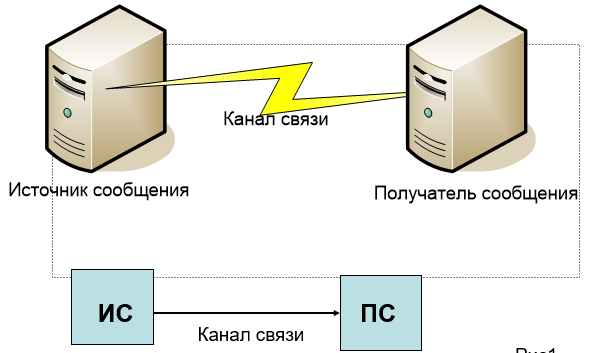
**Вопросы**

**по дисциплине «Информационная безопасность», 2023-24 уч. год, летний семестр**

1. **Сущность проблемы информационной безопасности систем.** **Характеристики и параметры ИС и ИВС.**

Информационная система – совокупность аппаратно-программных средств, с помощью которых выполняются операции над данными: сбор, передача, обработка, хранение и визуализация информации.



Безопасность ИС/ИВС (информационно-вычислительная система) – способность противодействовать попыткам несанкционированного доступа или нанесения ущерба владельцам и пользователям системы при умышленных и неумышленных воздействиях на нее.

Информационная безопасность – все аспекты, связанные с определением,

достижением и поддержанием конфиденциальности, целостности, доступности

информации или средств ее обработки:

1) конфиденциальность – доступ к

ней осуществляют только субъекты, имеющие на нее право;

2) целостность – избежание несанкционированной модификации

информации;

3) доступность – избежание временного или постоянного сокрытия

информации от пользователей, получивших права доступа.

Основные хар-ки:

1. Алфавит – конечная совокупность символов, с помощью кот. можно представить любое сообщение в ИС: A{ai}
2. Мощность = кол-во символов алфавита N(A)
3. Энтропия – информационная хар-ка алфавита; кол-во информации (бит) в среднем на 1 символ алфавита.
4. Кол-во инф. I в произвольном сообщении Xk, k – число символов в сообщении: I(Xk) = H(A)\*k
5. **Характеристика угроз безопасности современным ИС и ИВС.**

Одним из важнейших дестабилизирующих работу ИВС факторов считают

электромагнитные и ионизирующие излучения. Ионизирующие излучения также могут

иметь естественную (солнечная радиация) и искусственную (изотопы урана и тория

излучают даже пластмассы) природу.

Основные факторы (угрозы):

1) действия злоумышленника;

2) наблюдение за источниками информации;

3) подслушивание конфиденциальных разговоров и акустических сигналов

работающих механизмов;

4) перехват электрических, магнитных и электромагнитных полей, электрических

сигналов и радиоактивных излучений;

5) несанкционированное распространение материальных носителей за пределами

организации;

6) разглашение информации компетентными людьми;

7) утеря носителей информации;

8) несанкционированное распространение информации через поля и электрические

сигналы, случайно возникшие в аппаратуре;

9) воздействие стихийных сил (наводнения, пожары и т. п.);

10) сбои и отказы в аппаратуре сбора, обработки и передачи информации;

11) отказы системы электроснабжения;

12) воздействие мощных электромагнитных и электрических помех (промышленных и природных).

Несанкционированный доступ с помощью деструктивных программных средств

осуществляется, как правило, через компьютерные сети.

Классификацию вредоносного ПО можно представить следующим образом:

1) вирусы

2) черви

3) кейлоггеры;

4) трояны

5) боты

6) снифферы

7) руткиты

Выделяют несколько основных угроз безопасности, возникающих при использовании бесплатных точек доступа Wi-Fi:

1) сети, организованные хакерами, могут выдавать

себя за вполне легальные бесплатные точки доступа;

2) атаки с помощью вредоносного ПО компьютера, подключенного к этой точке доступа; 3) сниффинг;

4) хищение персональной информации методом «человек посередине»

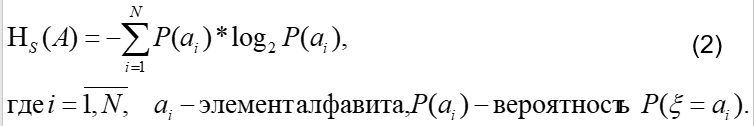
5) Фишинг.

1. **Политика безопасности современных ИС и ИВС**

Методы и средства защиты разделяются на 3 класса:

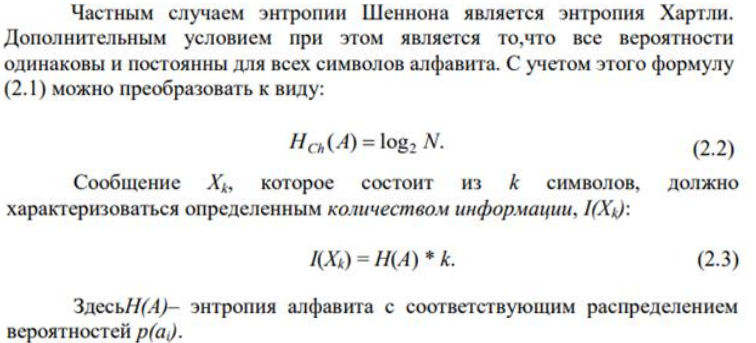
1. Законодательная и нормативно-правовая база: акты национального законодательства, конституция, указы президента и другие правовые акты
2. Организационно-технические и режимные меры и методы: организация охраны, режима, работа с кадрами и т.д + технические средства безопасности: дверные замки, ключ-карты, пропуски и т.д
3. Аппаратные, программные и программно-аппаратные средства защиты: авторизация, мониторинг, антивирусы, шифрование данных, ЭЦП, пароль, биометрия (сетчатка, голос и тд)
4. **Энтропия источника сообщения. Энтропия Шеннона.**

Энтропия – информационная хар-ка алфавита; кол-во информации (бит) в среднем на 1 символ алфавита.

Рассчитывается следующим образом:****

1. **Энтропия источника сообщения. Энтропия Хартли.**

p(ai) = const

**0**

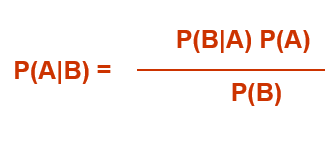
1. **Двоичный симметричный канал передачи информации.**

Для изучения механизма воздействия помех на процесс передачи данных и

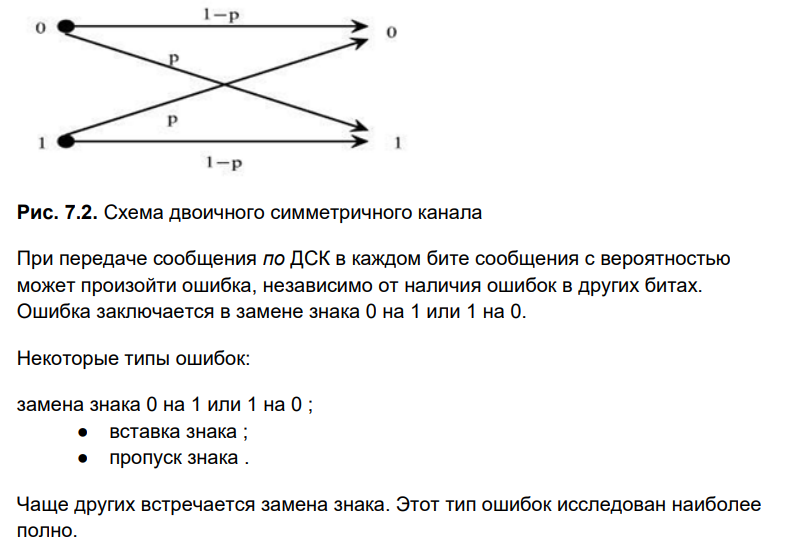
способов защиты от них необходима некоторая модель. Процесс

