# Основные понятия криптологии, криптографии и криптоанализа

Защита данных в ЭВМ и информационно-вычислительных сетях с помощью шифрования считается одним из наиболее надежных способов решения проблемы безопасности.

Изучением вопросов шифрования данных занимается наука - ***криптология***, включающая криптографию и криптоанализ.

***Криптография*** изучает методы и алгоритмы шифрования данных (правила построения и использования шифров), направленные на то, чтобы сделать эти данные бесполезными для противника.

Методы криптографии также используются для подтверждения подлинности источника данных и контроля целостности данных.

Заметим, что криптография всегда являлась обязательным элементом безопасных информационных систем. Однако особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нельзя обеспечить физическую защиту каналов связи.

***Криптоанализ*** - это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

Прежде всего поясним, чем отличается шифрование от кодирования. С теоретической точки зрения не существует четкого различия между кодами и шифрами. Однако в современной практике различие между ними, как правило, является достаточно четким. ***Коды*** оперируют лингвистическими элементами, разделяя закрываемый текст на такие смысловые элементы, как слова и слоги. В ***шифре*** всегда различают два элемента: алгоритм и ключ. Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно длинного текста.

Определим ряд основных терминов, используемых в криптографии.

В соответствии с ГОСТ 28147-89 [1.1] под ***шифром*** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

***Ключ*** - это конкретное (секретное или открытое) состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является ***криптостойкость***, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется *интервалом времени, необходимым для раскрытия шифра*.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

* достаточная криптостойкость (надежность закрытия данных);
* простота процедур шифрования и расшифрования;
* незначительная избыточность информации за счет шифрования;
* нечувствительность к небольшим ошибкам шифрования и др.

Криптографическое закрытие информации имеет многовековую историю развития и применения.

Можно выделить следующие три периода развития криптографии. **Первый период** - эра донаучной криптологии, являющейся ремеслом узкого круга искусных умельцев. Началом **второго периода** можно считать 1949 г., когда появилась работа К.Шеннона “Теория связи в секретных системах”, в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина. И, наконец, начало **третьему периоду** было положено появлением в 1976 г. работы У Диффи и М.Хеллмана “Новые направления в криптографии”, где показано, что секретная связь возможна без предварительной передачи секретного ключа. Так началось и продолжается до настоящего времени бурное развитие наряду с обычной классической криптографией и криптографии с открытым ключом.

Все традиционные криптографические системы можно подразделить на:

1. Шифры перестановки:
	1. Шифр перестановки “скитала”.
	2. Шифрующие таблицы.
	3. Применение магических квадратов.
2. Шифры простой замены:
	1. Полибианский квадрат.
	2. Система шифрования Цезаря.
	3. Аффинная система подстановок Цезаря.
	4. Система Цезаря с ключевым словом.
	5. Шифрующие таблицы Трисемуса.
	6. Биграммный шифр Плейфейра.
	7. Криптосистема Хилла.
	8. Система омофонов.
3. Шифры сложной замены:
	1. Шифр Гронсфельда.
	2. Система шифрования Вижинера.
	3. Шифр “двойной квадрат” Уитстона.
	4. Одноразовая система шифрования.
	5. Шифрование методом Вернама.
	6. Роторные машины.
4. Шифрование методом гаммирования.
5. Шифрование, основанное на аналитических преобразованиях шифруемых данных.

**Шифрование перестановкой** заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

**Шифрование заменой (подстановкой)** заключается в том, что символы шифруемого текста заменяются символами того же самого (простая замена), также одно или нескольких других алфавитов (сложная замена) в соответствии с заранее обусловленной схемой замены.

**Шифрование гаммированием** заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой ***гаммой шифра***. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Данный способ является одним из основных для шифрования информации в автоматизированных системах.

**Шифрование аналитическим преобразованием** заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифра, а символами умножаемого вектора последовательно служат символы шифруемого текста. Другим примером может служить использование так называемых однонаправленных функций для построения криптосистем с открытым ключом.

Классические криптографические методы и алгоритмы разделяют на два основных типа:

* ***симметричные (с секретным ключом)*,**
* ***асимметричные (с открытым ключом)***.

