КРИПТОГРАФИЯ

ЛЕКЦИЯ №2

ЛЕКТОР: ИЩУКОВА ЕВГЕНИЯ АЛЕКСАНДРОВНА, К.Т.Н.,

ДОЦЕНТ КАФЕДРЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Магические квадраты

В квадрат размером 4 на 4 (размеры могли быть и другими) вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу – 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: « *ПРИЕЗЖАЮ СЕГОДНЯ* ». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам, а в пустые клетки ставятся **произвольные буквы** .

16У	3И	2Р	13Д
5З	10Е	11Г	8Ю
9С	6Ж	7А	12О
4Е	15Я	14Н	1П

После этого шифрованный текст выписывается построчно:

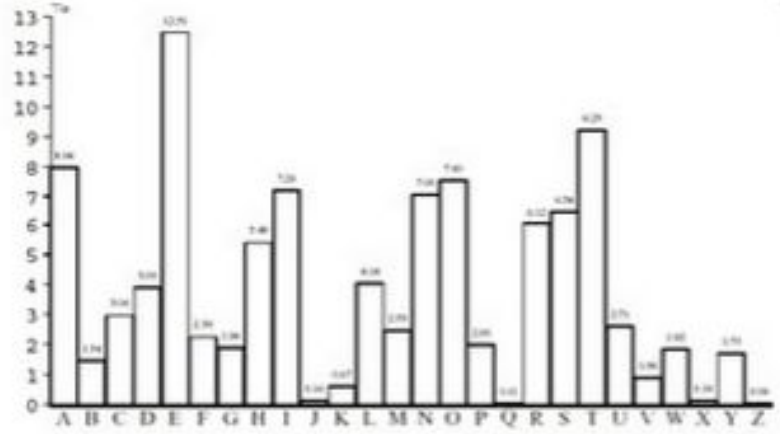
УИРДЗЕГЮСЖАОЕЯНП

При расшифровывании текст вписывается в квадрат и открытый текст читается в последовательности чисел «магического квадрата».

Данный шифр – обычный шифр перестановки, но считалось, что особую стойкость ему придает волшебство «магического квадрата».

Леон Альберти

(1466 г. “Трактат о шифрах”)



Провел анализ частот букв

Выдвинул идею

«двойного шифрования»

« Шифр, достойный коро»лей

Многоалфавитный шифр

Шифровальный диск

Иоганнес Тритемий

«Полиграфия» - первая печатная книга по криптографии (1499 г.)

Шифр «Аве Мария»

буквы шифруемого текста заменялись на заранее оговоренные слова

Например: **Н** = «Я», «ЗДЕСЬ»

Е = «ЖДУ», «МОЙ»

Т = «ДОМА», «КЛЮЧ»

«НЕТ» = «Я ЖДУ ДОМА»,

«ЗДЕСЬ МОЙ КЛЮЧ»

«Таблица Тритемия»

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

Усложнение шифра Тритемия

- произвольный порядок расположения букв исходного алфавита;

- усложненный порядок выбора строк таблицы при шифровании.

Джованни Батиста Порта

(книга "О тайной переписке")

Предложил «*биграммный шифр*», в котором каждому двухбуквенному сочетанию открытого текста в шифрованном тексте соответствовал специально придуманный знак (символико-геометрические фигуры)

Предложил использование квадратной таблицы с периодически сдвигаемым смешанным алфавитом и паролем.

