Классические криптоситемы

- *Криптология* – наука о создании и анализе систем безопасности связи. Говоря о криптологии, иногда имеют в виду не безопасную, а секретную связь. Однако секретность является только одним элементом безопасности или целостности информации. Целостность информации связана с вопросами подлинности, своевременности, согласованности и т.д., а также со всеми вопросами, обычно возникающими с документными записями.
- Криптологию принято делить на две части: криптографию и криптоанализ. *Криптография* - это наука о методах обеспечения секретности и подлинности (идентичности) данных при их передаче по линиям связи или хранении. *Криптоанализ* – это наука о методах раскрытия или подделки данных. Иными словами криптография и криптоанализ нацелены на решение взаимно обратных задач.

Цели криптографии менялись на протяжении всей её истории. Сначала она служила только для обеспечения секретности, чтобы препятствовать несанкционированному доступу к информации, передаваемой по военным и дипломатическим каналам связи. По мере развития информатики криптография носила широкое применение для защиты информации во многих прикладных областях: истории болезни, юридические и финансовые документы, закрытые коммерческие данные и т.п.

В настоящие время криптография используется не только не только для защиты информации от несанкционированного доступа, но и для обеспечения её подлинности и целостности криптографических систем применяются физическая защита, различные организационно - технические мероприятия и стеганография. Стеганография занимается методами скрытия самого факта передачи сообщения (симпатические чернила, молоко для написания текста, шумоподобные методы радиопередачи и д.р.).

- Открытым текстом называют исходные сообщение, которое должен защищать криптограф.
- Шифр - это множество обратимых преобразований формы открытого текста, проводимых с целью его защиты.
- Процесс применения обратимого преобразования шифра к открытому тексту называется *зашифрованием*, а результат этого преобразования - *шифротекстом* или *криптограммой*. Соответственно процесс обратного преобразования шифротескта в открытый текст называется *расшифрованием*. Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра, называют *ключом*. Такой ключ, в частности, может передаваться отправителем получателю заранее до отправления криптограммы каким - либо надежно защищенным способом.

Дешифрование - атака на шифр, раскрытие шифра со стороны взломщика. Специальным видом шифра является код. *Код* - это своего рода словарь, где элементы открытого текста (буквы, сочетания букв, слова и даже фразы) так называемые *кодвеличины* заменяются группами символов (букв, цифр, других знаков). Эти группы символов называют *кодообозначениями*. Принципиальной разницы между шифром и кодом нет.

Одним из основных понятий криптографии является стойкость. *Стойкость* - это способность противостоять попыткам хорошо вооруженного современной техникой и знаниями криптоаналитика дешифровать перехваченный шифротекст, раскрыть ключи шифра или нарушить целостность и подлинность информации.

В истории развития криптографии можно условно выделить три основных этапа. Первый период - эра донаучной криптологии, являющейся уделом узкого круга искусных умельцев.

Началом второго периода можно считать 1949 год, когда появилась работа известного американского ученого Клода Шеннона «Теория связи в секретных системах». В этой работе проведено фундаментальное научное исследование шифров и вопросов их стойкости, благодаря чему криптология оформилась как прикладная математическая наука.

Третий период связывают с появлением в 1976 году работы У. Диффи и М. Хеллмана «Новые направления в криптографии, « где показано, что секретная связь возможна без предварительной передачи секретного ключа.

Ещё несколько веков назад само применение письменности можно было рассматривать как способ закрытия информации, т.к. владение письменностью было уделом немногих.

Один из самых древних шифротекстов, написанных клинописью, был обнаружен в Месопотамии и датируется *XX* веком до н.э. Известны также древнеегипетские религиозные и медицинские шифротексты.

