1 История Криптографии

История криптографии началась около 4 тысяч лет назад. Её периодизируют по технологическим характеристикам используемых методов шифрования.

1. Первый период(с 3-го тысячелетия до н.э. и до IIX века): Основной принцип - замена алфавита через замену одних букв на другие буквы или символы
2. Второй период(с IX века до начала XX века) Впервые появляются полиалфавитные шифры(полиалфавитный шифр - шифр, состоящий из нескольких шифров простой замены, которые используются для шифрование очередного символа. Выбор текущего шифра простой замены осуществляется согласно некоторому правилу)
3. Третий период(нач. XX до сер. XX века) Появляются электромеханические устройства, которые шифруют и расшифровывают текста. Но при этом активно используются полиалфавитные шифры.
4. Четвёртый период - с 70-ых годов XX века - н.в.) Математическая криптография, т.е. шифрование с открытым ключом. В нашей жизни мы настолько часто сталкиваемся с криптографией, что она стала неотъемлимой частью нашей жизни:
   (a) Электронные подписи
   (b) Запросы в браузере(по протоколу https)
   (c) Защита транзакций(банковские переводы, блокчейн транзакции)

1.1 Первый период

Первым известным применением криптографии приянто считать использование специальных иероглифов около 4000 лет назад в Древнем Египте. Но криптография египтян использовалась не с целью зашифровать текст. Писцы в Древнем Египте соревновались в изобретательности, чтобы привлечь внимание к своим текстам.

1.1.1 Атбаш

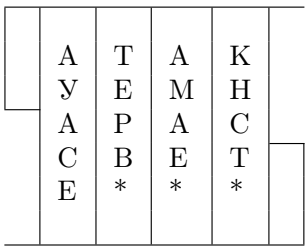
Примеры использования криптографии можно встретить в священных писаниях, например, в книге пророка Иеремии(VI век до н.э.) использовался шифр **Атбаш**, где буквы заменялись по формуле: i-ая буква алфавита заменялась на $n - i + 1$-ую букву алфавита(n - размер алфавита).

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

1.1.2 Скитала

А в Древней Спарте использовался шифр **Скитала**. Для шифрование нужен цилиндр и узкая полоска пергамента, на которой писалось сообщение. Потом полоску наматывали на цилиндр по спирали так, чтобы не было ни нахлестов, ни просветов. Сообщение пишут на намотанной пергаментной ленте по длинной стороне цилиндра. После этого, как достигался конец ленты, цилиндр поворачивался на часть оборота и написание сообщение продолжалось.

Схема:

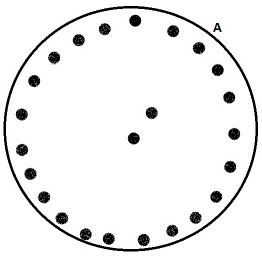


А после разматывания ленты, шифротекст будет таким: "АУАСЕТЕРВ*АМАЕ*КНСТ*"

1.1.3 Диск Энея

Диск Энея представлял собой диск диаметром 13-15 см и толщиной 1-2 см с проделанными в нем отверстиями, количество которых равнялось числу букв в алфавите.

Каждому отверстию сопоставлялась конкретная буква, а в центре находилась катушка с ниткой



На самом деле, диск Энея нельзя назвать криптографическим инструментом, так как прочитать зашифрованное сообщение мог каждый желающий. Но именно это устройство стало прародителем первого поистине криптографического инструмента: линейка Энея.

1.1.4 Линейка Энея

Линейка Энея - один из первых криптографических инструментов, используемый в передаче важных сообщений.

Количество отверстий в линейке равнялось количеству букв в алфавите. Каждому отверстию сопоставлялась буква(в произвольном порядке). К линейке прикреплялась катушка с ниткой. При шифровании нить протягивалась через прорезь, затем через отверстие первой буквы шифруемого текста(в месте прохождения завязывался узелок). Затем нить возвращалась в прорещь и аналогично шифровалась вторая буква текста. После шифрования нить извлекалась и переавалась получателю.

1.2 Средневековье и эпоха Возрождения

Современная криптография возникла среди арабов. Именно они первые систематически задокументировали криптоаналитические методы. Аль-Кинди изобрел метод частотного криптоанализа, который описал в своей книге "Манускрипт о дешифровке криптографических сообщений". Так же, именно арабы внесли в словарь криптологии такие понятия, как алгоритм и шифр.

Самый ранний пример омофонического шифра подстановки(в омофоническом шифре каждая буква может заменяться на несколько различных букв, чтобы скрыть настоящую частоту повторения исходной буквы) использовался герцогом Мантуйским в начале XV века.