возникновения ошибок описывает модель под названием двоичный

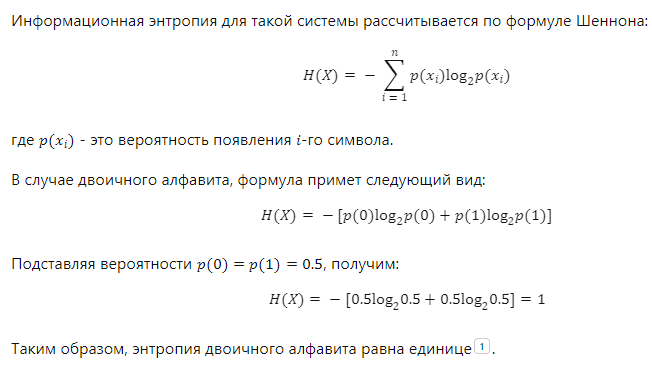
симметричный канал (ДСК), схема которой показана на рис.7.2.

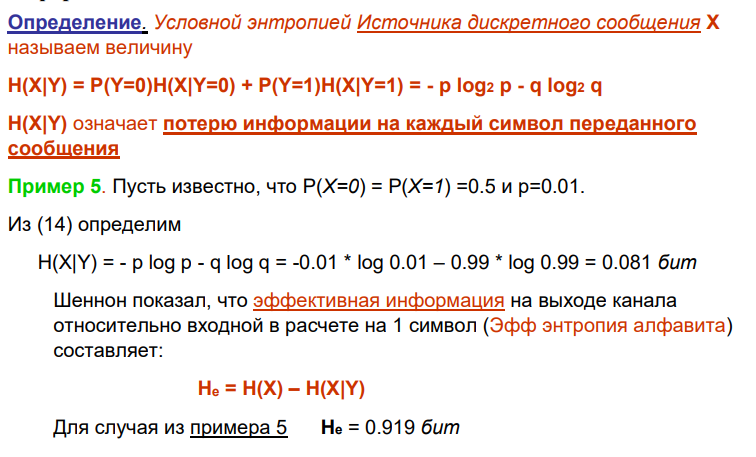


Математическая основа – теорема Байеса:



1. **Энтропия двоичного алфавита.**

****

1. **Условная энтропия. Энтропийная оценка потерь при передаче информации.**
2. **Базовые понятия криптографии. Основы теории больших чисел. Проблема дискретного логарифма.**

Если известны три некоторых числа (а, х, n), то достаточно легко можно

вычислить число y: y = a^xmod n. (4.10)

Обратная задача: найти х, если известны а, у, n. Эта задача решается

гораздо труднее. Ее называют задачей (проблемой) дискретного

логарифмирования, по аналогии с вещественными числами, для которых х

= loga y.

### Основные Понятия Криптографии

Криптография — это наука о методах защиты информации путем преобразования данных, чтобы они стали недоступны для несанкционированного доступа. Вот основные понятия криптографии:

#### 1. Шифрование и Расшифрование

- Шифрование: Процесс преобразования открытого текста в зашифрованный текст с использованием криптографического алгоритма и ключа.

- Расшифрование: Обратный процесс, преобразующий зашифрованный текст обратно в открытый текст с использованием ключа.

#### 2. Типы Криптографии

- Симметричная криптография: Использует один и тот же ключ для шифрования и расшифрования. Пример: AES (Advanced Encryption Standard).

- Асимметричная криптография: Использует пару ключей — открытый ключ для шифрования и закрытый ключ для расшифрования. Пример: RSA (Rivest-Shamir-Adleman).

#### 3. Хэш-функции

- Функции, которые преобразуют произвольный входной текст в фиксированный выходной хэш. Примеры: SHA-256, MD5.

#### 4. Цифровые подписи

- Используются для проверки подлинности и целостности сообщения. Создаются с использованием закрытого ключа и проверяются с использованием соответствующего открытого ключа.

#### 5. Цифровые сертификаты

- Электронные документы, подтверждающие подлинность открытого ключа, выданные удостоверяющим центром.

### Основы Теории Больших Чисел

Теория больших чисел играет ключевую роль в криптографии, особенно в контексте асимметричной криптографии. Вот несколько основных понятий:

#### 1. Простые числа

- Числа, которые делятся только на 1 и на себя. Примеры: 2, 3, 5, 7, 11, и т.д.

- Теорема о простых числах: Любое целое число больше 1 является либо простым числом, либо может быть разложено на произведение простых чисел.

#### 2. Сложность факторизации

- Процесс нахождения простых множителей числа. Для больших чисел это вычислительно сложная задача, что делает её основой безопасности алгоритмов, таких как RSA.

#### 3. Арифметика по модулю

- Операции с остатками при делении. Пример: \(a \mod n\) — остаток от деления \(a\) на \(n\).

- Пример: \(17 \mod 5 = 2\), так как \(17 = 3 \times 5 + 2\).

#### 4. Функция Эйлера

- Обозначается как \(\varphi(n)\). Количество чисел, меньших \(n\), которые взаимно просты с \(n\).

- Пример: \(\varphi(9) = 6\), так как числа 1, 2, 4, 5, 7, 8 взаимно просты с 9.

#### 5. Логарифмы по модулю

- Обратная операция к возведению в степень по модулю, известная как проблема дискретного логарифма. Трудность её решения используется в таких алгоритмах, как Diffie-Hellman и DSA (Digital Signature Algorithm).

#### 6. Алгоритм Евклида

- Используется для нахождения наибольшего общего делителя (НОД) двух чисел. Может быть расширен для нахождения коэффициентов Безу.

### Применение Теории Больших Чисел в Криптографии

- RSA: Основывается на трудности факторизации произведения двух больших простых чисел.

- Diffie-Hellman: Основан на сложности вычисления дискретного логарифма.

- Эллиптические кривые: Используют свойства эллиптических кривых над конечными полями, предоставляя высокий уровень безопасности при меньших размерах ключей.

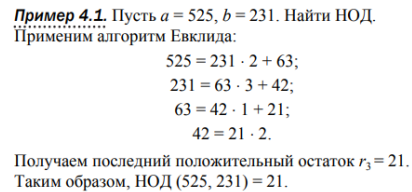
Эти основы теории больших чисел и криптографии позволяют создавать надёжные и безопасные системы для защиты информации в цифровом мире.

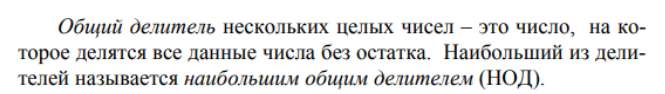
1. **Основная теорема арифметики. Алгоритм Евклида нахождения НОД**

Основная теорема арифметики: всякое натуральное число N (кроме 1) можно представить как произведение простых множителей.

while b != 0:

a, b = b, a%b

****

****

1. **Основы модулярной арифметики. Вычеты.**

В модулярной арифметике мы интересуемся остатком от деления числа а на число n.

