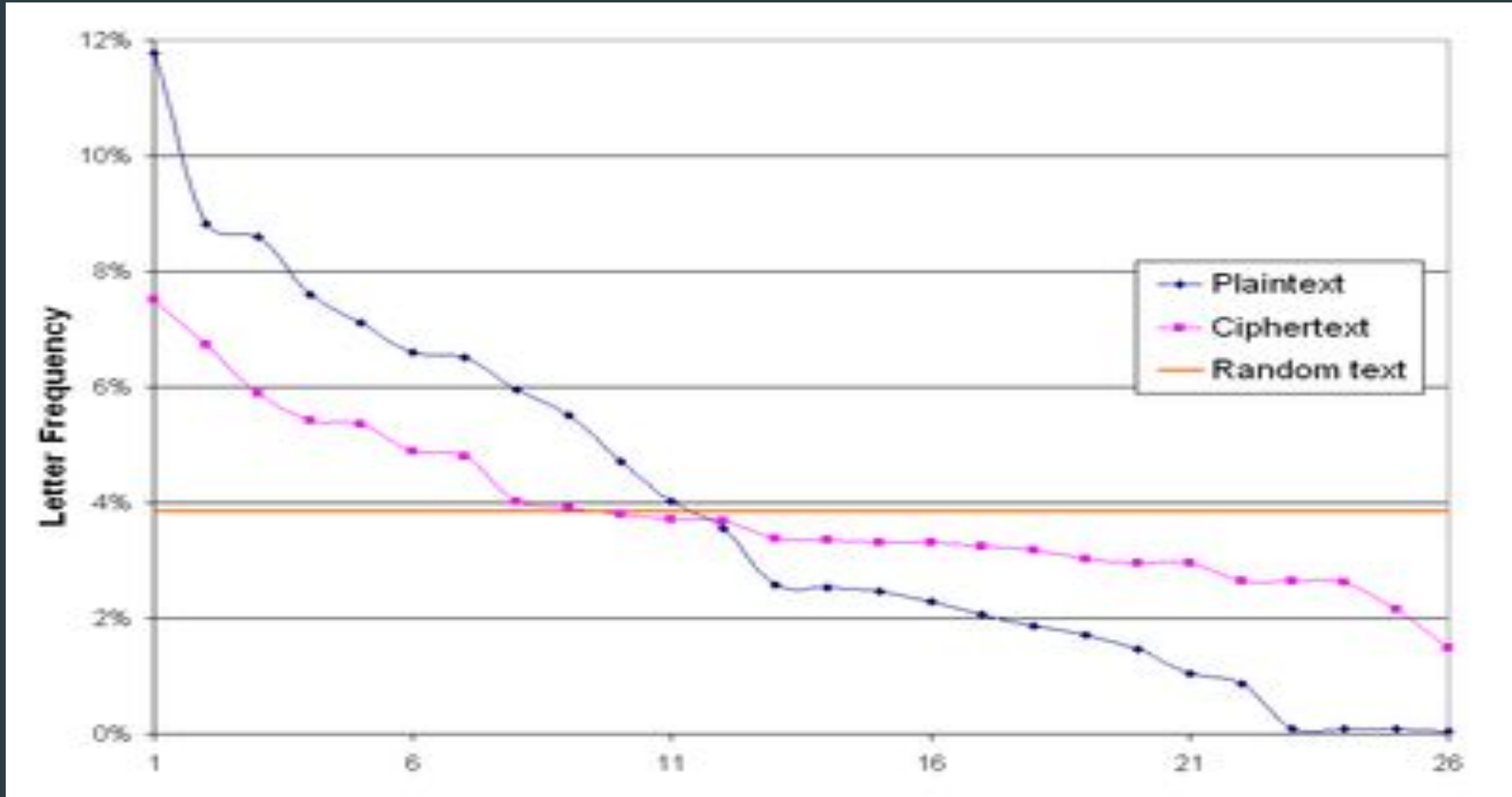
Алгоритм шифрования

Первый символ исходного текста **B** зашифрован последовательностью **C**, которая является первым символом ключа. Первый символ **D** шифрованного текста находится на пересечении строки **C** и столбца **B** в таблице Виженера.

Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста **t** получается на пересечении строки **i** и столбца **l**.

	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

Шифр Виженера «размывает» характеристики частот появления символов в тексте



Главный недостаток шифра Виженера
– повторяемость его ключей.

Расшифровывание производится следующим образом:

- необходимо найти в таблице Виженера строку, соответствующую первому символу ключевого слова;
- в данной строке необходимо найти первый символ зашифрованного текста;
- столбец, в котором находится данный символ, соответствует первому символу исходного текста;
- следующие символы зашифрованного текста расшифровываются подобным образом.

Если буквы **A—Z** соответствуют числам **0—25**, то шифрование Виженера можно записать в виде формулы:

$$C_i \equiv (P_i + K_i) \bmod 26;$$

Расшифровка:

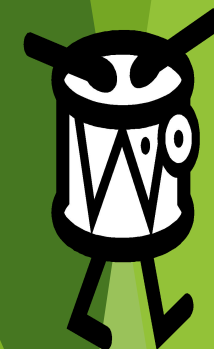
$$P_i \equiv (C_i - K_i + 26) \bmod 26;$$

Русский квадрат Виженера

Ключ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
1	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
16	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
18	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
19	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
20	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
21	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
22	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
23	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
24	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
25	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
26	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
27	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
28	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
29	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
30	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
31	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю



Задание № 4.



- Запишите с использованием квадрата Виженера фразу:

НАУКА УМЕЕТ МНОГО ГИТИК

- Для шифрования придумайте сами кодовое слово из 4 букв и замените буквы на новые

Например: Ваш код **дама**. Тогда, для кодирования составим таблицу и заполним её с использованием квадрата Виженера:

1	н	а	у	к	а		у	м	е	е	т		м	н	о	г	о		г	и	т	и	к
2	д	а	м	а	д		а	м	а	д	а		м	а	д	а	м		а	д	а	м	а
3	с	а	я	к	д		у	ш	е	й	т		ш	н	т	г	ь		г	м	т	ф	к

1 – исходный текст; **2** – кодовое слово; **3** – закрытый текст