В ***симметричных методах*** для шифрования и расшифровывания используется один и тот же секретный ключ.

Рассмотрим некоторые из них.

# Симметричные криптосистемы

**Шифры перестановки**

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Н | О | Н | С | Б | Н | Я |
| Е | Е | О | Я | О | Е | Т |
| Я | С | В | Е | Л | П | Н |
| С | Т | И | Щ | Е | О | Ы |
| Н | А | Т | Е | Е | Н | М |

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Л | У | Н | А | Т | И | К |   |   | А | И | К | Л | Н | Т | У |
| 4 | 7 | 5 | 1 | 6 | 2 | 3 |   |   | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Н | О | Н | С | Б | Н | Я |   |   | С | Н | Я | Н | Н | Б | О |
| Е | Е | О | Я | О | Е | Т |   |   | Я | Е | Т | Е | О | О | Е |
| Я | С | В | Е | Л | П | Н |   |   | Е | П | Н | Я | В | Л | С |
| С | Т | И | Щ | Е | О | Ы |   |   | Щ | О | Ы | С | И | Е | Т |
| Н | А | Т | Е | Е | Н | М |   |   | Е | Н | М | Н | Т | Е | А |

До перестановки                                                После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю\_шестого” можно зашифровать следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 4 | 1 | 3 |   |   | 1 | 2 | 3 | 4 |   |   | 1 | 2 | 3 | 4 |
| 4 | П | Р | И | Е |   | 4 | И | П | Е | Р |   | 1 | А | З | Ю | Ж |
| 1 | З | Ж | А | Ю |   | 1 | А | 3 | Ю | Ж |   | 2 | Е | \_ | С | Ш |
| 2 | \_ | Ш | Е | С |   | 2 | Е. | \_ | С | Ш |   | 3 | Г | Т | О | О |
| 3 | Т | О | Г | О |   | 3 | Г | Т | О | О |   | 4 | И | П | Е | Р |

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ\_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5\*5 их 14400.

**Шифры простой замены**

**Система шифрования Цезаря** - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5\*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

**Шифры сложной замены**

**Шифр Гронсфельда** состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

|  |  |
| --- | --- |
|   | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| А | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| Б | \_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ |
| В | Я\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ |
| Г | ЮЯ\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ |
| . | ………… |
| Я | ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_АБ |
| \_ | БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_А |

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

|  |  |
| --- | --- |
| Сообщение | ПРИЕЗЖАЮ\_ШЕСТОГО |
| Ключ | АГАВААГАВААГАВАА |
| Шифровка | ПНИГЗЖЮЮЮАЕОТМГО |

Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США **DES (DataEncryptionStandard)**. Коммерческий вариант алгоритма DES использует ключ длиной 56 бит, что требует от злоумышленника перебора **72·1012** возможных ключевых комбинаций. Более криптостойкая (но втрое менее быстродействующая) версия алгоритма DES - **TripleDES** (тройной DES) позволяет задать ключ длиной 112 бит.

Другим популярным алгоритмом шифрования является **IDEA (InternationalDataEncryptionAlgorithm)**, отличающийся применением ключа длиной 128 бит. Он считается более стойким, чем DES.

Отечественный стандарт шифрования данных - **ГОСТ 28147-89** “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”определяет алгоритм симметричного шифрования с ключом длиной до 256 бит.

Общая технология использования симметричного метода шифрования представлена на рис.2.1.

Текст
***Е-1(Е(Т))***

Зашифрованный текст
***Е(Т)***

Текст
***Т***

**Дешифратор**

**Шифратор**

*Секретный ключ* ***Е***

*Генератор ключей* ***{Е}***

**Рис. 2.1. Использование симметричного метода шифрования с секретным ключом**

К достоинствам симметричных методов относят высокое быстродействие и простоту.

Основным недостатком указанных методов является то, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. По существу, в открытых сетях должен быть предусмотрен физически защищенный канал передачи ключей.

Названный недостаток послужил причиной разработки методов шифрования с открытым ключом -асимметричных методов.