История технологий шифрования

Открытый текст

- *Открытый текст – сообщение, подлежащее засекречиванию. В результате применения методов шифрования сообщение делают непонятным для посторонних.*
- Открытый текст — в криптографии исходный текст, подлежащий шифрованию, либо получившийся в результате расшифровывания. Может быть прочитан без дополнительной обработки.
- Открытым текстом будет называться информация даже в том случае, если она сохранена в нетекстовом виде — например, музыка или звук. Главное, чтобы для использования данной информации не требовалось производить дешифрование.

Перестановка и замена

- В случае *перестановки* знаки открытого текста перемешиваются, нарушается их нормальный порядок следования. Перетасовать буквы слова *«секрет»* так, чтобы получить *«еткрсе»,* и означает сделать перестановку.

- При *замене* знаки открытого текста замещаются другими знаками. Так, слово *«секрет»* может быть заменено на *19 5 3 18 5 20.*
- Системы замены основаны на идее *шифроалфавита* – перечня эквивалентов, используемых для преобразования открытого текста в шифрованный.

Много- и одно- алфавитность

- В том случае, когда используется только один шифроалфавит, система замены называется *одноалфавитной.* Но когда применяются два или большее число шифроалфавитов по какому-то заранее определенному правилу, система замены становится *многоалфавитной.*

Коды и шифры

- Среди систем замены следует делать различия между *кодами* и *шифрами.* Код состоит из тысяч слов, фраз, букв и слогов и соответствующих им *кодовых слов* или *кодовых обозначений,* которые заменяют эти элементы открытого текста. По существу, код является огромным шифром замены, в котором основными единицами открытого текста служат слова и фразы. В шифрах же основная единица – это знак, иногда пара знаков.

Номенклатор

- В течение 450 лет, начиная примерно с 1400 г. и до 1850 г., в шифровальной практике доминировали системы, которые являлись наполовину кодом и наполовину шифром. В них обычно был отдельный шифралфавит, включавший побуквенные замены и кодо-подобный перечень имен, слов и слогов. От этого перечня, первоначально состоявшего только из имен, и произошло название для таких систем – *номенклатор.*

Шифр текст

- Проведение соответствующих преобразований открытого текста в шифрованный называется *шифрованием* или *кодированием* открытого текста. То, что получается в результате, носит название *шифртекста.*

Криптограмма

- Окончательно обработанное и отосланное секретное сообщение называется *криптограммой.* Термин «шифртекст» обращает внимание на результат зашифровывания, в то время как термин «криптограмма» подчеркивает сам факт передачи.
- На практике оба слова часто употребляются в значении шифртекста.

Расшифровывание и криптоанализ

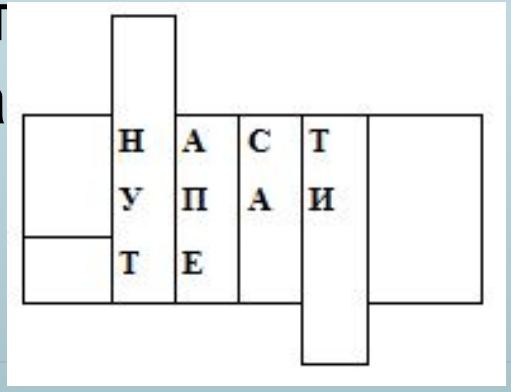
- *Расшифрование* означает проведение обратных преобразований шифртекста лицами, владеющими на законном основании ключом и системой шифрования, для получения открытого текста. Этот процесс следует отличать от *криптоанализа,* который ставит своей целью прочтение открытого текста (или, другими словами, *дешифрование)* криптограммы людьми, не имеющими в своем распоряжении ни ключа, ни системы, то есть лицами, являющимися третьей стороной, «противником».
- Успешный криптоанализ шифра или кода часто называют его *вскрытием* или *взломом.*

Криптология

- Криптология – это наука, охватывающая составление шифров *(криптографию)* и криптоанализ.

Аристотель

- В V – VI вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли скиталами.
- Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать ег… шифрованным сообщением, сдвига… вершине.



