Криптография и защита информации

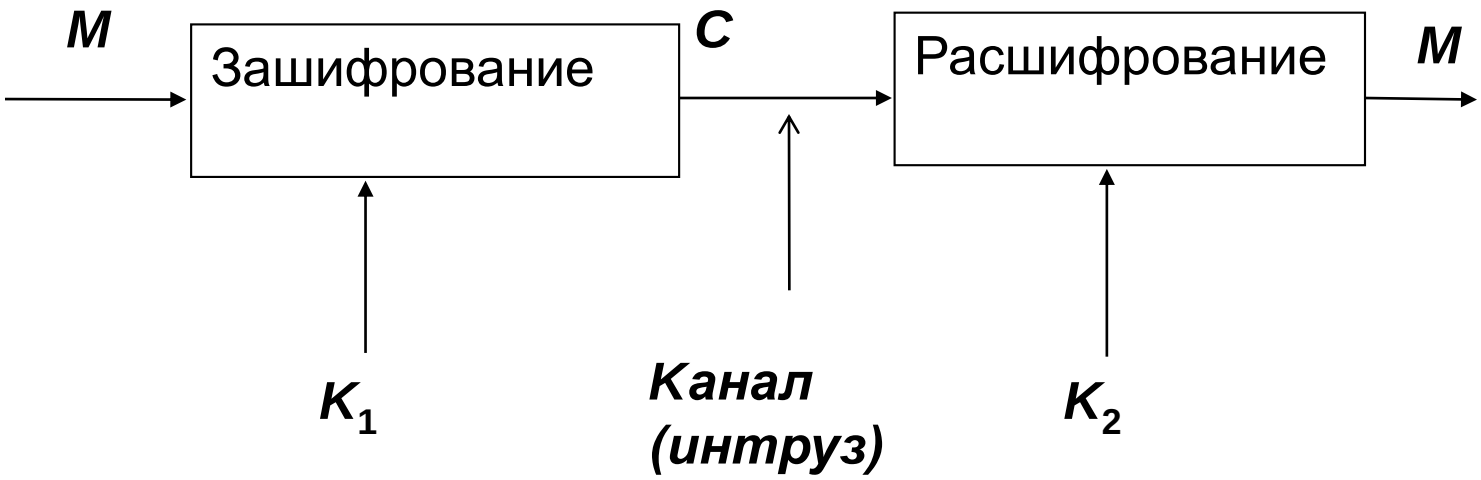
Основные понятия и классификация

Определение 1. Криптография (с греч. *κρσπτός* криптос «тайный"и *γράφω* графо «писать") – наука (раздел математики), о методах обеспечения конфиденциальности или безопасности информации, связанной с тайной, интегральностью данных и идентификацией

Криптоанализ — наука о методах получения исходного значения зашифрованной информации без наличия секретного и не известного аналитику ключа

Определение 2. Криптология (с греч. *κρσπτός* и *λόγος* – логос – «слово")– наука, объединяющая криптографию и криптоанализ.

Определение 3. Криптосистема – это понятие, относящееся к совокупности программно-технических средств, функционирующих на основе установленных криптографических алгоритмов и осуществляющих зашифрование и расшифрование данных



Прямое преобразование называют *шифрованием* или *зашифрованием* (в соответствии со стандартом ISO 7492-2 –*зашифрование*, encrypt),
обратное - *расшифрованием* или *дешифрованием* (*расшифрование*, decrypt).
Исходное сообщение называется *открытым текстом* (*M*, от английского message).
Зашифрованное сообщение – *шифртекстом* или *шифрограммой* (*C*, от английского cipher).

Огюст Керкгоффс (1883) - «Военная криптография»
(фр. *La Cryptographie Militaire*).
Описал шесть требований, которым должна удовлетворять защищённая система.:
1.шифр должен быть физически, если не математически, невскрываемым;
2.система не должна требовать секретности, на случай, если она попадёт в руки врага;
3.ключ должен быть простым, храниться в памяти без записи на бумаге, а также легко изменяемым по желанию корреспондентов;
4.зашифрованный текст должен передаваться по телеграфу;
5.аппарат для шифрования должен быть легко переносимым, работа с ним не должна требовать помощи нескольких лиц;
6.аппарат для шифрования должен быть относительно прост в использовании, не требовать значительных умственных усилий или соблюдения большого количества правил.

•**Определение 4.** **M** означает множество сообщений, состоящих из символов определенного алфавита.

Элемент из **M** открытый текст (**явный**):

$\mathbf{M=m_1, m_2, ..., m_n}$

•**Определение 5.** **C** означает множество сообщений, состоящих из символов того же или иного алфавита.

Элемент из **C** (**шифрограмма**): $\mathbf{C=c_1, c_2, ..., c_n}$

Определение 6. **K** означает множество **ключей** (элемент этого множества - ключ)

- Каждый элемент **e** $\in$ **K** определяет взаимно однозначное отображение (биекцию) M на C и обозначается E_e ($E_e : M \rightarrow C$).
- E_e - функция зашифрованиия,
- Каждый элемент **d** $\in$ **K**, D_d определяет взаимно однозначное отображение (биекцию) C на M и обозначается D_d $D_d : C \rightarrow M$),
- D_d - функция расшифрованиия.
- **Определение 7.** Процесс вычисления значения функции E_e для аргумента m $\in$ M называется зашифрованием явного текста **m**.

