

ПОГРУЖЕНИЕ В ТАЙНЫ ДЕШИФРОВКИ И КРИПТОЛОГИИ

Вецпиебалга 2011

Что такое расшифровка?

Можно выделить три вида:

- Дешифровка (расшифровать = перевести)
- Криптография (расшифровать = рассекретить)
- Стеганография (расшифровать = проявить «невидимку»)

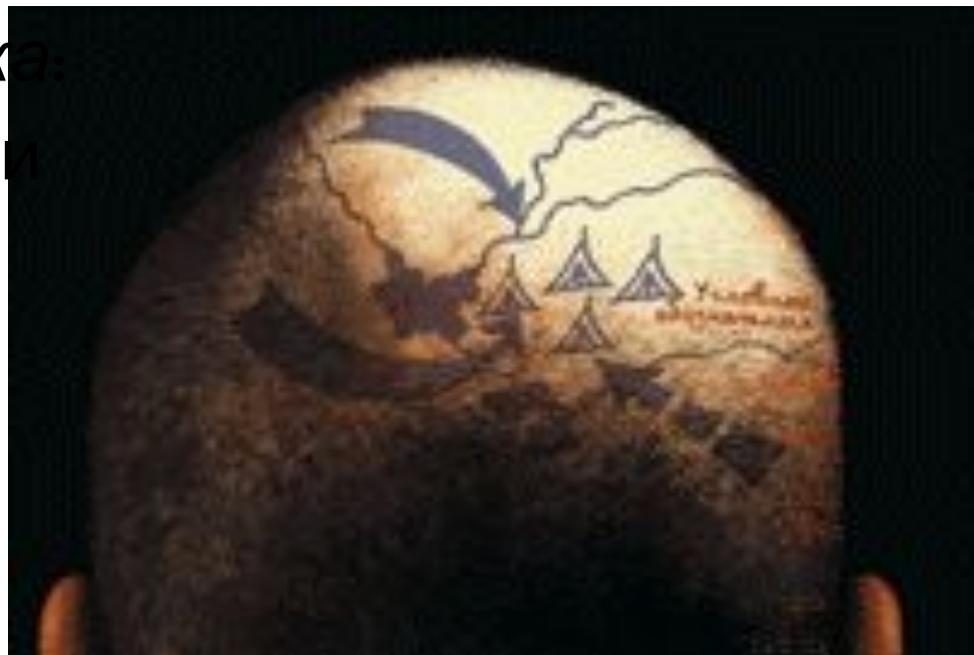
Стеганография

Стеганография (от греч. *στεγανός* — скрытый и *γράφω* — пишу, буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Задача расшифровщика:
понять способ передачи

Примеры:

невидимые чернила,
побрить раба



Криптография

Криптогра́фия (от др.-греч. κρυπτός — скрытый и γράφω — пишу) — наука о методах обеспечения конфиденциальности информации (невозможности прочтения информации посторонним) .

