Министерство образования и науки РФ
ФГБОУ ВПО «Новосибирский государственный педагогический университет»
Факультет технологии и предпринимательства

Криптография, криптология, криптоанализ

Выполнил: *студент 31 группы*
Лохман А.Э.
Проверил: *канд.пед.наук*
Лейбов А.М

2015

Содержание:

1.История развития криптологии.

2.Криптография и криптоанализ;

- Разделы криптографии.
- Классы методов криптографии.

3. Криптографические стандарты.

- Основные области применения DES-алгоритма.

4. Характеристики криптографических средств защиты.

Можно выделить следующие три периода развития криптологии:

Первый период — эра донаучной криптологии, являвшейся ремеслом-уделом узкого круга искусных умельцев.

Второй период -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.

Третий период -1976 г. , это работы У. Диффи, 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.

Криптология разделяется на два направления — **криптографию** и **криптоанализ.** Цели этих направлений прямо противоположны:

- **Криптография** занимается поиском и исследованием математических методов преобразования информации;

- сфера интересов **Криптоанализа** — исследование возможности расшифровывания информации без знания ключей;

Современная криптография включает в себя такие разделы как:

- **криптосистемы с открытым ключом;**
- **симметричные криптосистемы;**
- **системы электронной подписи;**
- **управление ключами.**

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Криптосистемы разделяются на симметричные и асимметричные (с открытым ключом):

Использование симметричного метода шифрования

Симметричные криптосистемы

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. Существуют весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и стандарт на подобные методы — ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю;

Использование асимметричного метода шифрования

Асимметричные криптосистемы

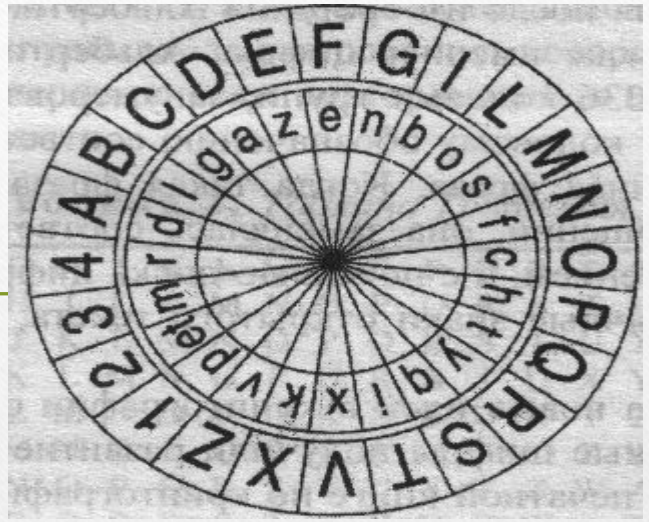
Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:

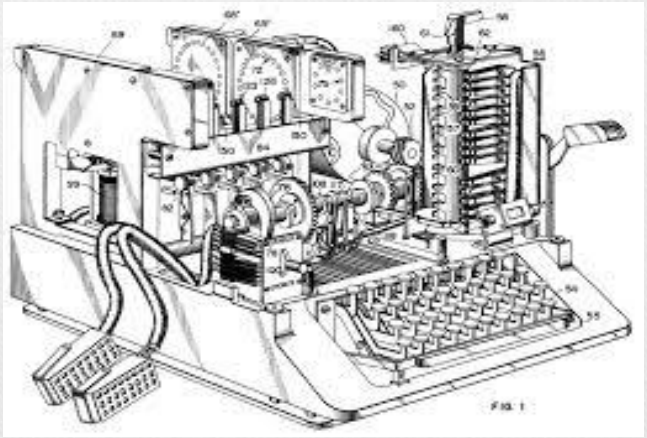
- открытый ключ K используется для шифрования информации, вычисляется из секретного ключа k;
- секретный ключ k используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи.

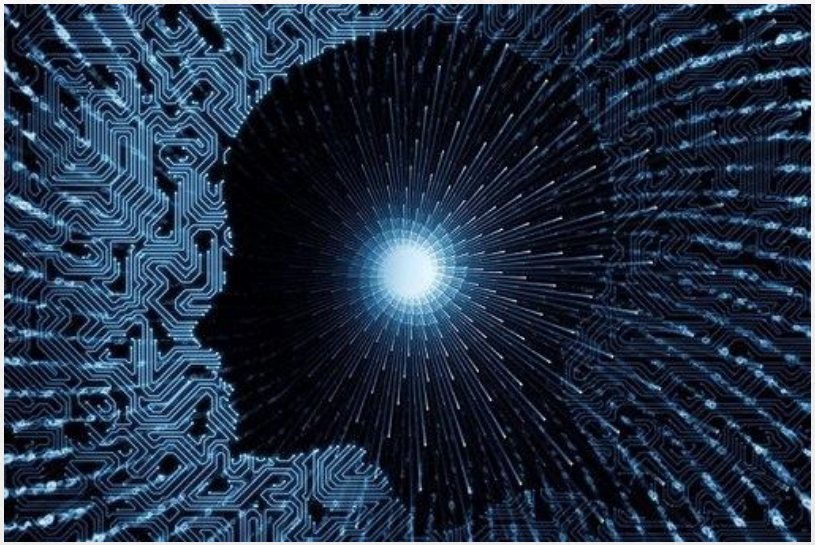
Асимметричные системы называют также двухключевыми криптографическими системами, или криптосистемами с открытым ключом.

