

Криптография

Лекция 0. Вводная.

Дмитрий Яхонтов

“Кочерга”, 2018

История. Древний мир

- Месопотамия, Египет, Индия

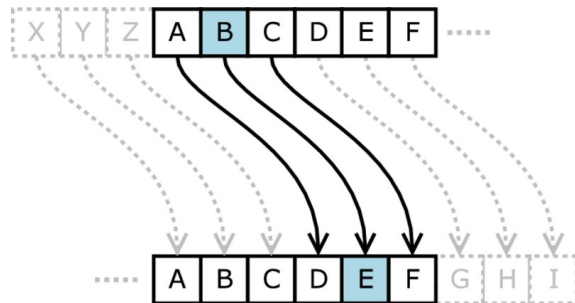
Криптография появляется почти сразу после возникновения письменности и представляет собой скорее искусство, чем науку

- Греция и Рим

IV в до н.э. — шифры Энея

II в до н.э. — квадрат Полибия

I в до н.э. — шифр Цезаря



	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Υ
5	Φ	X	Ψ	Ω	

Средние века

- Шифры перестановки
- Одноалфавитные шифры замены
- Омофонические замены

(одному символу соответствует несколько символов кодового алфавита)

с VII в н.э. — развитие криптографии в арабских странах

IX в н.э. — Аль-Кинди “Манускрипт о раскрытии тайных сообщений”

- Атака по открытому тексту
- Частотный анализ

Возрождение

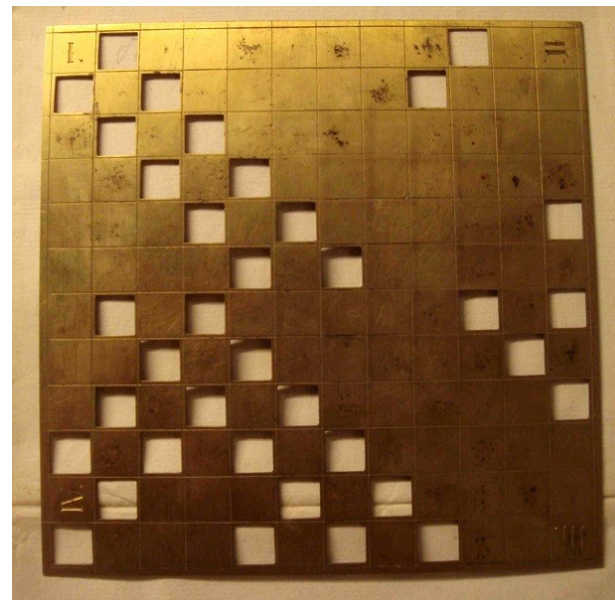
- Биграммные и триграммные шифры замены
- Полиалфавитные шифры

1452 г. — первая организация, специализирующаяся на криптографии

1550 г. — решётки Кардано

1585 г. — шифр Виженера

М	У	Р	Р	Е	Т	Т	У	Р	Л	А	И	Н	Т	Е	Х	Т
К	О	С	Н	Е	Р	Г	А	К	О	С	Н	Е	Р	Г	А	К
10	14	2	7	4	17	6	0	10	14	2	7	4	17	6	0	10
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
W	M	R	Y	I	K	Z	Y	Z	Z	C	P	R	K	K	X	D



Новое время

1830е гг. — появление телеграфа, рост интереса к криптографии

1863 г. — Фридрих Касиски. Метод вскрытия полиалфавитных шифров

1883 г. — Огюст Керкгоффс “Военная криптография”

1. шифр должен быть математически, или хотя бы физически невскрывается
- 2. система не должна требовать сохранения в тайне
(секретным должен быть только ключ)**
3. ключ должен быть простым и легко изменяемым
4. система должна быть пригодна для сообщения через телеграф
5. работа с системой не должна требовать помощи нескольких лиц
6. система должна быть проста в использовании