Полибий(118 гг. до н. э)

- Значительным шагом вперед, по сравнению с предыдущими системами шифрования представлял шифр, предложенный Полибием. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами: парами чисел *(i,j)*, где *i* - номер строки, *j* - номер столбца. Применительно к латинскому алфавиту квадрат Полибия имеет следующий вид

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

Цезарь

- В I в до н. э. Гай Юлий Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на

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
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

- Сообщение, направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело так: YHQL YLGL YLFL

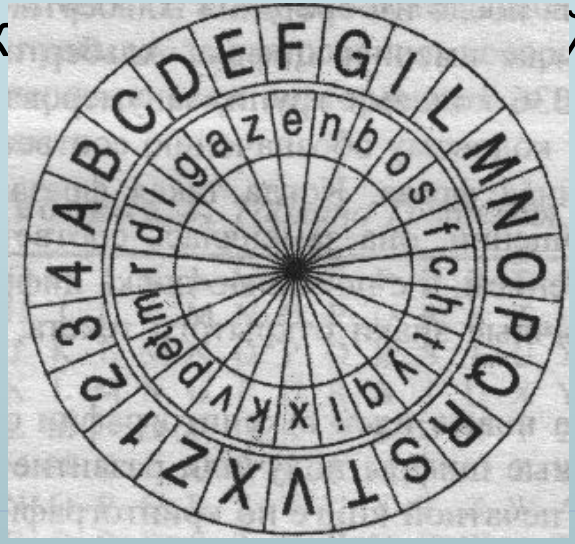
Что объединяет этих людей?

Шехаб аль-Калкашанди(855 год)

- «Относительно сокрытия в буквах тайных сообщений», 7 способов шифрования
- Автор первой инструкции по криптоанализу

АЛЬБЕРТИ Леон Батиста (1404 – 1472)

- В своем труде «Трактат о шифрах» (1466 г.) впервые(в европе) предложил шифр многоалфавитной замены, который делал сообщение практически невскрываемым. В этой работе был предложен шифр, основанный на использовании **шифровального диска**.
- Его работа «Трактат о шифре» 1466 года считается первой европейск й по криптологии.



Иоганн Тритемиус(1508)

- Тритемий предлагал использовать таблицу для многоалфавитного зашифрования самым простым из возможных способов: первая буква текста шифруется первым алфавитом, вторая буква — вторым и т. д. В этой таблице не было отдельного алфавита открытого текста, для этой цели служил алфавит первой строки. Таким образом, открытый текст, начинающийся со слов HUNC CAVETO VIRUM …, приобретал вид HWPF GFBMCZ FUEIB …

Иоганн Тритемиус(1508)

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

текст, начинающийся со слов HUNC CAVETO VIRUM …, приобретал вид HWPF GFBMCZ FUEIB …