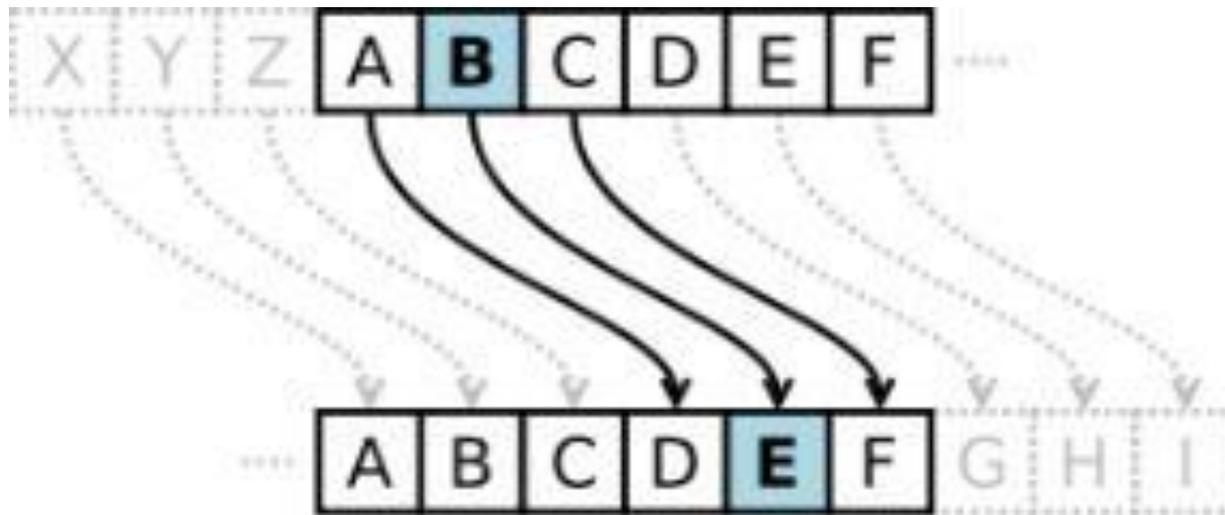
Задача расшифровщика: подобрать ключ

- Шифры подстановки
- Шифры перестановки

Криптография: шифры подстановки

- Шифр Цезаря
- Квадрат Полибия

	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



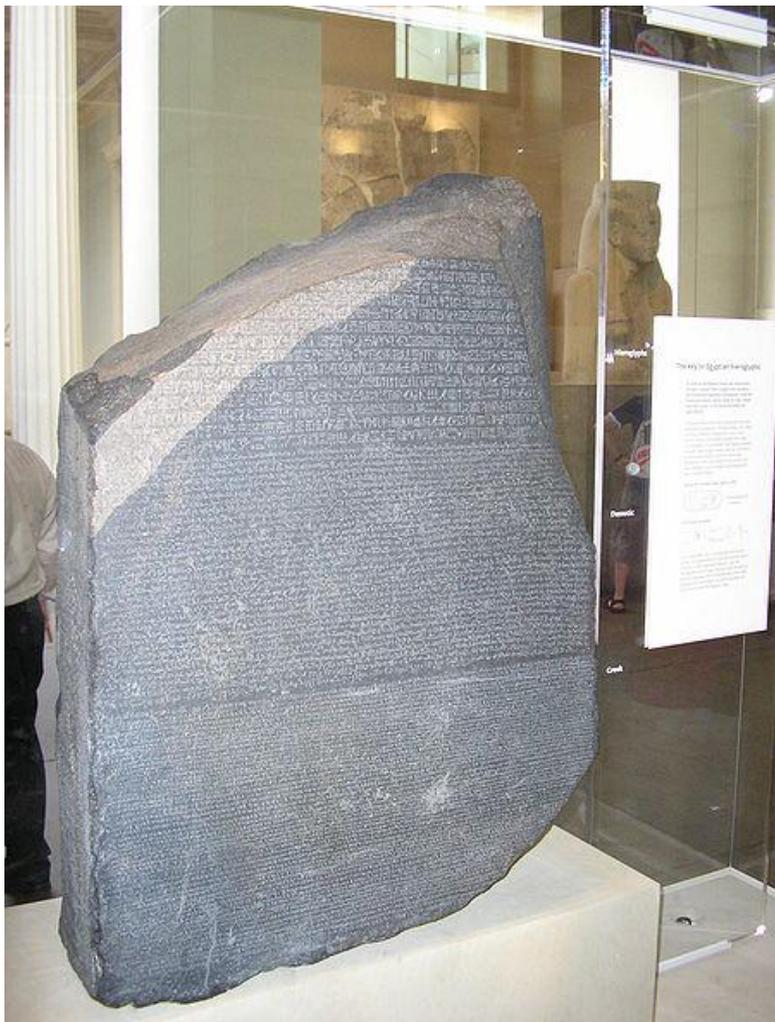
Дешифровка

Дешифровка — анализ документа, написанного на неизвестном языке и/или неизвестной системой письма

Задача расшифровщика: анализируя исторический документ, перевести его.

Дешифровка египетских иероглифов

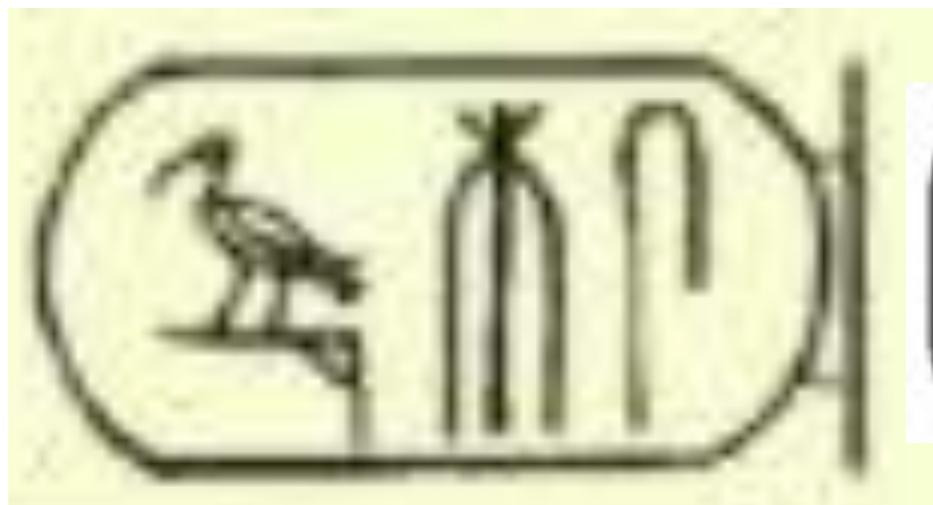
Розеттский камень



Жан-Франсуа Шампольон



Картуши



Известно:



Язык «без гласных»

- Египетские иероглифы:



CHRISTOPHER=KRISTOFR

- Арабский:
 - كَتَبَ — КаТаБа — *он писал*
 - أَكْتُبُ — аКТуБу — *я пишу*
 - كِتَابٌ — КиТа:Бун- *книга*
 - كُتُبٌ — КуТуБун — *книги*

Определители

Определитель помещался в конце слова и служил для пояснения смысла написанного и не обозначал никаких звуков или слов

□ человек, мужчина



□ женщина



□ глаз, смотреть, видеть



□ ночь, темнота



Фотографии



Фотографии



Фотографии