Первая мировая война

- Использование криптографии на фронте повсеместно
- Словарные и табличные шифры

1917 г. — шифр Вернама (одноразовые шифроблокноты)

P L A I N T E X T
11111 11110 00100 00011 11011 10101 00010 10010 10101

----- XOR -----

E C X J P O Q D S
00010 01101 10010 01100 11111 00111 11101 01111 10001

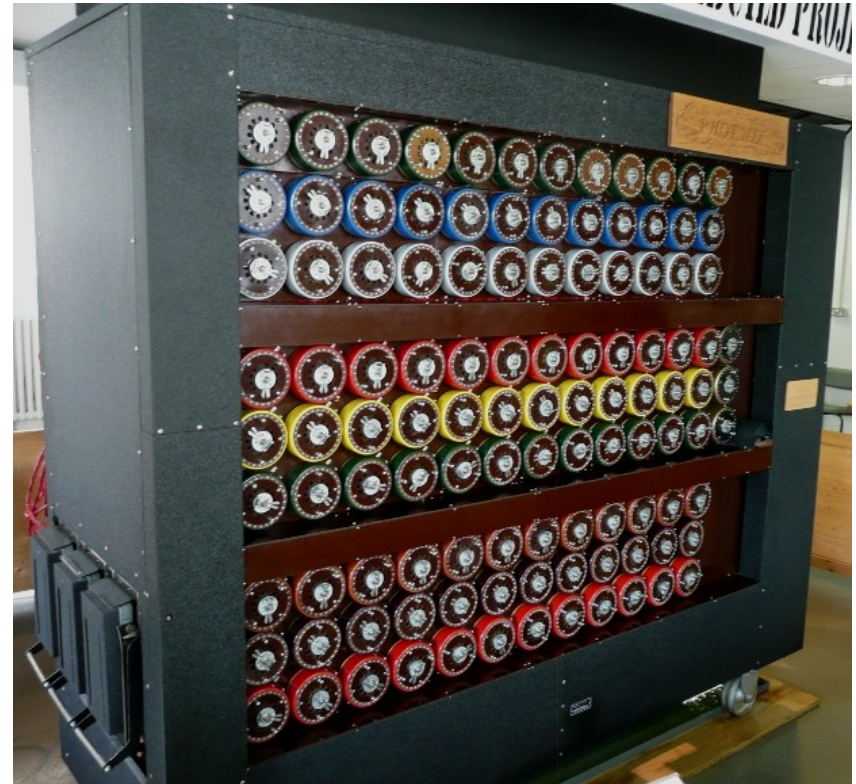
=====

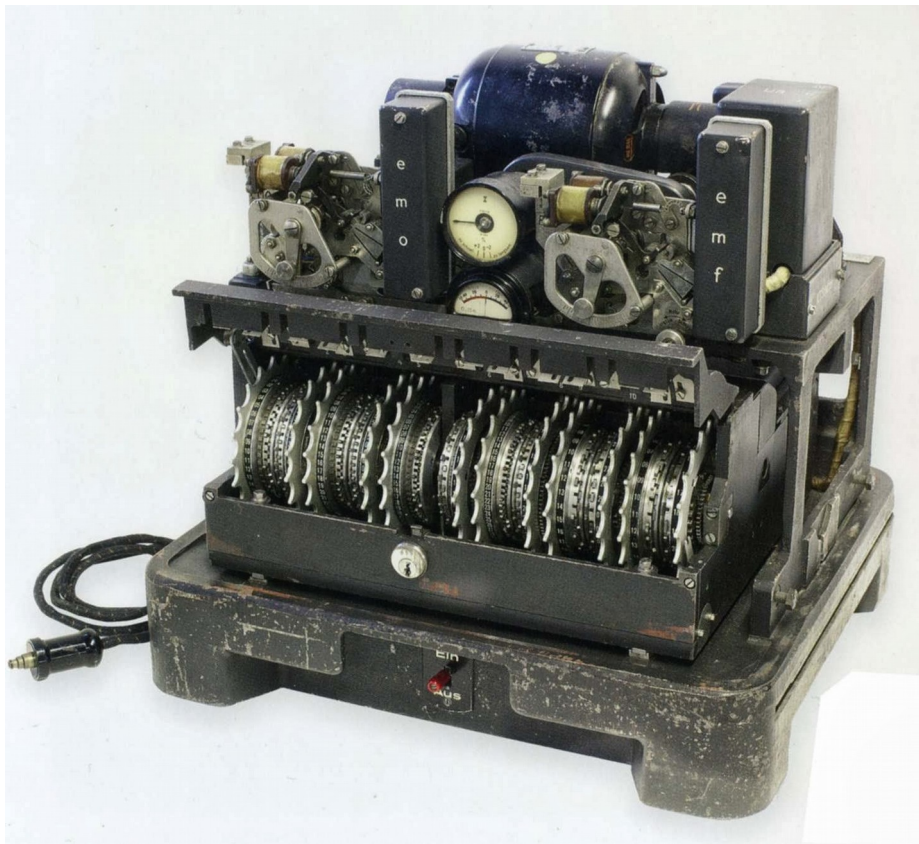
Q W Z D A X P Q U
11101 10011 10110 01111 00100 10010 11111 11101 00101



