Криптография - это наука о том, как обеспечить секретность сообщения

Криптология - это раздел математики, изучающий математические основы криптографических методов

Периоды криптографии:

1. Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами)

ШИФР ЦЕЗАРЯ
(шифр сдвига, сдвиг Цезаря)

Пример шифра Цезаря (шифрование с использованием ключа К=3) :

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

Зашифруем слово «FAMILI»
Получаем: IDPLOL (сдвиг на 3)

Пример шифрование с использованием ключа К=3 в русском алфавите.

Исходный алфавит:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный:

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Оригинальный текст:

Ученикам, чтобы преуспеть, надо догонять тех, кто впереди, и не ждать тех, кто позади.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Ццъзрлнгп ъхсдю тузцфтзхя ргжс жсёсрхя хзш нхс етзузжл л рз йжгхя хзш нхс тскгжл

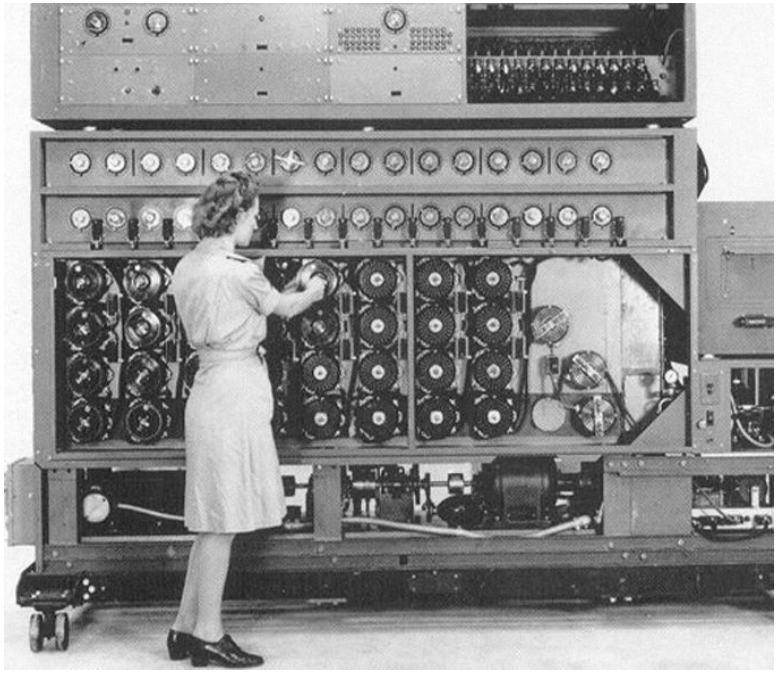
2. Второй период (хронологические рамки — с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века) ознаменовался введением в обиход полиалфавитных шифров

Например, в процессе шифрования используется таблица Виженера, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой и равно числу букв алфавита.

	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

3. Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

К примеру, немецкая машина «Энигма», использовалась для шифрования засекреченной информации во время второй мировой войны.
Вторая мировая война послужила своеобразным катализатором развития компьютерных систем — через криптографию.



Wehrmacht Enigma («Энигма»)

Шифровальная машина Третьего рейха. Код, созданный при помощи «Энигмы», считается одним из сильнейших из использованных во Второй мировой.

Turing Bombe («Бомба Тьюринга»)

Разработанный под руководством Алана Тьюринга дешифратор. Его использование
позволило союзникам расколоть казавшийся монолитным код «Энигмы».

4. Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической» или же, более корректно, криптографией с секретным ключом.

5. Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом.

Криптоанализ - это наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа.

Взаимосвязь алгебры и критологии

Опр. 1. Шифрование - это обратимое преобразование открытого текста в шифртекст. Оно определяется двумя взаимно обратными отображениями,

Ek: T $\rightarrow$C и Dk: C$\rightarrow$T,

где T - множество открытых текстов, C - множество всех шифртекстов, k -- ключ, выбираемый из пространства ключей K. Если обозначить через E множество {Ek: k$\in$K} всех отображений зашифрования, а через D множество {Dk: k$\in$K} всех отображений дешифрования, то для любых t $\in$T, k$\in$K выполняется равенство

Dk(Ek(t)) =t.

Тогда совокупность (T, C, K, E, D) называется шифром, или шифр-системой.
Простейшими и старейшими классами шифров являются шифры перестановки и шифрзамены. В этих шифрах C =T =, где A - алфавит текста, n - длина сообщения.