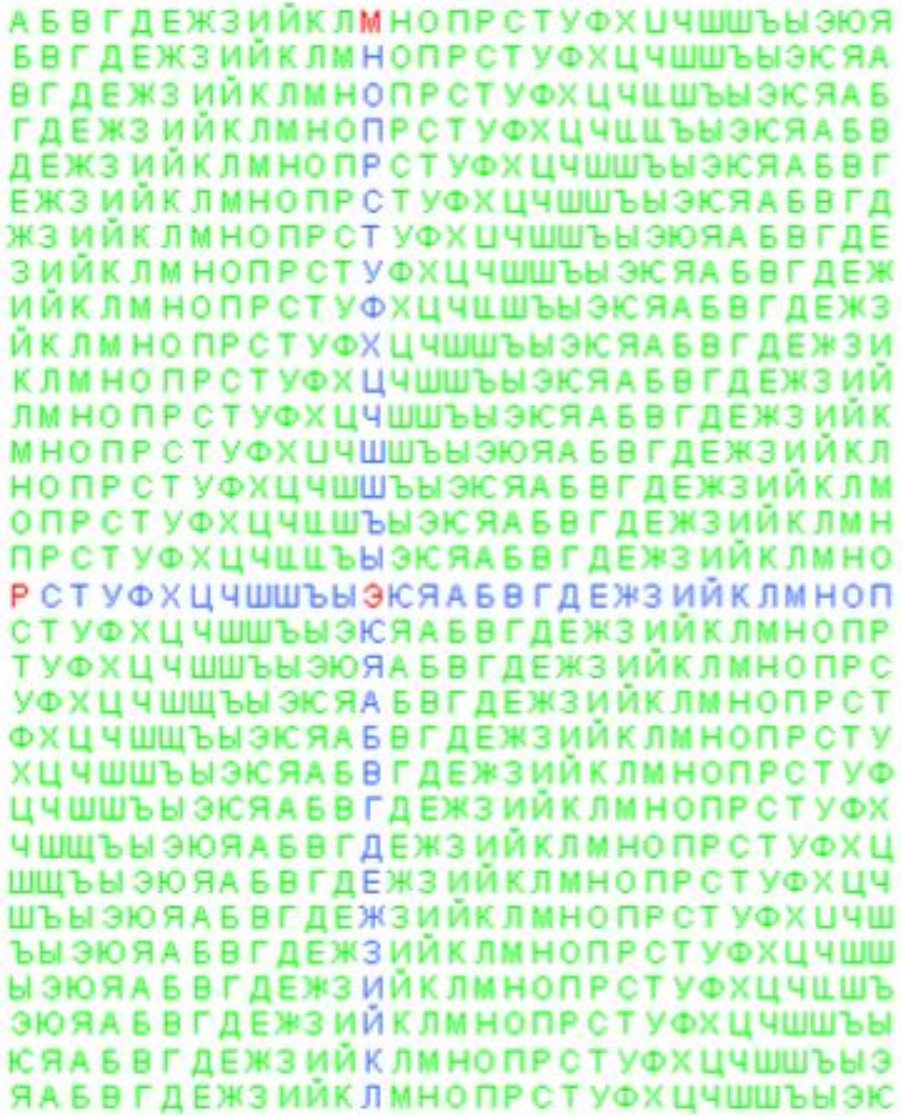
Шифрование осуществляется при помощи лозунга, который пишется над открытым текстом.

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.

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

Таблица Виженера

(1585 г. “Трактат о шифрах”)



монастырьмонастырьмон

раскинулосьмореширoко

эоякщапыйюйшовчфшлышы

Книжные шифры

n – номер страницы

m – номер строки

t – номер буквы

Френсис Бэкон

(английский философ и ученый, XVII в.)

Требования к шифрам

не должны
поддаваться
дешифрованию

не должны требовать
много времени
для написания и чтения

не должны
возбуждать
никаких подозрений

Шифратор Томаса Джефферсона

(в 1790 г. предложил механизм для реализации шифра многоалфавитной замены)

Деревянный цилиндр разрезается на 36 дисков. Эти диски насаживаются на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. Для латиницы количество ключей 36! 26!, т.е. порядка 10^{60}

Шифратор Джефферсона реализует шифр многоалфавитной замены.

Ключ:

- порядок расположения букв на каждом диске
- порядок расположения этих дисков на общей оси

Это изобретение стало предвестником появления так называемых дисковых шифраторов, нашедших широкое распространение в XX веке.