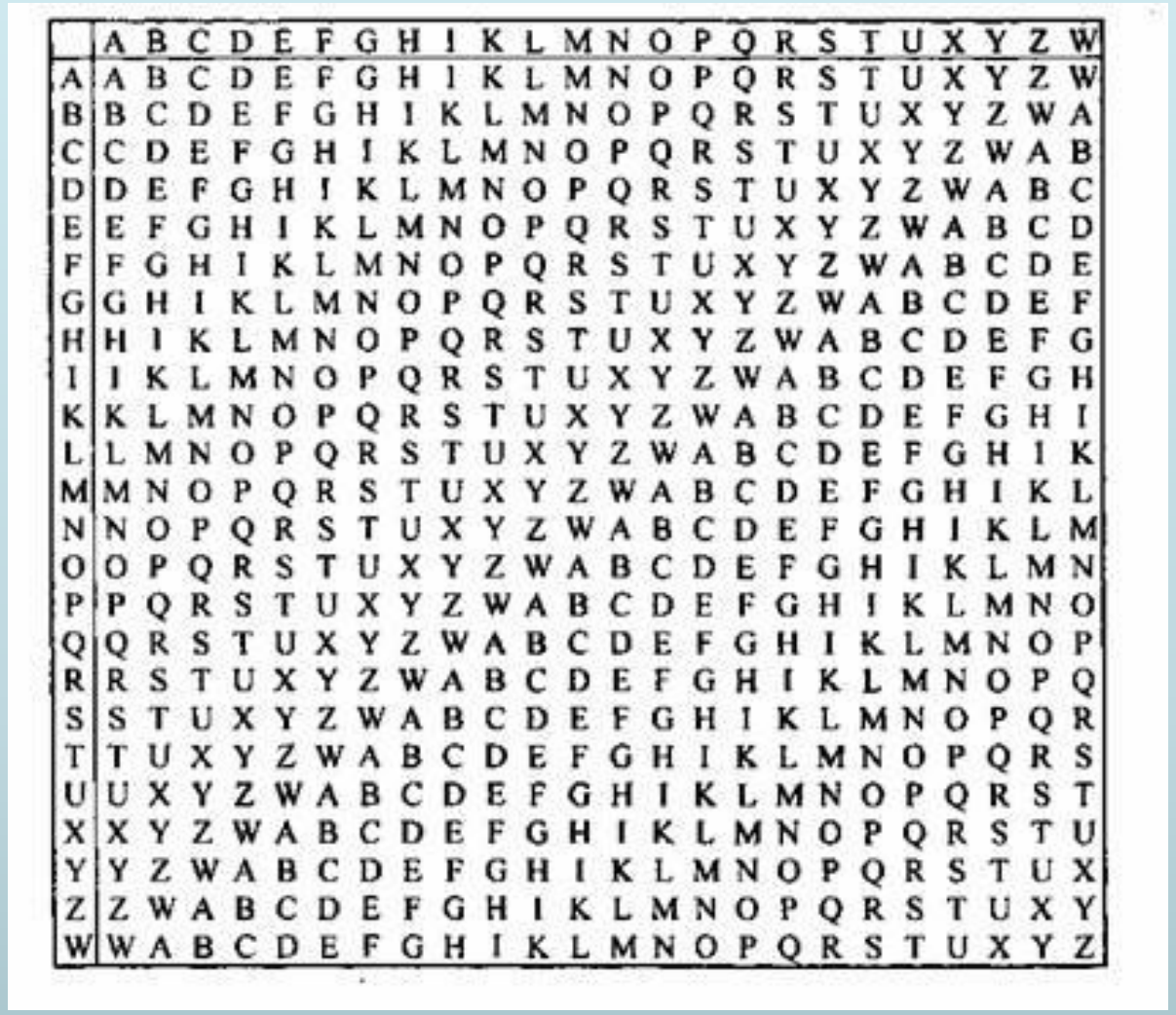
Джованни Баттиста Белазо(1553)

- Предложил использовать для многоалфавитного шифра буквенный, легко запоминаемый ключ, который он назвал паролем. Паролем могло служить слово или фраза. Пароль периодически записывался над открытым текстом. Буква пароля, расположенная над буквой текста, указывала на алфавит таблицы, который использовался для зашифровывания этой буквы.

Блез Виженер(XVI век)

- Написал книгу «Трактат о шифрах», где систематизировал существующие идеи в области криптографии. В частности описал использование таблиц для многоалфавитной замены с применением лозунга, циклического сдвига, самоключа.

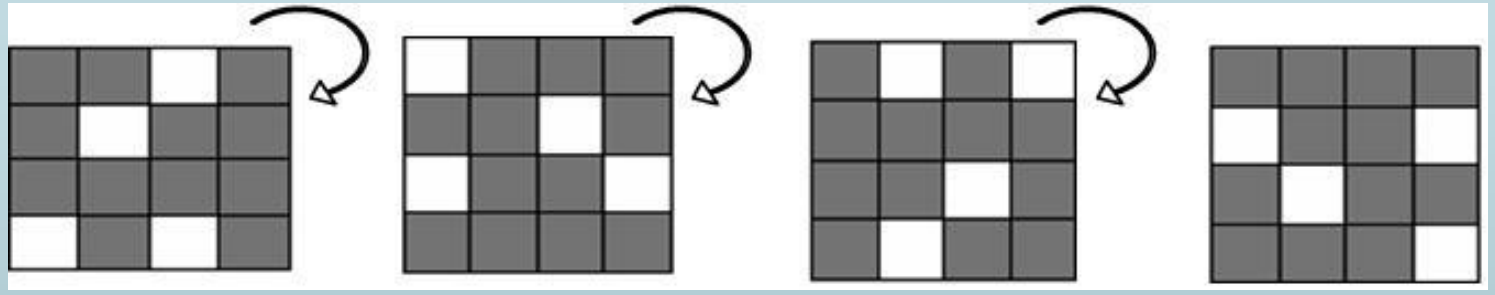
Блез Виженер(XVI век)