Определение 8. Процесс вычисления значения функции D_d для аргумента $c \in C$ называется расшифрованием криптограммы **C**.

- Чтобы сконструировать схему шифрования, нужно выбрать множества **M**, **C**, **K** и определить множества $\{E_e : e \in K\}$ і $\{D_d : d \in K\}$

В проблематике современной криптографии можно выделить следующие три типа основных задач:

1) обеспечение *конфиденциальности* (*секретности*),

2) обеспечение *анонимности* (*неотслеживаемости*),

3) обеспечение *аутентификации* информации и источника сообщения.

Классификация систем шифрования (шифров)

1. **На основе процедуры шифрования**
- Ш. подстановочные
- Ш. перестановочные
2. **На основе генерирования и использования ключа**
- Ш. блочные
- Ш. поточные (потоковые)

3. **На основе типа ключа**
- Ш. симметричные (с тайным ключом): $e=d$
- Ш. асимметричные (с открытым или публичным ключом): $e \neq d$

Подстановочный шифр - замена символов открытого текста соответственно символами того же или иного алфавита - подстановка.

Простым примером является **шифр Цезаря**.

Шифр Виженера (Vigenère) – основан на замене символов открытого текста для значений зашифрованного текста соответственно символами того же алфавита, используя в каждом случае шифр, подобный на ш. Цезаря (с изменением параметра подстановки, ***k*** – на основе квадрата Виженера), а также дополнительную ключевую информацию - ключевое слово.)

Перестановочный шифр – основан на перестановке (пермутации) символов открытого текста.

Примером является **rail fence cipher (**буквально – шифр изгороди**)**, символы открытого текста записываются сверху-вниз с диагональным наклоном, как бы на последовательных «рельсах» воображаемой изгороди, затем двигаясь вверх, когда достигается нижняя «рельса».
Затем сообщение считывается построчно – так формируется окончательный вид ширтекста.
Например, если у нас есть 3 «рельсы» и сообщением является слово 'INFORMATICS', то шифртекстом будет ' IOACNRTSFMI ' :

I - - O - - A - - C
-N - - R - - T - - S
- - F - - M - - I

Наибольшая уязвимость подстаночных и перестановочных шифров – сохранение в зашифрованных документах вероятностных свойств символов используемого алфавита
Пример. Частотные свойства английского алфавита

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
.082	.015	.028	.043	.126	.022	.020	.061	.070
j	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**
.002	.008	.040	.024	.067	.075	.019	.001	.060
s	**t**	**u**	**v**	**w**	**x**	**y**	**z**	
.063	.091	.028	.010	.023	.001	.020	.001	

Наиболее часто встречающиеся пары букв:

“th”, “he”, “in”, “ee”,

и тройки:

“the”, “ing”, “and”

Предположим, что используется аффинная система подстановки:
$e_k(m) = am + b \pmod{26}$, m – символ открытого текста
с неизвестными для криптоаналитика ***a, b***

Предположим также, что анализируется следующий шифртекст:

QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

1.Аналитик подсчитывает встречаемость каждого символа:

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
0	4	4	3	0	1	0	4	0	1	0	6	6	0	4	0	6	3	0	1	1	4	2	5	2	1

2. Из этого следует, что три буквы встречаются чаще других: по шесть раз. Наиболее частовстречающимися двумя буквами в английском тексте являются «e» и «t». Мы предполагаем, что «L» - это шифрование «e»:

- - e- e- - - e- - - - - - - - - - - - - - e - - - - - - - - - - - e - - - - - - - - - - e - - - - - - - - -
QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

3. Полагаем далее, что “Q” – это зашифрованая “t” :

t - e - e- t -e- - - - - - - - - - - - t - e - - - - - t - - - --e - - - - - - - - - -e t - - - - - - t

QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

4 Обращаем внимание, что «t» и «e» располагаются три раза с одной и той же третьей буквой зашифрованного текста «M» между ними, что указывает на то, что «M» - это шифрование «h» (поскольку «the» является известной трехбуквенной последовательностью. Мы приходим к

t h e- e- t h e- - - - h - - - - - - - - t h e - - - - - t - - - - -e - h - - - - - - - - - - e t h - - - - - - t

QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

5. Дальнейшие шаги:

t h ewea t he r - - - h a - - - - - - - - t h ew- r - - t - - a -we - h - - - - - - - - - - - et h - - - - - - t

QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

6. Полагаем далее, что „H” - „s”, „X” - „o”:

t h ewea t he r i s c ha ng i ng i n t h ewo r l d t o da ywes hou l dd os omet h i n g f a s t

QMLRLBQMLYVHTMBODVODVOQMLRXYWCQXCBJRLHMXZWCCXHXFLQMVODUBHQ

Или theweatherischangingintheworldtodayweshoulddosomethingfast

Расшифрованный текст:

THE WEATHER IS CHANGING IN THE WORLD TODAY WE SHOULD DO SOMETHING FAST