Этьен Базери

В развитие идеи шифратора Джефферсона предложил в 1891 г., так называемый, “цилиндр Базери”

На общую ось надевались 20 цилиндров со случайным нанесением по ободу букв алфавита. Методом вращения цилиндров с одной стороны выстраивалось исходное сообщение, шифротекст читался с обратной стороны.

Шифровальные машины прошлого.

Фридрих Казисский

В книге “Искусство тайнописи и дешифрования ” изложил методы вскрытия шифров типа шифра Виженера.

При использовании такого шифра периодически повторяющиеся сочетания букв открытого текста, совпадая с периодическими продолжениями лозунга (исходной гаммы), порождают совпадающие сочетания букв в шифрованном тексте. Эти повторения могут быть эффективно использованы при дешифровании.

Линейка Сен-Сира

Линейка Сен-Сира является простым механическим воплощением шифра Виженера.

Развитием идеи линейки Сен-Сира явилось произвольное расположение букв алфавита на движке.

Основная слабость: периодическое повторение короткого ключа-лозунга.

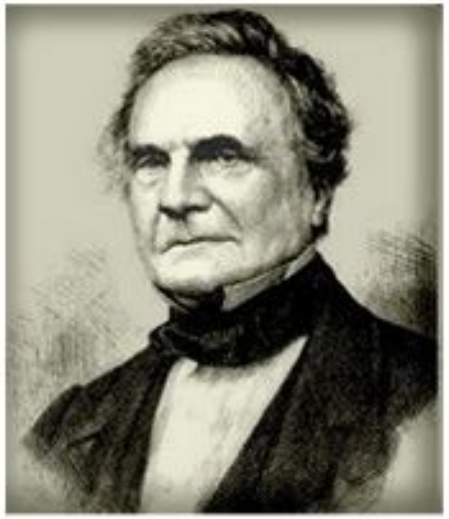
Огюст Керкгоффс

В 80-х годах XIX века издал книгу *"Военная криптография"* объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии.

Керкгоффс сформулировал общие требования к шифрам:

- **простота практического использования;**
- **надежность;**
- **операции шифрования и расшифрования не должны требовать значительных затрат времени.**

Чарльз Бэббидж



Бэббидж одним из первых математиков начал применять алгебру в области криптографии.

Алгебраическое моделирование шифров и их алгебраический анализ помогли ему проникнуть во внутренний смысл шифров.

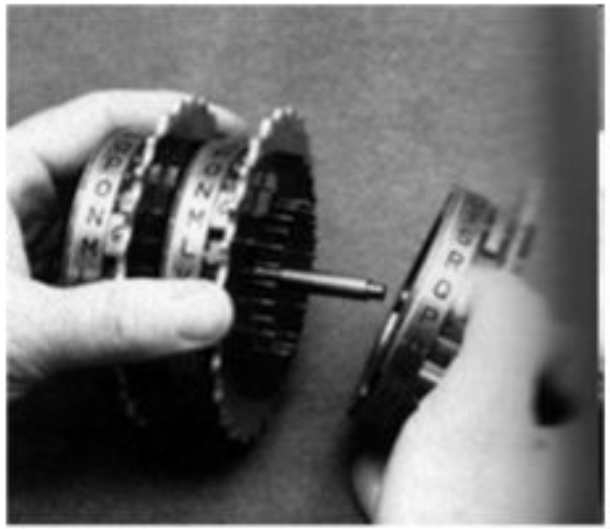
Однако содержание его математических замыслов в области их криптографического применения, к сожалению, в значительной степени утрачено.

Маркиз де Виари

Одним из первых после Бэббиджа предложил использовать алгебраические уравнения для описания процессов шифрования.

Им было положено начало механическому, а затем и электрическому воплощению шифров.