Если таким остатком является число b, то можно записать: a ≡ b mod n.

Такая формальная запись читается как «a сравнимо с b по модулю n». Множество всех

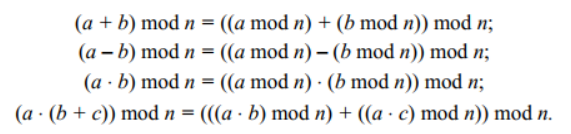
чисел, сравнимых с сравнимых с b по модулю n, называется классом вычетов по модулю n. Любое число класса называется вычетом по модулю n

При целочисленном (в том числе и нулевом) результате k деления числа а на число n

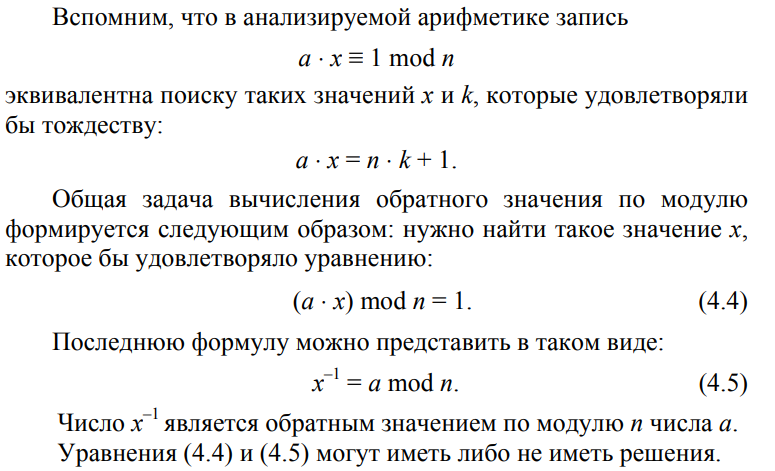
справедливо a = b + k ⋅ n.

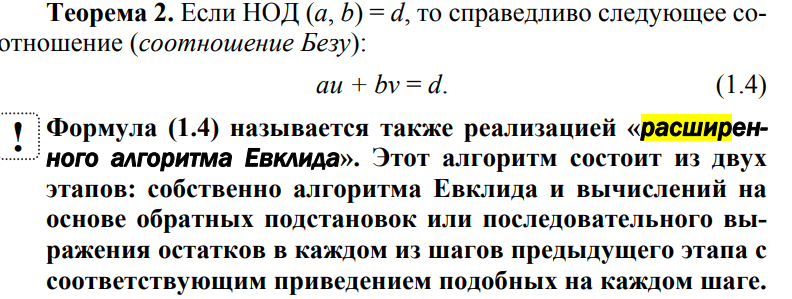
Модулярная арифметика также коммутативна, ассоциативна и дистрибутивна, как и

обычная арифметика.



1. **Обратные вычисления по модулю в криптографии. Расширенный алгоритм Евклида.**

****

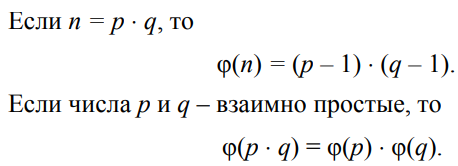
****

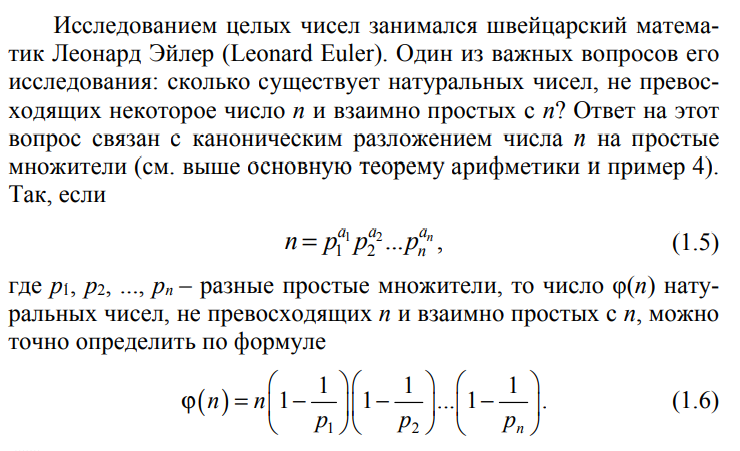
****

1. **Функция Эйлера в криптографии.**

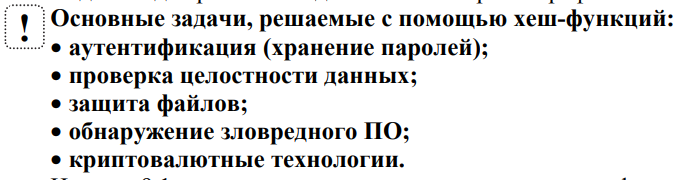
Количество натуральных чисел, меньших некоторого числа n и взаимно простых с ним, можно подсчитать на основе известной функции Эйлера. Если n – простое число, то







1. **Хеш-функция и ее свойства. Области использования хеш-функций.**

****Хеш-функция – математическая или иная функция h=H(M), которая принимает на входе строку символов переменной (произвольной) длины и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины, называемой значением хеш-функции.

Свойства:

1. *Детерминированность*: независимо от того, сколько раз вычисляется H(M), M – const, при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.
2. *Скорость вычисления хеша h*: если процесс вычисления h недостаточно быстрый, система просто не будет эффективной.
3. *Сложность обратного вычисления*: для известного H(М) невозможно (практически) определить М. Это важнейшее свойство хеш-функции для криптографических применений – свойство односторонности преобразования.
4. Даже *минимальные изменения в хешируемых данных* (М ≠ М') *должны* *изменять* *хеш*: Н(M) ≠ Н(М').
5. *Коллизионная устойчивость* (стойкость). Зная М, трудно найти такое М' (М ≠ М'), для которого H(М) = H(М').

Если последнее равенство выполняется, то говорят о коллизии 1-го рода.

Если случайным образом выбраны два сообщения (М и М'), для которых H(М) = H(М'), говорят о коллизии 2-го рода.

1. **Общая характеристика алгоритмов хеширования классов MD и SHA.**

Базовые алгоритмы обоих рассматриваемых семейств (MD и SHA) условно можно разделить на 5 стадий:

• расширение входного сообщения;

• разбивка расширенного сообщения на блоки;

• инициализация начальных констант;

• обработка сообщения поблочно (основная процедура алгоритма хеширования);

• вывод результата.