По существу, все шифры осталавись уязвимыми для метода частотного криптоанализа до разработки полиалфавитного шифра, и многие оставались такимы и после этого. Полиалфавитный шифр был наиболее ясно описан Леоном Баттистом Альберти около 1467 года. За это он был назван "отцом западной криптографии". Французский криптограф Блез де Виженер разработал метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Шифр Виженера

Шифр Виженера состоит из послежовательности нескольких шифров Цезаря с различными значениями сдвига. А значение сдвига определяется ключевым словом. Шифровка и дешифровка осуществляется с помощью таблицы 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

Пример: Пусть исходный текст имеет вид: **ATTACKATDAWN**, а ключевое слово - **LEMON**

Тогда ключевое слово записывается циклически, пока его длины не будет соответствовать длине исходного текста:

LEMONLEMONLE

Далее первый символ исходного текста(A) зашифровывается последовательностью L. Первый символ шифротекста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст:	ATTACKATDAWN
Ключевое слово:	LEMONLEMONLE
Шифротекст:	LXFOPVEFRNHR

1.2.1 С XIX Века до Второй мировой войны

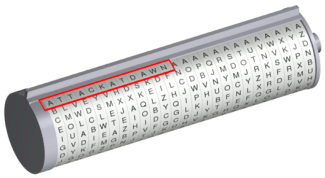
Несмотря на то, что криптография имеет долгую и сложную историю, только в XIX веке что-то большее, чем специальные подохды к шифрованию и криптоанализу. Например, Чарльз Бэббидж во время Крымской войны научился расшифровывать шифр Виженера с автоключом. Но его открытие держали в военном секрете и его результаты не публиковались.

В Первой мировой войне, криптоаналитический отдел Британского Адмиралтейства взломал немецкие шифры, что сыграло важную роль в нескольких морских сражениях во время войны, в частности - в обнаружении крупных немецких вылазок в Северном море.

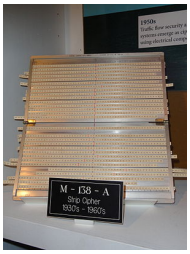
Наиболее известным результатом работы криптоаналитиков временя Первой мировой войны является расшифровка телеграммы Циммермана, подтолкнувшая США к вступлению в войну на стороне Антанты.

1.3 Криптография во время Второй Мировой Войны

Во Вторую Мировую Войну широко использовались механические и электромеханические шифровальные машины, но иногда их использование было непрактичным, поэтому не пренебрегали ручными методами шифрования. Например, в условиях, близким к боевым, США использовали M-94 и M-138-A, в основе которых лежит полиалфавитный шифр.

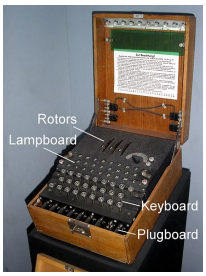


M-94

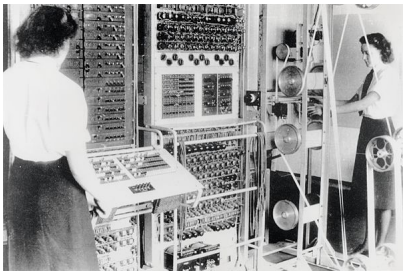


M-138-A

Германия создала электромеханическую роторную машину, известную как Enigma.



Но польский математик Мариан Реевский, в польском бюро шифров, в 1932 году выяснил структуру Енигмы, используя математику и части документации Енигмы. На протяжении 7 лет они продолжали читать зашифрованные немцами сообщения, несмотря на то, что Енигма много раз улучшалась. С 1939 года с ними трудились и английские математики(например, Алан Тьюринг). Вскрое немцы поменяли шифр, который англичане назвали "Танни". Их новая шифровальная машина имела не 5 колес, как Энигма, а целых 12. Билл Татт построил статистическую модель "Танни". Но статистический анализ требовал большого объема вычислений, для выполнения которых создали Colossus.



Криптографы США смогли взломать Японский шифр JN-25. Это помогло США выиграть Мидуэйское сражение.

1.4 Криптография с открытым ключом

Криптографическая система с открытым ключом - система шифрования или электронной подписи, при которой открытый ключ передается по открытому каналу и используется для шифрования сообщения. А для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом широко используется в сетевых протоколах: SSL, SSH.

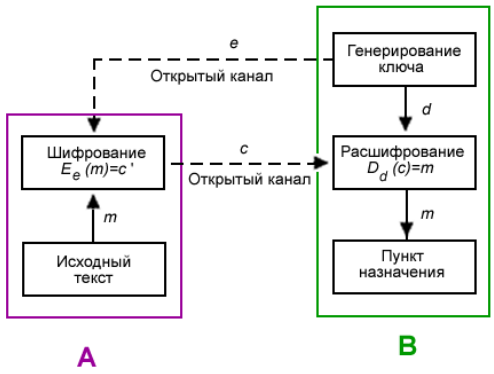


Рис. 1: Схема

В основе известных криптографических систем лежат функции, найти обратную к которым очень сложно. Например, RSA держится на сложности факторизации больших чисел, схема Эль-Гамаля - на сложности вычисления дискретного логарифма.