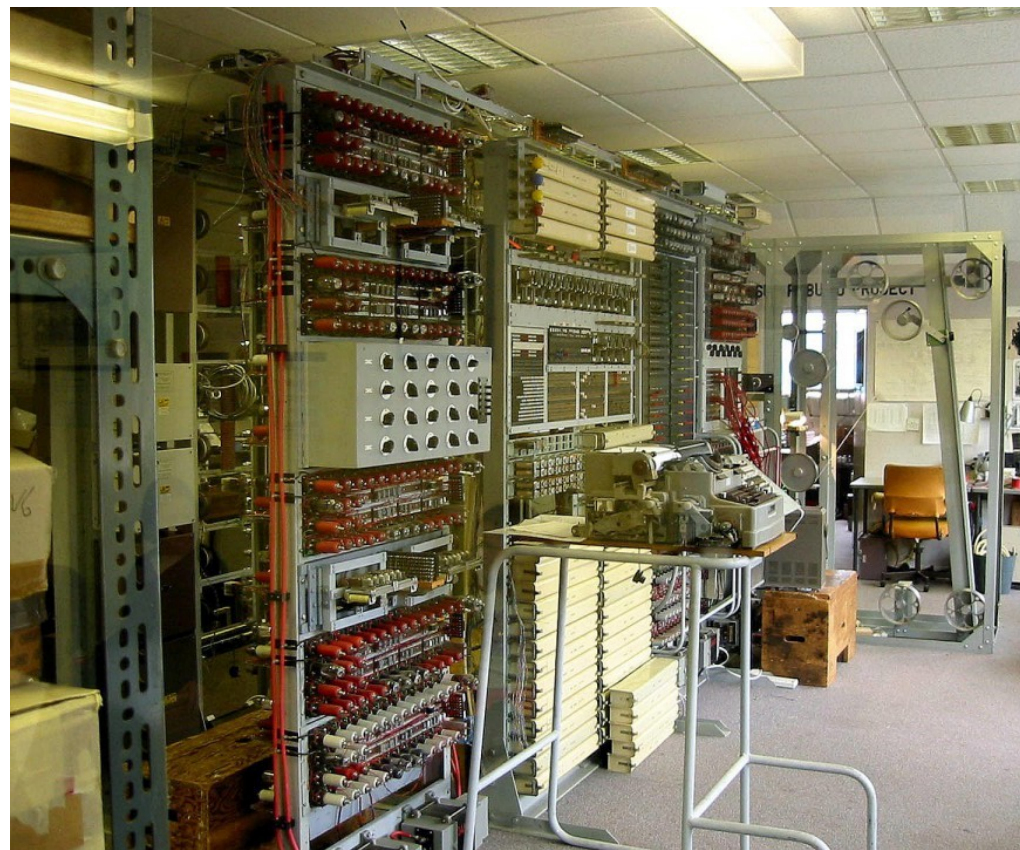
Вторая мировая война

- Электромеханические машины
- Компьютеры для криптоанализа





Шифровальная машина *Lorenz*



Компьютер *Colossus*

Вторая половина XX века

- Блочные шифры
- Асимметричная криптография
- Открытые стандарты

1949 г. — Клод Шеннон “Теория связи в секретных системах”

1960-е гг. — блочные шифры на ячейках перестановки и замены

1976 г. — Уитфилд Диффи и Мартин Хеллман

“Новые направления в криптографии”

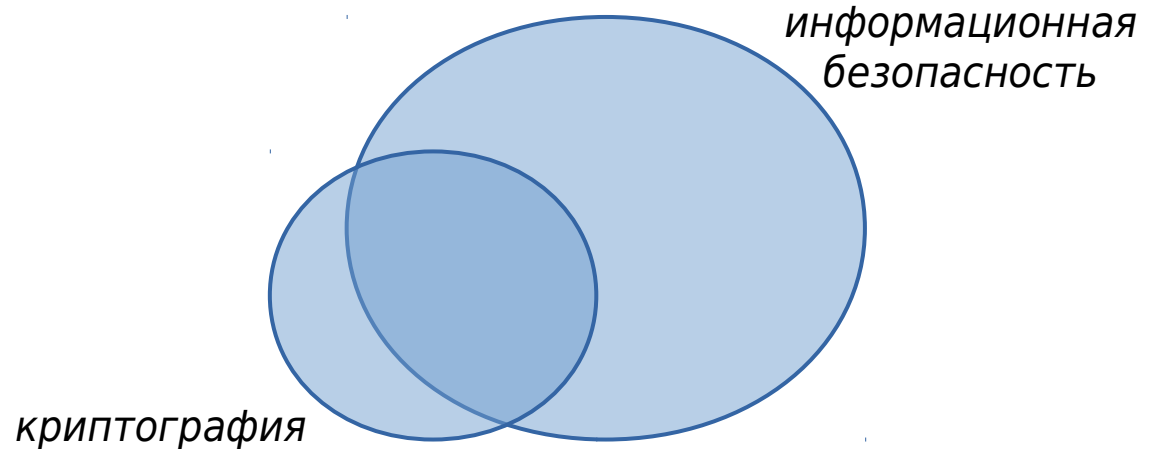
1977 г. — Рональд Ривест, Ади Шамир и Леонард Адлеман

Алгоритм RSA

1997-2000 гг. — конкурс AES (Advanced Encryption Standard)

Криптография — наука об алгоритмических методах обеспечения

- конфиденциальности
- целостности данных
- аутентификации
- невозможности отказа от авторства



Криптоанализ — наука о методах расшифровки данных без ключа

- полное вскрытие — нахождение ключа шифрования
- местная дедукция — восстановление открытого текста
- частичное вскрытие — получение некоторой информации
об открытом тексте

Виды криптоанализа:

- по шифротексту
- по паре “открытый текст – шифротекст”
- по произвольному открытому тексту

Принцип Керкгоффа

Стойкость криптосистемы не должна быть основана на том, что алгоритмы держатся в тайне. “Враг знает систему”.

Единственным секретным элементом должен быть ключ.

Нарушение этого принципа —

Безопасность через неясность (англ. *Security through obscurity*)

Имена агентов



Alice (A)

стороны-участники протокола



Bob (B)



Carol (C)

ещё участники



Dave (D)



Eve (Eavesdropper) — пассивный злоумышленник



Mallory (Malicious) — активный злоумышленник



Trent (Trusted) — доверенный арбитр