1. **Алгоритмы хеширования класса MD. Области использования.**
2. **Алгоритмы хеширования класса SHA. Области использования.**
3. **Общая классификация криптографических методов защиты информации.**

**1. По генерации ключа:**

а) симметричные (один ключ для зашифрования/расшифрования): DES, 3DES, Blowfish

б) ассиметричные (с открытым и закрытым ключами): RSA, Эль-Гамаль, ранцевый алгоритм

**2. По способу обработки информации:**

а) блочные (обрабатывают группы битов): Blowfish, IDEA, ГОСТ 28147-89

б) потоковые (поток символов по одному): Вернама

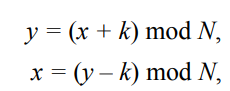
**3. По алгоритму шифрования:**

а) подстановочные (на места исходных букв подставляются другие буквы алфавита): Цезарь (и с ключевым словом тоже), аффинная подстановка, Виженера

б) перестановочные (буквы переставляются местами друг с другом и не заменяются другими буквами): вертикальный перестановочный шифр

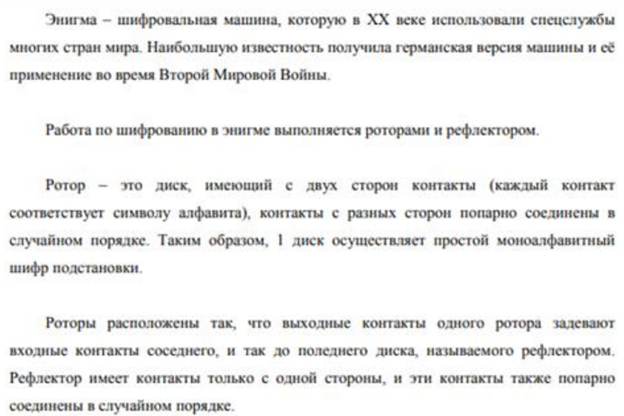
1. **Подстановочные шифры. Шифр Цезаря.**

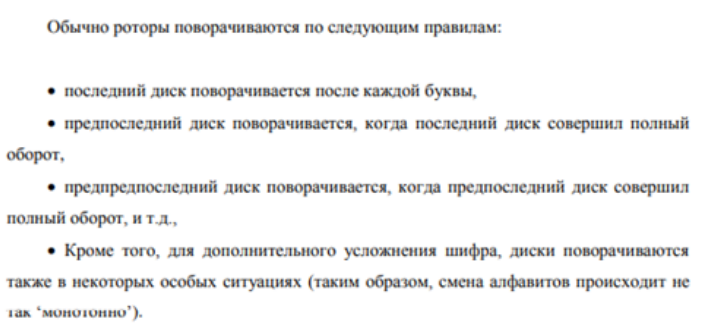
Если сопоставить каждому символу алфавита его порядковый номер (индекс), начиная с 0, то зашифрование и расшифрование можно выразить соотношениями:



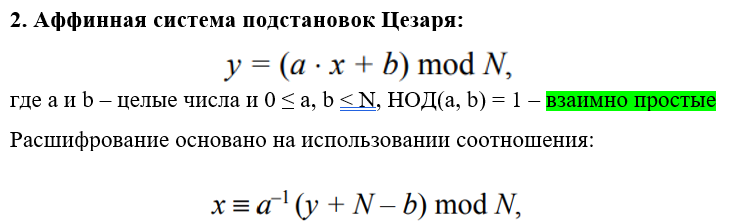
где х и y – соответственно порядковые номера (индексы) символов открытого и зашифрованного текстов; k – ключ; N – мощность алфавита (количество символов).

Пример: k=3, N=26, M=”abc”. C=”def”

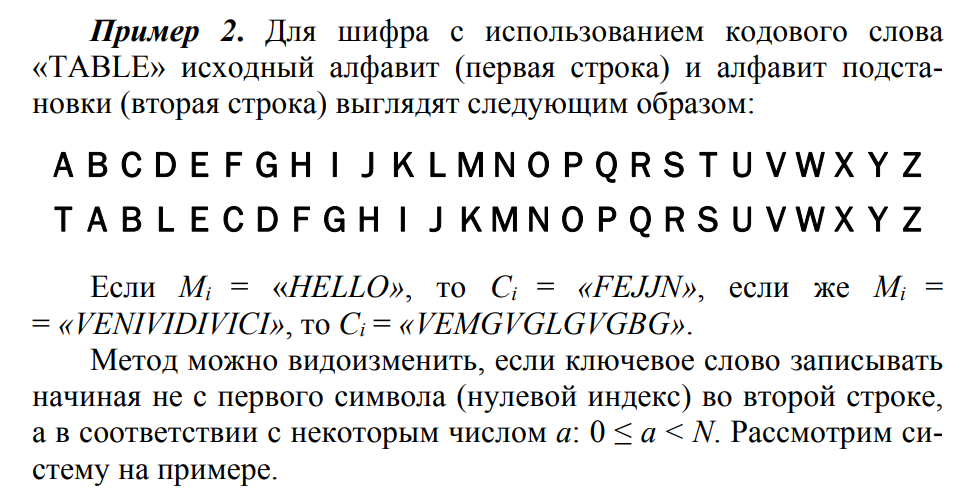
1. **Особенности реализации шифровальной машины Энигма.**



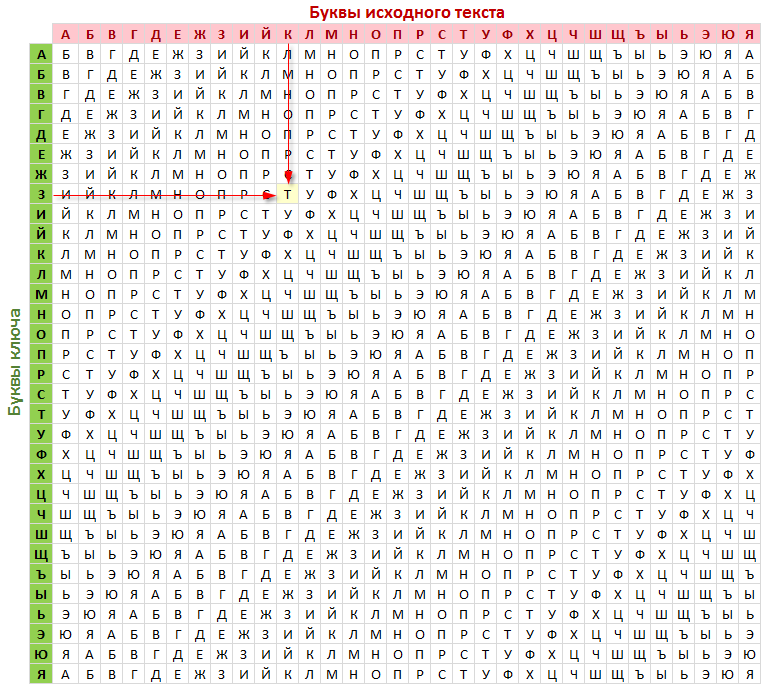
1. **Шифр на основе аффинной системы подстановок Цезаря.**

****

1. **Система шифрования Цезаря с ключевым словом.**



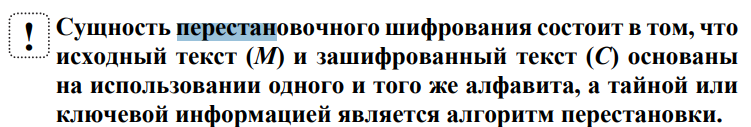
1. **Шифр Виженера.**



Например, m=АРТЕМ, ключ = ИЮНЬ. Добиваем ключ до длины сообщения, если необходимо, и шифруем: берем букву на пересечении буквы исходного сообщения и ключа: АРТЕМ  
 ИЮНЬИ

