**Тема Симметричные криптосистемы**

**Цель:** Изучить симметричные блочные криптоалгоритмы

**Вопросы практического занятия:**

*Основные понятия и термины современной криптографии. Классификация современных криптосистем. Классическая сеть Фейстеля. Потоковые шифры. Блочные шифры. Методы криптоанализа. Способы реализации стеганографических системе их достоинства и недостатки.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы.

**Контрольные вопросы:**

1 Как называется раздел науки, объединяющий криптографию и криптоанализ?

Раздел науки, объединяющий криптографию и криптоанализ, принято называть **криптологией**.

2 Какие задачи решает криптография?

*Криптография* в переводе с греческого означает "тайнопись". В настоящее время *криптография* занимается поиском и исследованием математических методов преобразования информации. Параллельно развивается и совершенствуется *криптоанализ* – наука о преодолении криптографической защиты информации.

*Криптография* решает следующие задачи: *шифрование данных* с целью защиты от несанкционированного доступа; проверка подлинности сообщений; проверка целостности передаваемых данных; обеспечение невозможности отказа.

3 Что представляет собой криптографический алгоритм?

Набор правил, который используется для шифрования информации, чтобы ее могли прочитать только авторизованные стороны. Алгоритм позволяет генерировать зашифрованный текст, который невозможно прочитать без расшифровки.

4 Какие требования предъявляются для современных криптографических систем защиты?

Для современных криптографических систем защиты информации сформулированы следующие требования:

* зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
* знание алгоритма шифрования не должно влиять на надежность защиты;
* любой ключ из множества возможных должен обеспечивать надежную защиту информации;

алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

5 В чем суть криптографического метода замены и перестановки?

Суть этого метода заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного) текста. Перестановки в классической криптографии обычно получаются в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры. Методы шифрования заменой (подстановкой) основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

6 Объясните метод шифрования одноконтурной обыкновенной подстановки?

При **полиалфавитной одноконтурной обыкновенной подстановке** для замены символов исходного текста используются несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй – символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется. Под каждой буквой шифруемого теста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;

Каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;

Полученный текст может разбиваться на группы по несколько знаков.

7 Объясните метод шифрования простой перестановки?

Простая [перестановка](http://fkn.ktu10.com/?q=node/7696) **без ключа** *(с ключом [рассматривается здесь](http://fkn.ktu10.com/?q=node/4399))*— один из самых простых методов шифрования.

Делают так:

1. **Сообщение записывается в таблицу по столбцам.**
2. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю **нужно договориться об общем ключе в виде размера таблицы**.

например, **зашифруем фразу "ВРАГ БУДЕТ РАЗБИТ",**  
разместим текст в "таблице" - по три столбца (и не будем вообще использовать пробелы)-  
запишем текст столбцами:

[?](http://fkn.ktu10.com/?q=node/4395)

|  |  |
| --- | --- |
| 1  2  3  4  5 | В   Г   Д   Р   Б    Р   Б   Е   А   И    А   У   Т   З   Т |

при считывании по строкам получим шифровку (разделяю на группы по 4-ре только для визуального удобства - можно вообще не разделять):

[?](http://fkn.ktu10.com/?q=node/4395)

|  |  |
| --- | --- |
| 1 | ВГДР БРБЕ АИАУ ТЗТ |

То есть мы получаем [перестановку](http://fkn.ktu10.com/?q=node/7696) (как результат действия [подстановки](http://fkn.ktu10.com/?q=node/6508)) исходного множества букв (потому так и называется) таким образом:

[?](http://fkn.ktu10.com/?q=node/4395)

|  |  |
| --- | --- |
| 1  2 | ВРАГ  БУДЕ  ТРАЗ  БИТ  ВГДР  БРБЕ  АИАУ  ТЗТ |

Фактически - чтобы сразу расшифровать такую строку:

[?](http://fkn.ktu10.com/?q=node/4395)

|  |  |
| --- | --- |
| 1 | ВРАГ  БУДЕ  ТРАЗ  БИТ |

достаточно знать **число столбцов в исходной таблице**,то есть **число столбцов и будет являться *ключом*** данной криптосистемы.

8 Объясните шифрование методом гаммирования?

**Под***гаммированием***понимают процесс наложения по определенному закону гаммы шифра на открытые данные.***Гамма шифра -***это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных.**

**Процесс зашифрования заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом, например с использованием операции сложения по модулю***2.*

**Следует отметить, что перед зашифрованием открытые данные разбивают на блоки 7^ одинаковой длины, обычно по***64***бита. Гамма шифра вырабатывается в виде последовательности блоков***vj)***аналогичной длины.**

**Уравнение зашифрования можно записать в виде**



**где***Т$ - i-й***блок шифртекста; -***i-й***блок гаммы шифра;***-*

*i-й***блок открытого текста;***М-***количество блоков открытого текста.**

**Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на зашифрованные данные. Уравнение расшифрования имеет вид**



**Получаемый этим методом шифртекст достаточно труден для раскрытия, поскольку теперь ключ является переменным. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого текста и злоумышленнику неизвестна никакая часть исходного текста, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.**

9 Какова стойкость комбинированные методы шифрования?

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких [различных способов](https://win-keys.ru/windows-8/kak-zarabotat-dengi-rebenku-8-let-devochke-kak-shkolniku-bystro-i-legko.html) шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Как показали исследования, стойкость комбинированного шифрования не ниже произведения стойкостей используемых способов.

10 Что является важнейшим показателем надежности криптографического закрытия?

Важнейшим показателем надежности криптографического закрытия информации является его *криптостойкость*— тот минимальный объем зашифрованного текста, который можно вскрыть статистическим анализом. Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

11 Как определяется трудоемкость метода шифрования?

*Трудоемкость метода шифрования* определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

12 Что такое маршрутная перестановка?

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют **маршрутной перестановкой**.

Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

13 Что называется «поворотной решеткой»?

Ключом шифра, называемого "поворотная решетка", является трафарет, изготовленный из квадратного листа клетчатой бумаги размера n×n (n - четно). Некоторые из клеток вырезаются. Одна из сторон трафарета помечена. При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причем каждая клетка оказывается под вырезом ровно один раз. Буквы сообщения, имеющего длину n2, последовательно вписываются в вырезы трафарета, сначала наложенного на чистый лист бумаги помеченной стороной вверх. После заполнения всех вырезов трафарета буквами сообщения трафарет располагается в следующем положении и т. д. После снятия трафарета на листе бумаги оказывается зашифрованное сообщение.

14 Оцените количество ключей шифра вертикальной перестановки. Во сколько раз это

15 В чем отличие шифров простой и сложной замены?

В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены.

16 Какие шифры сложной замены вам известны?

Система шифрования Альберти, Шифр Тритемия , Шифр Гронсфельда, Система шифрования Вижинера, Шифр «двойной квадрат» Уитстона, Шифрование методом Вернама