В середине *IX* века до н.э. использовалось шифрующие устройство - *скиталь* для получения шифра перестановки. При шифровании слова писались на узкую ленту, намотанную на цилиндр, вдоль образующей этого цилиндра (скиталя). После этого лента разматывалась и на ней оставались переставленные буквы исходного текста. Ключом в этом случае являлся диаметр этого цилиндра

В начале нашей эры создается *шифр замены*. Так в 56 году н.э. во время войны с галлами Юлий Цезарь использует *шифр простой замены*, строящийся следующим образом:

Под алфавитом открытого текста пишется тот же алфавит со сдвигом на три позиции по циклу. При шифровании буквы открытого текста у верхнего алфавита заменялись буквами нижнего алфавита.

А Б В Г Д Е Ж … Э Ю Я

Г Д Е Ж … Э Ю Я А Б В

Полибианский квадрат. Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (203-120 гг. до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы (необязательно в алфавитном порядке).

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения вначале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца.

Тюремный шифр. Эта звуковая разновидность полибианского квадрата была разработана заключенными. Система состояла из нескольких ударов, обозначающих строки и столбцы в таблице с буквами алфавита. Один удар, а потом еще два соответствовали строке 1 и столбцу 2, т.е. букве **Б**. Пауза служила разделителем между строками и столбцами. Таким образом, зашифровать исходное сообщение «АБРАМОВ» можно следующим образом.

А	тук ___ тук
Б	тук ___ тук, тук
Р	тук, тук, тук ___ тук, тук, тук, тук, тук, тук
А	тук ___ тук
М	тук, тук, тук ___ тук, тук
О	тук, тук, тук ___ тук, тук, тук, тук
В	тук ___ тук, тук, тук

В начале *XV* века н.э. Альберти предложил оригинальный шифр замены, на основе двух концентрических кругов, по окружности которых записывались алфавиты открытого текста и шифротекста. При этом шифроалфавит был не последовательным АБВГ… ЭЮЯ, а произвольным АЭВЮГ… и мог быть еще и смещен на любое число позиций.

Здесь была впервые реализована идея увеличения стойкости шифросистемы путем повторения шифрования с помощью разных шифросистем (меняя последовательность шифроалфавита и его сдвиг относительно алфавита открытого текста).

В *XVI* веке н.э. французский дипломат Вижинер предложил оригинальный *шифр сложной замены,* получивший впоследствии название *системы Виженера*

Шифруемый текст	**ЗАЩИТАИНФОРМАЦИИ**
Ключ	**МОРЕМОРЕМОРЕМОРЕ**
Зашифрованный текст	**УОИОЭОШТЯЫЯСМГШО**

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

↓

М МНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛ
О ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМН
Р СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОП
Е ЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД

АЛГОРИТМ ШИФРОВАНИЯ:

1. Под каждой буквой открытого текста записываются буквы ключи, повторяющие ключ требуемое число раз (чтобы покрыть все буквы текста).

2. Шифруемый текст по подматрице МОРЕ заменяется буквами, расположенными на пересечении линий, соединяющих буквы первой строки и буквы ключа, находящейся под ней.

Алгоритм расшифрования

Ключ	**МОРЕ**	**МОРЕ**	**МОРЕ**	**МОРЕ**
Шифр	**УОИО**	**ЭОШТ**	**ЯЫЯС**	**МГШО**
Расшифрованный текст	**ЗАЩИ**	**ТАИН**	**ФОРМ**	**АЦИИ**

В строках М,О,Р,Е отыскиваются буквы шифрованного текста и заменяются буквами первой строки. Это *шифр сложной замены* или *многоалфавитный шифр замены*.

В тоже время Ф. Бекон впервые предложил представление букв алфавита *пятизначным двоичным кодом*: А - 00001, Б - 00010… Такой способ шифрования обладал слабой стойкостью, однако эта идея, через три столетия легла в основу электрической и электронной связи на основе кодов Морзе, Бодо, телеграфных кодов.

Известный математик К. Гаусс в 18 - 19 веках создал *шифр с многократной подстановкой* или *равночастный шифр* в основе которого лежит прием *рандомизации* (*random* - случайный) открытого текста, который преобразовался в шифротекст, содержащий символы большего алфавита. При этом часто встречающиеся буквы открытого текста заменяются случайными символами из большего алфавита. В результате все символы шифротекста равночастны.