С=ЙПАВХ

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

1. **Перестановочные шифры.**

В классической криптографии шифры перестановки делятся на два подкласса:

• шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;

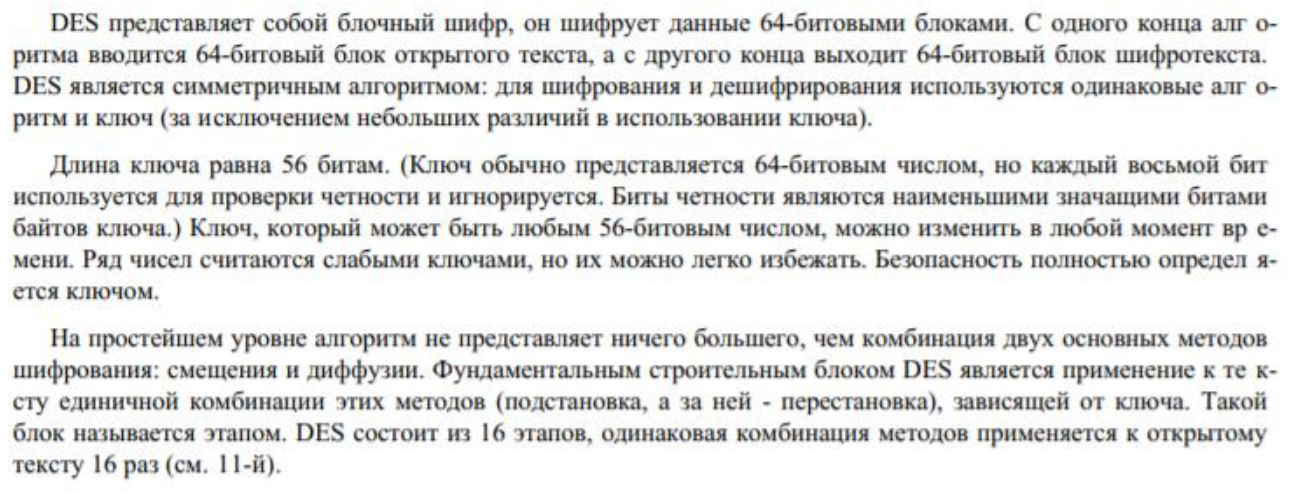
• шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

Практикум с. 40

1. **Методы симметричного криптопреобразования. Стандарт DES. Общая характеристика.**

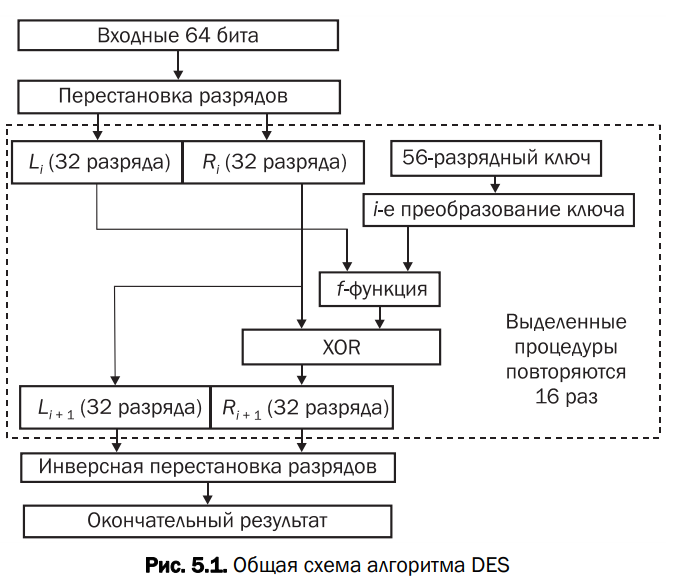
Симметричная = один и тот же ключ для зашифрования и расшифрования сообщения.

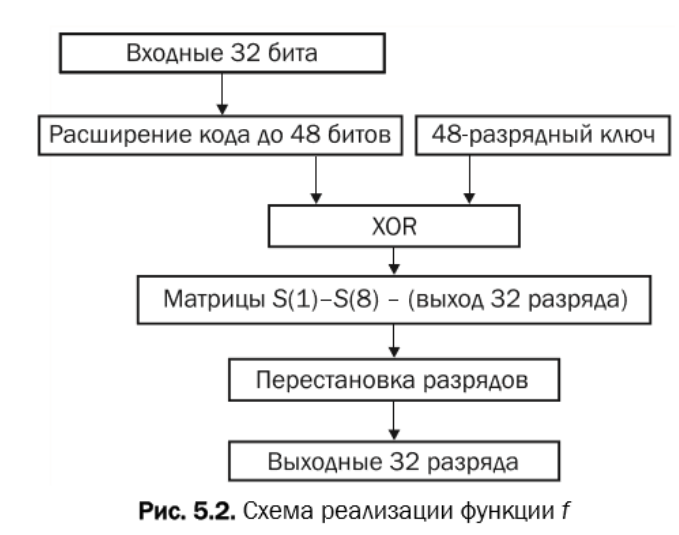
Симметричные алгоритмы подразделяются на два подкласса. Одни алгоритмы обрабатывают открытый текст побитово (иногда побайтово). Такие алгоритмы называют потоковыми.

Другие алгоритмы обрабатывают группы (блоки) битов открытого текста. Эти алгоритмы называют блочными. Примеры симметричных алгоритмов: DES, ГОСТ 28147-89, Lucifer, Blowfish. DES является блочным алгоритмом и оперирует с блоками данных размером 64 бита. При этом используется ключ длиной 56 битов (обычно 64 бита, но каждый восьмой бит для проверки четности и он игнорируется).

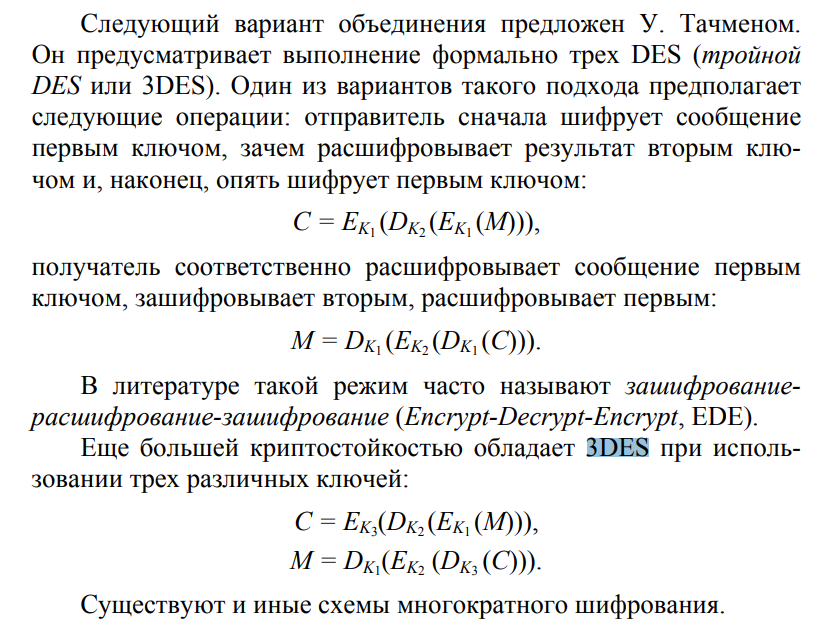
1. **Методы симметричного криптопреобразования. Стандарт DES. Структура одного цикла. Криптостойкость алгоритма.**