Опр. 2. Роль ключа k в шифре перестановки играет произвольная перестановка k∈Sn из группы перестановок множества {1, ..., n}; таким образом, пространство ключей K=Sn, отображение шифрования определяется равенством:

$$E_k\,(a_1, a_2, \ldots a_n) = a_{k(1)} a_{k(2)} \ldots a_{k(n)},$$

а отображение расшифрования определяется равенством:

$$D_k(a_1, a_2 \ldots a_n) = a_{k-1(1)} a_{k-1(2)} \ldots a_{k-1(n)}.$$

Опр. 3. Роль ключа k в шифре замены, играет произвольная перестановка k∈ Sn из группы перестановок алфавита A; таким образом, пространство ключей K= Sn, отображение шифрования определяется равенством:

$$E_k(a_1, a_2, \dots a_n) = k(a_1), k(a_2), \dots k(a_n),$$

а отображение расшифрования определяется равенством:

$$D_k(a_1, a_2, \dots a_n) = k^{-1}(a_1)k^{-1}(a_2) \dots k^{-1}(a_n).$$

Пример. 1. Если верить истории, то первый шифр перестановки использовали в Спарте. На цилиндр, который назывался сцитала, плотно, виток к витку наматывалась узкая пергаментная лента. Затем, вдоль оси цилиндра записывался текст. Кода ленту снимали с цилиндра, на ней оставалась цепочка букв, на первый взгляд, совершенно беспорядочная. Лента сматывалась и передавалась адресату, который читал сообщение, наматывая ленту на такую же сциталу. После этого текст опять становился понятным. Ключом к шифру является диаметр сциталы. Поэтому она не очень хорошо защищала доверенные тайны, ведь достаточно скоро, Аристотель придумал устройство «антисцитала», который предложил наматывать ленту на конус, сдвигая ее от вершины к основанию конуса. Там, где диаметр конического сечения совпадал с диаметром сциталы, на ленте проступали осмысленные слоги и слова, после чего изготовлялась сцитала соответствующего диаметра и буквы складывались в связный текст.

Пример 2. Первый шифр замены изобрел Юлий Цезарь. В качестве перестановки букв алфавита он использовал просто циклический сдвиг на три буквы. Обратная перестановка тоже, естественно, является циклическим сдвигом.

В общем случае в этом шифре использовался сдвиг вида

$$i \to (i + k) \mathrm{mod} 26,$$

и ключом являлось число k. Так как ключевое пространство невелико, алгоритм шифрования Цезарь, видимо, не особо афишировал.

Пример 3. К классу шифров перестановки относятся шифры маршрутной перестановки. Идея у них такая. Сообщение записывается в таблицу по одному маршруту, например по горизонталям, а считывается по другому, например по вертикалям. Для увеличения ключевого пространства использовалась еще перестановка столбцов таблицы.

ШИФР С ЗАМЕНОЙ БУКВ ЦИФРАМИ

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
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

Например :«LIFE» - «12 9 6 5»

ЦИФРОВАЯ ТАБЛИЦА

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	1	2	3	4
7	5	6	7	8	9
8	0	.	,	?	!

Первая цифра в шифре – столбец, вторая – строка или наоборот. Так слово «MIND» можно зашифровать как «33 24 34 14».

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

1 МЕТОД. Вместо каждой буквы в слове используется соответствующая ей буква снизу (A = F, B = G и т.д.). Пример: CIPHER - HOUNIW.

2 МЕТОД. Указываются соответствующие каждой букве цифры из таблицы. Первой пишется цифра по горизонтали, второй - по вертикали. (A = 11, B = 21…). Пример: CIPHER = 31 42 53 32 51 24

Цветовая таблица

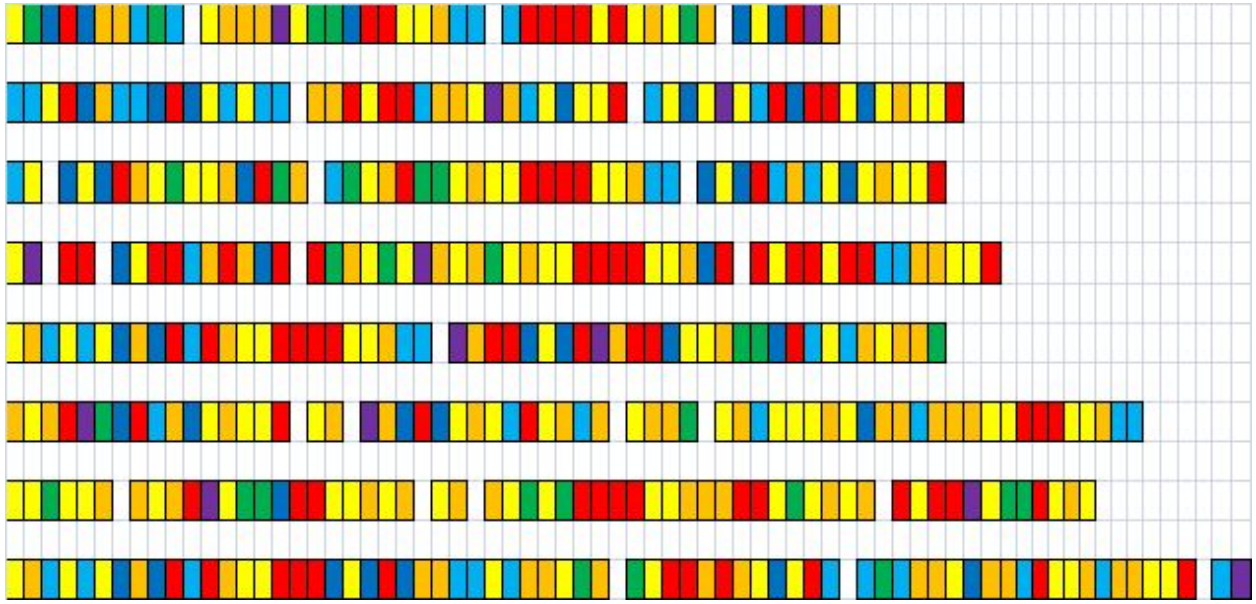
	А	Б	В	Г	Д	Е	Ё
	Ж	З	И	Й	К	Л	М
	Н	О	П	Р	С	Т	У
	Ф	Х	Ц	Ч	Ш	Щ	Ъ
	Ы	Ь	Э	Ю	Я	0	1
	2	3	4	5	6	7	8
	9	.	,	:	;	!	?