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

КАРДАНО Джероламо (1501–1576)

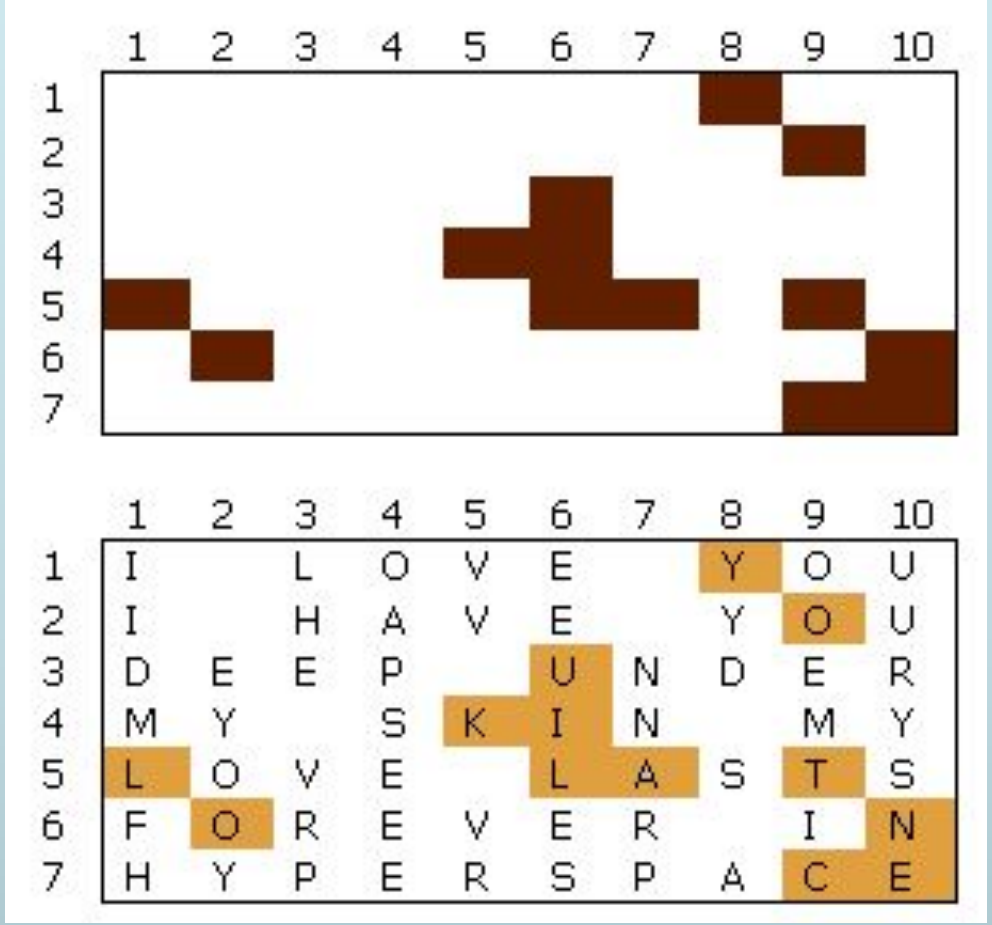
- Увлечение теорией магических квадратов привело Кардано к открытию нового класса шифров перестановок, названных решетками или трафаретами. Они представляют собой квадратные таблицы, где четверть ячеек прорезана так, что при четырех поворотах они покрывают весь квадрат.



КАРДАНО Джероламо (1501–1576)

- Подобным методом маскировки сообщения пользовались многие известные исторические лица, например, кардинал Ришелье во Франции и русский дипломат и писатель А. Грибоедов. Так, Ришелье использовал прямоугольник размера 7x10. Для длинных сообщений прямоугольник использовался несколько раз. Прорези трафарета размещались в позициях:

КАРДАНО Джероламо (1501–1576)



ВИЕТ Франсуа (1540-13.12. 1603)

- Очень успешно расшифровывал испанские шифры при дворе французского короля Генриха III, после его смерти так же занимал важные посты при дворе Генриха IV
- За расшифровку испанских криптограмм был обвинён Испанией в чёрном колдовстве и приговорён к сожжению на костре, но так и не был выдан Испании.