DES является блочным алгоритмом и оперирует с блоками данных размером 64 бита. При этом используется ключ длиной 56 битов; дополнительно к ним вычисляются 8 битов четности: 8-й бит в каждом из 8 байтов ключа. Такая длина ключа соответствует 1017 комбинаций, что обеспечивало до недавнего времени достаточный уровень безопасности. Практикум с. 75

****

****

1. **Методы симметричного криптопреобразования. Стандарты 3DES. Реализация и криптостойкость.**

****

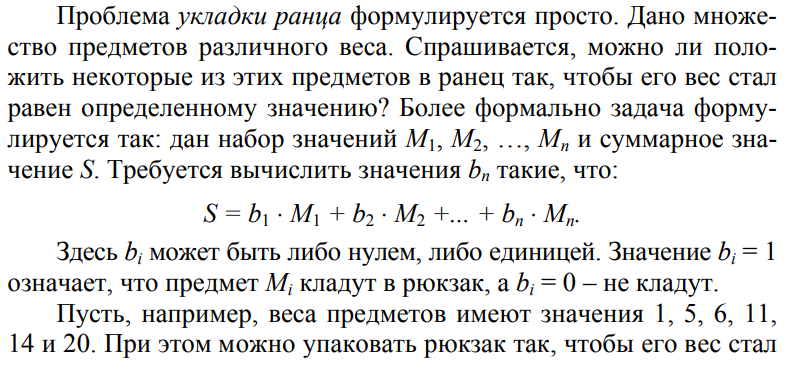
1. **Шифровальная машина Энигма. Устройство, функционирование, криптостойкость.**

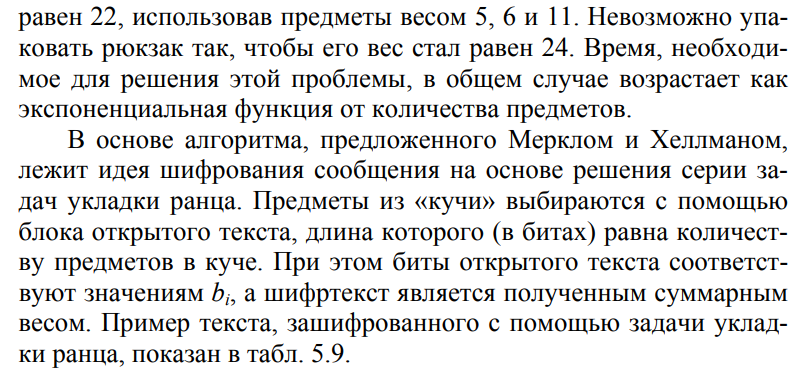
В pdf норм

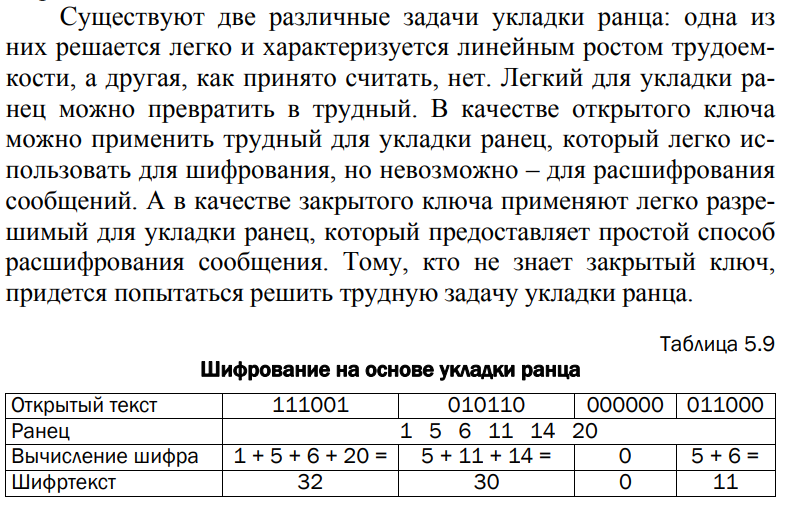
1. **Сравнительная характеристика алгоритмов Lucifer, IDEA, ГОСТ 28147-89, Blowfish.**

**В Pdf норм (какая же залупа на вопросе)**

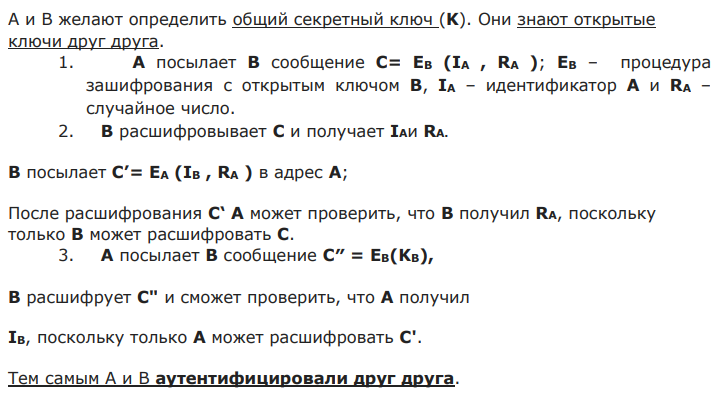
1. **Криптографические системы с открытым (публичным) ключом. Задача об укладке ранца.**

****

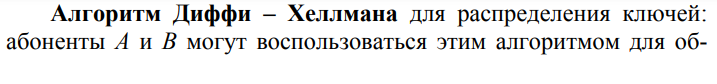
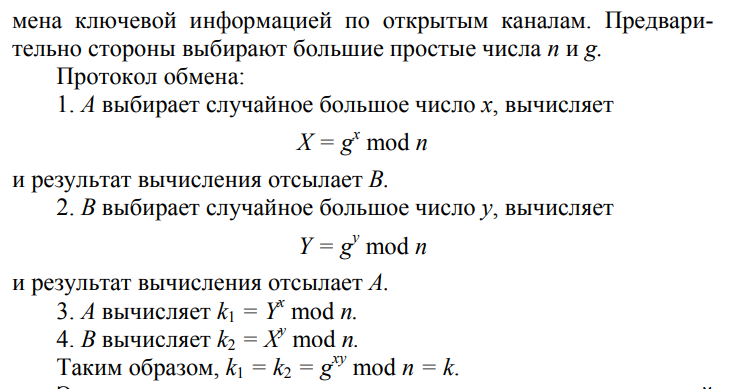
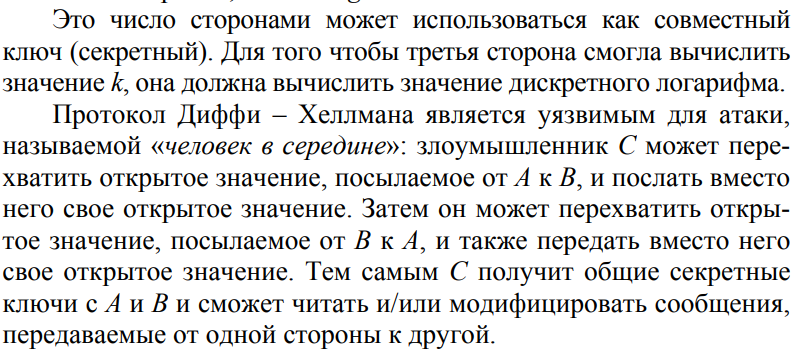
****