- **Термины распределение ключей и управление ключами** относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

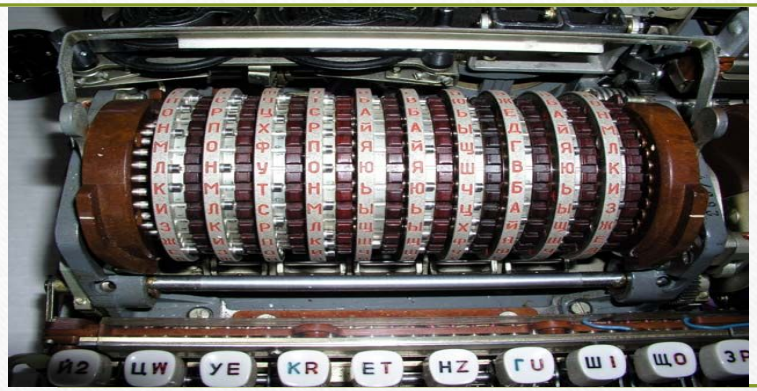


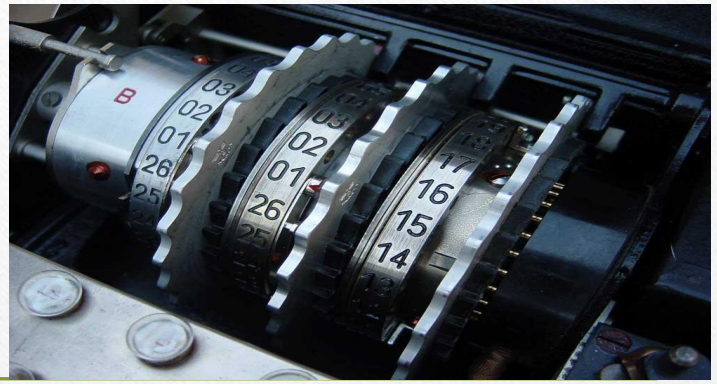


Классы методов криптографии:



1. *Шифрование*
2. *Кодирование*
3. *Другие виды*





Под шифрованием понимается такой вид криптографиского закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифование. Каждый из этих способов может иметь несколько разновидностей.

Под кодированием понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодировании кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений). При символьном кодировании кодируется каждый символ защищаемого сообщения. Символьное кодирование по существу совпадает с шифрованием заменой.

Таблица 8.1. **Таблица простой замены**

Исходные символы шифруемого текста	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
Заменяющие символы	S	P	X	L	R	Z	I	M	A	Y	E	D	W	T	B	G	V	N	J	O	C	F	H	Q	U	K

Шифрование заменой (подстановка). В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из одного (одно- или моноалфавитная подстановка) или нескольких (много- или полиалфавитная подстановка) алфавитов.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита. Таблица замены может иметь следующий вид (табл. 8.1).

Шифрование методом перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв.

Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП.

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить не значащей буквой (например, О) до числа, кратн го пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное из менение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявятся серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки не¬значащими буквами).

Криптографические стандарты

Широко известны алгоритмы блочного шифрования, принятые в качестве государственных стандартов шифрования данных в США и России.

Data Encryption Standart. В 1973 г. Национальное бюро стандартов США начало разработку программы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс среди фирм-разработчиков США, который выиграла фирма IBM, представившая в 1974 г. алгоритм шифрования, известный под названием DES (Data Encryption Standart).

Основные области применения DES-алгоритма:

- хранение данных в ЭВМ (шифрование файлов, паролей);
- аутентификация сообщений (имея сообщение и контрольную группу, несложно убедиться в подлинности сообщения);
- электронная система платежей (при операциях с широкой клиентурой и между банками);
- электронный обмен коммерческой информацией (обмен данными между покупателем, продавцом и банкиром защищен от изменений и перехвата).

Характеристики криптографических средств защиты

Важнейшей характеристикой надежности криптографического закрытия информации является его стойкость. Под этим понимается тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, по стойкости шифра можно определить допустимый объем информации, зашифровываемый при использовании одного ключа.

При выборе криптографического алгоритма для использования в конкретной разработке одним из определяющих факторов является его стойкость, т. е. устойчивость к попыткам противоположной стороны его раскрыть. Вопрос о стойкости шифра при ближайшем рассмотрении сводится к двум взаимосвязанным вопросам:

- можно ли вообще раскрыть данный шифр;
- если да, то насколько это трудно сделать практически;

Все современные криптосистемы построены по принципу Кирхгоффа, т. е. секретность зашифрованных сообщений опре¬деляется секретностью ключа. Это значит, что даже если сам ал¬горитм шифрования известен криптоаналитику, тот тем не ме¬нее не в состоянии расшифровать сообщение, если не располагает соответствующим ключом. Все классические блочные шифры, в том числе DES, соответствует этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полным перебором по всему ключевому пространству, т. е. по всем возможны значениям ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Список литературы:

- http://www.i2r.ru/static/567/out_15736.shtml
- А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин «Основы криптографии».
- Владимир Жельников «Криптография от папируса до компьютера».