БЭКОН Фрэнсис (1561 - 1626)

- Он впервые предложил и осуществил на практике кодирование букв латинского алфавита с помощью двузначных цифр, и сделал систему числовых обозначений общепринятой (несмотря на то, что арабы использовали подобную систему более пяти веков назад, в Европе об этом практически ничего не знали)
- Впервые предложил двоичное кодирование букв латинского алфавита
- Создал механическое устройства для реализации шифра многоалфавитной(5) замены.

Джованни Порта(1563)

- Воскресил смешанные алфавиты, которые применял Альберти, и объединил идеи Альберти с идеями Тритемия и Белазо в современную концепцию многоалфавитной замены. Его шифр называется **шифр простой биграммной замены.**

- Шифрование осуществляется при помощи лозунга, который пишется над открытым текстом. Буква лозунга определяет алфавит (заглавные буквы первого столбца), расположенная под ней буква открытого текста ищется в верхнем или нижнем полуалфавите и заменяется соответствующей ей буквой второго полуалфавита. Например, фраза, начинающаяся словами HUNC CAVETO VIRUM …, будет зашифрована при помощи лозунга DE LA PORTA в XFHP YTMOGA FQEAS.

Джованни Порта(1563)

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

Например, фраза, начинающаяся словами

HUNC CAVETO VIRUM,

будет зашифрована при помощи лозунга

DE LA PORTA

в

XFHP YTMOGA FQEAS.

Алексей Петрович Бестужев-Рюмин (1693 - 1768)

- Назначенный в 1742 году главным директором почт, сделал в России общепринятой практику перлюстрации дипломатической корреспонденции. Однако это потребовало создания сильной криптоаналитической службы для взлома иностранных шифров, в чем и состоит основная заслуга Бестужева.

- Первым, кого Бестужев-Рюмин привлек к данной работе, стал известный математик Христиан Гольдбах, назначенный 18 марта 1842 года статским советником при Коллегии иностранных дел с окладом в 1500 рублей. Успех пришел к Гольдбаху через год, когда он смог взломать шифр французского посланника Шетарди, а уже в августе 1743 года он дешифровал более 60 писем французского и прусского дворов (за что получил премию в размере 1000 рублей).

ДЖЕФФЕРСОН ТОМАС (1743–1826)

- Последним словом в донаучной криптографии, которое обеспечило еще более высокую криптостойкость, а также позволило автоматизировать (в смысле механизировать) процесс шифрования стали роторные криптосистемы. Одной из первых подобных систем стала изобретенная в 1790 году Томасом Джефферсоном, будущим президентом США, механическая машина. Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «прошитую» в нем подстановку.

Пауль Львович Шиллинг фон Канштадт (1786)

- В историю криптографии Шиллинг вошел, прежде всего, как изобретатель так называемого биграммного шифра, который являлся комбинацией шифра перестановки с шифром многозначной замены на биграммах (двухбуквенных сочетаниях). Соответственно шифрвеличинами были не буквы, а биграммы. Шифробозначениями являлись числа, по два на каждую биграмму. Важно при этом заметить, что шифровались не две рядом стоящие в открытом тексте буквы, а пара букв, разделенных некоторым заранее оговоренным расстоянии Т друг от друга.

Пауль Львович Шиллинг фон Канштадт (1786)

- Хотя приоритет создания биграммных шифров принадлежал еще Тритемиусу, впервые использованы на практике они были именно в России в 1830-е годы при непосредственном участии Шиллинга. Вследствие сложности этот шифр применялся лишь для наиболее значимой дипломатической переписки и был весьма устойчив ко взлому.