****

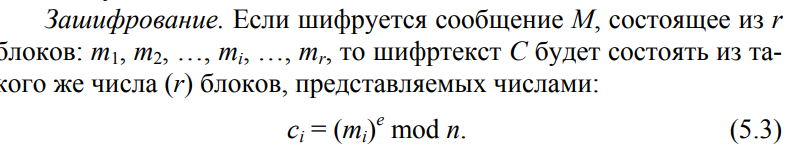
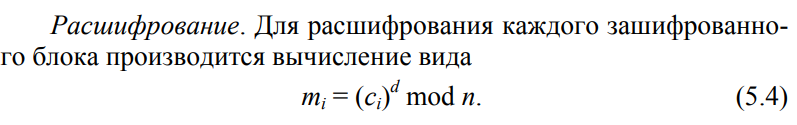
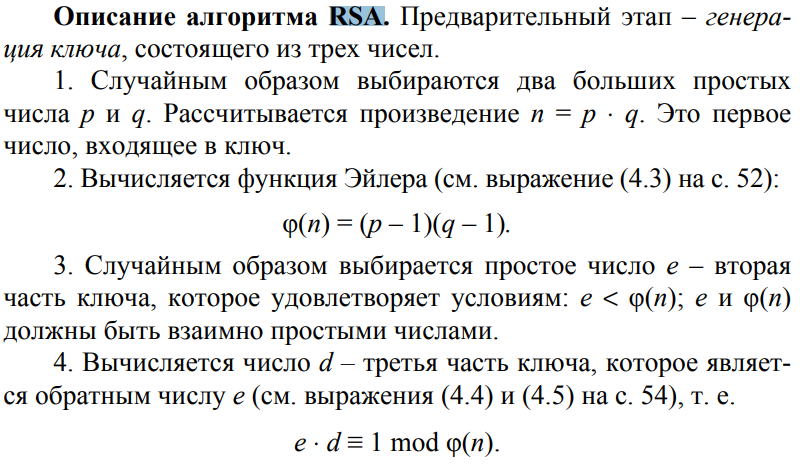
**Почитать расшифрование в практикуме с. 107**

1. **Управление криптографическими ключами. Алгоритм рукопожатия.**
2. **Распределение ключей на основе симметричных систем.**

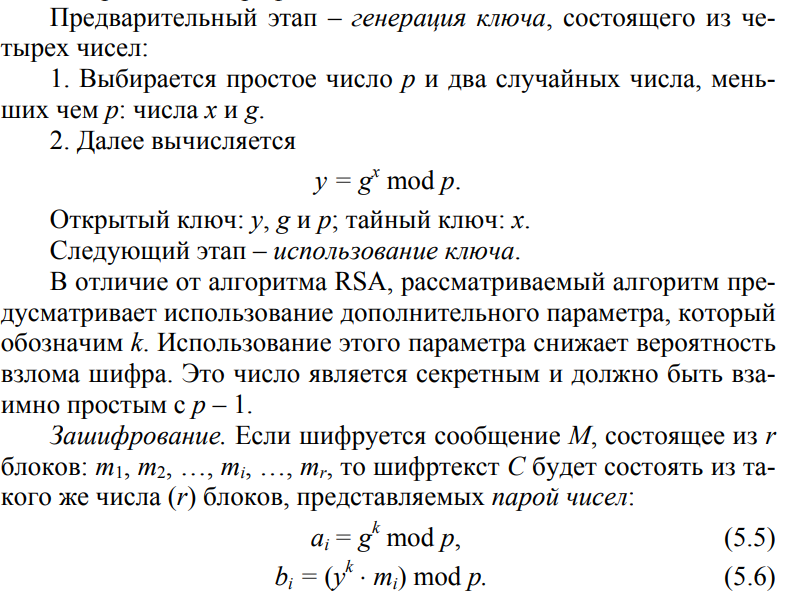
**Наверное pdf**

1. ** Алгоритм передачи ключа по Диффи-Хеллману.**
2. **Алгоритм шифрования RSA. Реализация и криптостойкость.**

**(e, n) – открытый ключ**

**(d, n) – закрытый**

Криптостойкость алгоритма. Зависит от трудоемкости решения проблемы разложения на множители больших чисел. «Лобовой метод» вскрытия системы RSA заключается в нахождении числа d, обратного е по модулю φ(n). Это легко сделать, если известны числа p и q. Отметим, что математически не доказано, что для восстановления сообщения по шифртексту и по значению открытого ключа нужно разложить n на множители. Тем не менее именно этот подход является наиболее очевидным. Известно, что факторизованы числа длиной более 512 битов. Значит, нужно выбирать n больше этого значения. Кроме того, числа p и q не должны быть слишком близкими друг к другу.

1. **Алгоритм шифрования Эль-Гамаля. Реализация и криптостойкость.**

Расшифрование:

g – первообразный корень по модулю p:

g^(ф(р)) mod p =1

1. **Потоковое шифрование. Типы. Гаммирование в потоковом шифровании.**

**pdf**

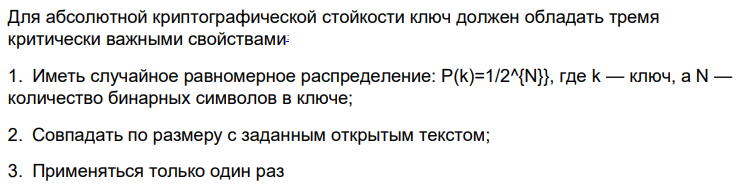
1. **Генерация ключевой информации для потокового шифрования. Генераторы ПСП на основе регистров сдвига.**

**Книга по крипте с. 102**

1. **Особенность шифра Вернама.**

Шифр является примером системы с абсолютной криптостойкостью. Для получения шифротекста открытый текст объединяется операцией «исключающее ИЛИ» с секретным ключом. Например: 11101 – ключ, 11000 – «А», их XOR: 00101.

Исходное сообщение восстанавливается такой же операцией XOR (шифротекст+ключ).

Для абсолютной криптостойкости ключ должен обладать 3-мя свойствами:

Без знания ключа такое сообщение не поддается анализу.

1. **Стеганографические методы защиты информации. Классификация и области использования. Метод наименее значащих бит.**

Стеганографическая система – совокупность средств и методов, которые используются для формирования скрытого канала передачи или хранения информации.

Стеганография подразделяется на **текстовую** и **компьютерную**.