XX век
Революция в шифровании



Метод Гильберта Вернама

Вернам предложил использовать «*гамму*» -перфоленту со случайными знаками для шифрования телетайпных сообщений

Электромеханические шифраторы

Энигма, М-209

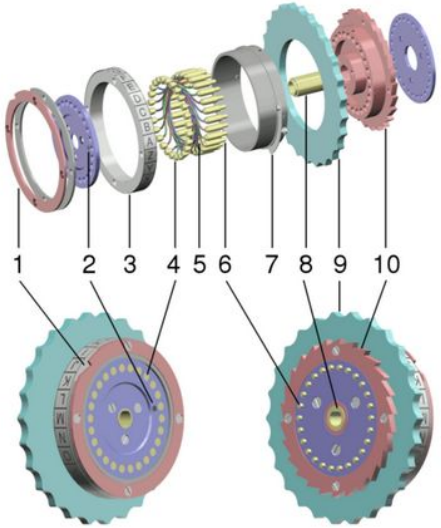
Клод Шеннон

«Теория связи в секретных системах»

Энигма

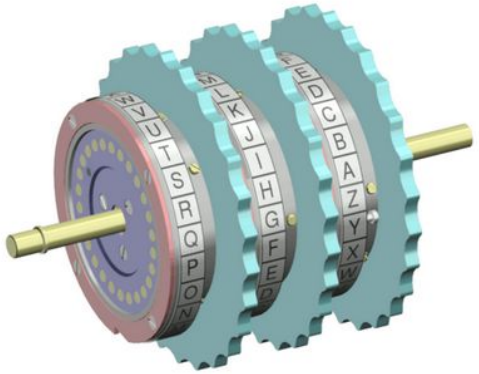
Эни́гма (от др.-греч. αἴνιγμα — загадка) — портативная шифровальная машина, использовавшаяся для шифрования и дешифрования секретных сообщений. Более точно, Энигма — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века.

Ротор в разобранном виде



1. кольцо с выемками
2. маркирующая точка для контакта «A»
3. алфавитное кольцо
4. залужённые контакты
5. электропроводка
6. штыревые контакты
7. пружинный рычаг для настройки кольца
8. втулка
9. пальцевое кольцо
10. храповое колесо

Три последовательно соединённых ротора



«Игра́ в имита́цию» (англ. *The Imitation Game*) — историческая драма о британском криптографе военного времени Алане Тьюринге, который взломал код немецкой шифровальной машины «Энигма» во время Второй мировой войны. Фильм срежиссирован Мортеном Тильдумом по сценарию Грэма Мура, основанному на романе «Алан Тьюринг: Энигма» Эндрю Ходжеса. Главную роль исполнилБенедикт Камбербэтч.

XX век
Революция в шифровании

- В 70-х годах XX века в США был принят первый гражданский стандарт на криптографическую защиту информации (DES, *Data Encryption Standard*)
- В 1976 г. Уитфрид Диффи *(Diffie)* и Мартин Хеллман *(Hellman)* предложили революционную концепцию криптографии с открытым ключом

Домашнее задание
Задача №1

1.5. Дана криптограмма:

ФН	×	Ы	=	ФАФ
+		×		−
ЕЕ	+	Е	=	НЗ
=		=		=
ИШЛА	+	МР	=	ИМН

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст.

Домашнее задание
Задача №2

2.5. Сообщение, записанное в алфавите

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ

зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении ее порядкового номера в алфавите с порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфавита, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Восстановите два исходных сообщения, каждое из которых содержит слово КОРАБЛИ, если результат их зашифрования при помощи одной и той же шифрующей последовательности известен:

ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ и ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ

Домашнее задание
Задача №3

2.6. Буквы русского алфавита занумерованы в соответствии с таблицей:

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	Ь	Ы	Э	Ю	Я
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	26	27	28	29	30

Для зашифрования сообщения, состоящего из n букв, выбирается ключ K — некоторая последовательность из n букв приведенного выше алфавита. Зашифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма.

Прочтите шифрованное сообщение: РБЬНТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.