В нашем столетии американский ученый Вернам предложил систему *побитового шифрования* открытого текста, представленного телеграфным двоичным кодом, когда каждый бит преобразуется с использованием бита ключа по алгоритму

0+0=1 0+1=1 1+0=1 1+1=0

Вернам предполагал использовать ключ только один раз. Длина ключа равна длине шифруемого открытого текста. Впоследствии К. Шеннон доказал что такой шифр не раскрываем. Однако сложности формирования, хранения и передачи ключа, длина которого равна длине открытого текста делают такой метод очень непрактичным и дорогостоящим

В целом при построении шифров могут использоваться ключи разных типов: долговременные, суточные и сеансовые (для передачи каждого конкретного сообщения).

В настоящие время вместо понятия шифра используется понятие криптографической системы с секретным ключом, которая задается следующими пятью компонентами:

$\tilde{M}$ - пространство открытых текстов

$\tilde{C}$ - пространство шифрованных текстов

$\tilde{K}$ - пространство ключей

$E_k \quad (k \in K)$ - мн-во преобразований зашифрования: $E_k : \tilde{M} \to \tilde{C} \, (k \in \tilde{K})$

$D_k \quad (k \in K)$ - мн-во преобразований расшифрования: $D_k : \tilde{C} \to \tilde{M} \, (k \in \tilde{K})$

Современные криптосистемы с секретным ключом подразделяются на *блочные* и *потоковые*.

Блочная криптосистема разбивает открытый текст M на блоки $M_1, M_2 \ldots$ и зашифровывает каждый блок с помощью одного и того - же E_k преобразования выбранного в соответствии с ключом K.

$$E_k(M) = E_k(M_1), E_k(M_2)\ldots$$

Для повышения стойкости блочных криптосистем используется *режим сцепления блоков шифра*. Если обозначить через E_k преобразование зашифрования в режиме сцепления блоков $C_1, C_2, \ldots$ шифрованного текста из блоков $M_1, M_2 \ldots$ открытого текста, то процесс этого зашифрования в режиме сцепления блоков шифра описывается соотношением

$$C_i = E_k[C_{i-1} \oplus M_i] \quad i = 1,2,\ldots$$

Поточная криптосистема разбивает открытый текст M на буквы или биты *m*1,*m*2,… и зашифровывает каждый m_i знак с помощью обратимого преобразования E_k выбранного в соответствии со k_i знаком ключевого потока $k_1, k_2, \ldots$.

Такие системы иногда называют *системами гаммирования*, а последовательность $k_1, k_2, \ldots$ называют *гаммой*.

- В свою очередь поточные криптосистемы делятся на *синхронные* и *самосинхронизирующиеся*.
- *Синхронные поточные криптосистемы* характеризуются тем, что, в отличие от самосинхронизирующихся, в них ключевой поток $k_1, k_2, \ldots$ получается независимо от открытого и шифрованного текстов.
- *Самосинхронизирующиеся поточные криптосистемы* характеризуется тем, что каждый знак ключевого потока (гаммы) в любой момент времени определяется фиксированным числом предшествующих знаков шифротекста.

Алгоритм, который вырабатывает ключевой поток (гамму) может быть либо *детерминированным*, либо *случайным*. Этот алгоритм называют *генератором ключевого потока*. Если такой генератор детерминированный, то он должен зависеть от секретного ключа. Если он случайный то сам является секретным ключом, но очень большой длины, что непрактично.

В последнее время широкое распространение получили криптосистемы *с открытым ключом*, построенные на основе предложенных Диффи и Хеллманом принципов открытого шифрования и открытого распределения ключей (1976 г.). Также криптосистемы называют также *двухключевыми криптосистемами* или *асимметричными криптосистемами*, в то время как обычные криптосистемы с секретным ключом называют *симметричными криптосистемами*.