Первый цвет в шифре – строка, вторая – столбец

Исходный текст:

Целью изучения данной темы является знакомство студентов с теорией шифрования текстов, а также формирование навыков исследования математических объектов и методики их использования при обучении и организации научно-исследовательской работы школьников; вовлечение студентов в научно-исследовательскую деятельность.

Зашифрованный текст:



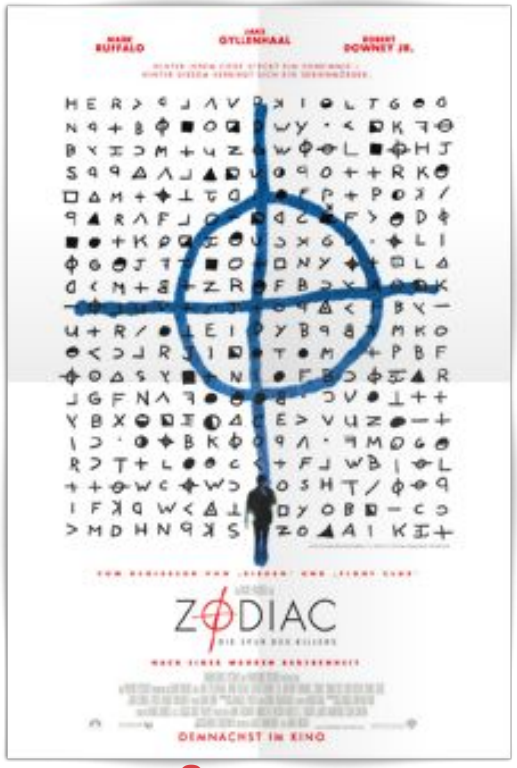
Джулиан Ассанж
Р. 1971

На своем портале WikiLeaks публично продемонстрировал всем желающим изнанку многих государственных структур. Коррупция, военные преступления, сверхсекретные тайны — вообще все, до чего дотянулся деятельный либертарианец, стало достоянием общественности. Помимо этого, Ассанж — создатель адской криптосистемы под названием «Отрицаемое шифрование» (Deniable encryption). Это способ компоновки зашифрованной информации, который обеспечивает возможность правдоподобного отрицания ее наличия.

Ьрэм Коэн

Р. 1975

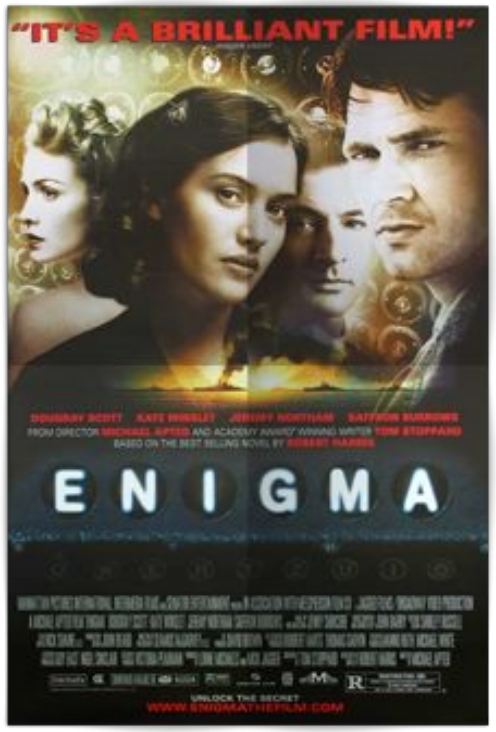
Американский программист, родом из солнечной Калифорнии. На радость всему миру придумал протокол BitTorrent, которым небезуспешно пользуются и по сей день.



Зодиак

2007 Г.

Напряженный триллер Дэвида Финчера, построенный на реальных событиях. Большую часть фильма умнейшие сотрудники полиции Сан-Франциско тщетно пытаются расколоть шифр зарвавшегося маньяка.



Энигма

2001 Г.

Игровой фильм в декорациях Второй мировой войны: блестящие математики собираются в Блетчли-Парке, чтобы разгадать новый шифр коварных нацистов. Картина полна необъяснимых загадок и тайн — впрочем, об этом можно догадаться и по названию.

Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому криптография в будущем станет "третьей грамотностью" наравне со "второй грамотностью" - владением компьютером и информационными технологиями.