Фридрих Казисский (1805)

- Новым вкладом в криптографию было изложение метода вскрытия многоалфавитного шифра с повторяющимся лозунгом на примере шифра Виженера, который ранее считался не дешифруемым.
- Казисский предложил метод статистического определения числа букв в лозунге, который основан на следующей идее: повторяемость букв в лозунге вместе с повторяемостью букв в открытом тексте дает повторяемость букв в шифрованном тексте. Автор пришел к выводу, что расстояние между повторениями в шифртексте будут равны или кратны периоду лозунга

Десиус Уодсворт (1817)

- Предложил механический шифратор. По предложенному им принципу собирались шифраторы в течении последующих полутора сотен лет

- Так, в устройстве Уодсворда используется 33 шифралфавита, а не 24 или 26, как в системах Тритемиуса или Виженера. Важнее то, что эти алфавиты используются не непосредственно один за другим, а в произвольном порядке, который зависит от букв открытого текста.

Этьен Базери (1846)

- Заявил во всеуслышание своим друзьям-офицерам в штабе корпуса, что известный ему французский военный шифр можно читать без ключа

- Базери начал заниматься шифрами прошлого, когда начальник генерального штаба попросил его помочь в прочтении шифрованных сообщений для изучения военных кампаний Людовика XIV. Базери успешно справляется с поставленной задачей, но на этом не останавливается – заодно ему удается вскрыть номенклаторы Франциска I, Франциска II, Генриха IV, Мирабо и Наполеона. Обнаружив, что шифры французского военного гения XIX века были чрезвычайно слабыми, в заголовке своей монографии о них Базери презрительно поставил слово «шифры» в кавычки

Этьен Базери (1846)

- Одним из изобретений Базери являлось повторение дискового шифратора Джефферсона («цилиндр Базери»).
- 20 колес, с нанесенным на них в случайной последовательности алфавитом, одевались в определенном ключом порядке на одну ось, поворачивались до тех пор, пока в одном ряду не набирали первые 20 букв сообщения, после чего шифровку считывали с другого ряда, также определяемого ключом, после чего операция повторялась. На этом, весьма незамысловатом принципе создавались практически все шифровальные машины до Второй мировой войны.

Эдвард Хеберн (1869 — 1952)

- Был американским изобретателем-самоучкой. С 1909 года он разработал целую серию электромеханических шифровальных машин с вращающимися дисками.
- Шифровальные машины Хеберна предназначались для защиты секретной переписки между различными компаниями от возможного перехвата конкурентами.
- В 1921 г. Хеберн основал первую в США компанию по производству шифрмашин, которую через десять лет ждал бесславный конец, связанный с финансовыми трудностями.

Виари и Керкгоффс (1888)

- Заложил алгебраическую основу для исследования шифров замены типа шифра Виженера. Используя уравнение шифрования, можно было отказаться от громоздкой таблицы Виженера.

- Закон Керкгоффса - «компрометация системы не должна причинять неудобств корреспондентам»

- Указал на возможность использования при дешифровании нескольких шифртекстов, полученных шифрованием различных открытых текстов на одном и том же ключе.

Керкгоффс

- «Я поражен тем, что наши ученые и профессора преподают и рекомендуют для применения в военное время системы, ключи к которым, несомненно, менее чем за час откроет самый неопытный криптоаналитик. Такое чрезмерное доверие к некоторым шифрам можно объяснить лишь недостатком научных исследований в области шифровального дела… Отсутствие серьезных работ по искусству прочтения тайнописи способствовало распространению самых ошибочных идей о стойкости наших шифрсистем».

Гильберт Вернам

- Предложил систему шифрования, названную системой одноразовых блокнотов, в которой для получения шифртекста использовалась случайная гамма, с периодом меньше длинны сообщения
- Реализовал автоматическое гаммирование телеграфных сообщений

Клод Элвуд Шеннон (1916 — 2001)

- Автор теории информации

- На прочном фундаменте своего определения количества информации Клод Шеннон доказал удивительную теорему о пропускной способности зашумленных каналов связи. Во всей полноте эта теорема была опубликована в его работах 1957-61 годов и теперь носит его имя.
- Доказал абсолютную стойкость шифров построенных на бесконечной гамме.

Уитфилд Диффи и Мартин Хеллман(1976)

- Основоположники ассиметричной криптографии

Задание

- Знать роль всех упомянутых персон в истории криптографии
- Знать определения

- Доклады на темы
- Биография Норберта Винера
- Биография Клода Шенона