Компоненты:

А) контейнер (файл куда будем осаждать (скрывать) сообщение

Б) тайное сообщение M, которое осаждаем в контейнере

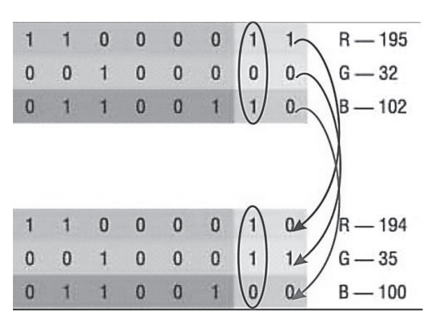
В) ключи

Г) контейнер со встроенным (осажденным) сообщением

**Методы текстовой стеганографии: 1) Синтаксические, 2) Лингвистические**. **Синтаксические** – те, которые не затрагивают синтаксис. Примеры: изменение интервалов между строк, различная длина пробелов между словами, внесение специфических изменений в шрифты (начертания отдельных букв), изменение интервала табуляции, увеличение длины строки (с помощью пробелов), использование регистра букв, метод невидимых символов. **Лингвистические** - те, которые затрагивают синтаксис. Примеры: метод переменной длины слова, метод первой буквы, метод синонимов, мимикрия, спам.



Метод наименее значащих битов основан на ограниченных способностях зрения или слуха человека, и людям тяжело различать незначительные вариации цвета или звука. Каждая точка цвета кодируется тремя байтами: R, G, B. Например:



Младшие биты (выделены бледным, справа) дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

1. **Понятие эллиптической кривой. Принципы построения криптосистемы на эллиптических кривых**

Эллиптические кривые (ЭК) – математический объект, который может быть определен над любым полем.

Эллиптическая кривая над вещественными числами – множество точек, описываемых уравнением y2=x3+ax+b, где a и b – константы, удовлетворяющие условию 4a3+27b2 ≠ 0;

Часть ЭК – бесконечно удаленная точка О.

Принципы построения в pdf

1. **Представление и описание эллиптической кривой на основе алгебраической геометрии**

В общем случае кубические уравнения для эллиптических кривых имеют вид:

y2 + а ⋅ х ⋅ у + b ⋅ y = х3 + с ⋅ х2+ d ⋅ x + е (5.13)

где a,b,c,d – действительные числа, удовлетворяющие некоторым простым условиям.

С другой стороны, эллиптическая кривая – это набор точек (x, y), удовлетворяющих уравнению (5.13) для переменных (x, y) и констант (a, b, c, d, e), принадлежащих множеству F, где F – поле.

Вспомним некоторые важные характеристики поля. Конечным полем называется алгебраическая система, которая состоит из конечного множества F и двух бинарных операций (сложения и умножения).

Порядком поля называется количество элементов в поле (во множестве F)

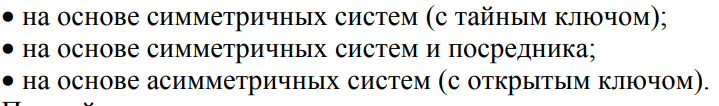
1. **Арифметические операции в эллиптической криптографии**

**pdf**

1. **ЭЦП. Назначение и свойства.**

**pdf**

1. **ЭЦП. Основные методы генерации. Атаки на ЭЦП**

****Методы генерации:

Целью атак на цифровые подписи является, в конечном итоге, возможность их подделки или фальсификации

Основные виды атак:

● Атака с использованием открытого ключа. Имеется в виду ключ субъекта, подписывающего документ. Криптоаналитик обладает только открытым ключом.

● Атака на основе известных сообщений. В распоряжении криптоаналитика имеются некоторые ЭЦП и соответствующие им документы.

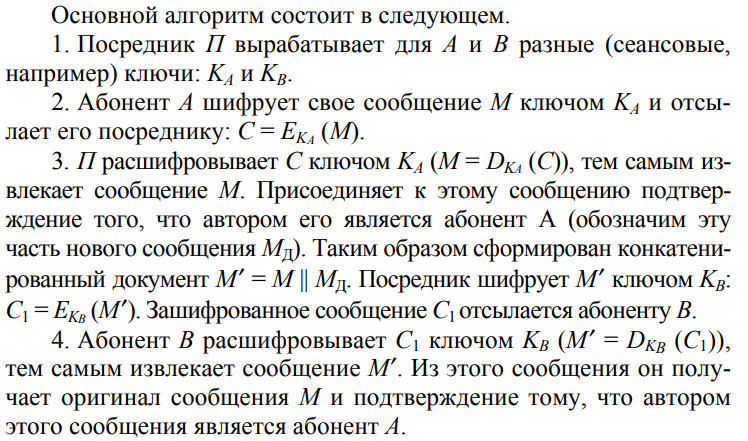
● Адаптивная атака на основе выбранных сообщений. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.

1. **ЭЦП на основе симметричной криптографии**

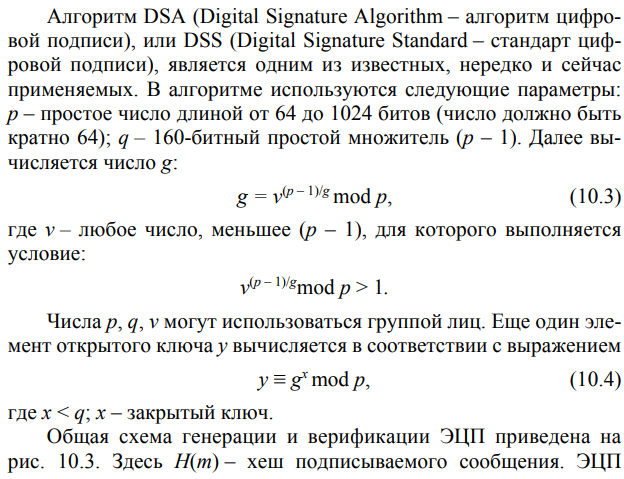
**Pdf**

1. **ЭЦП на основе алгоритма RSA**

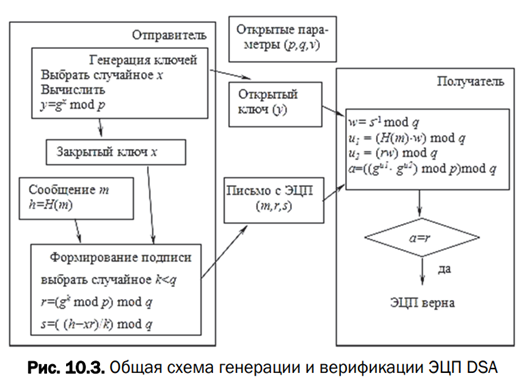
**pdf**

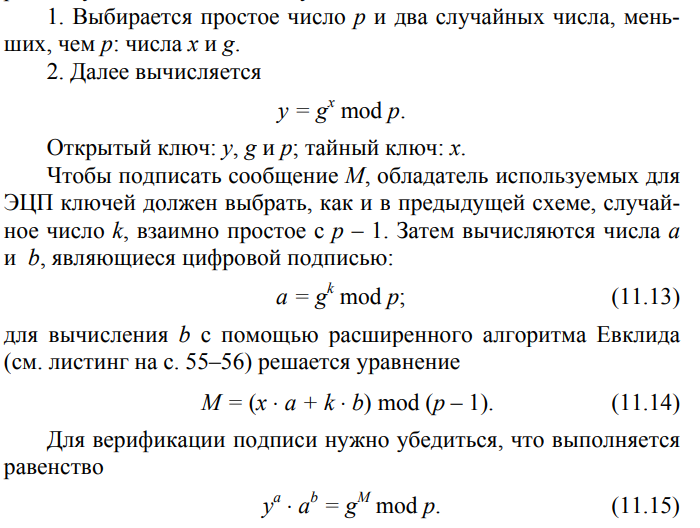
1. **ЭЦП на основе симметричной криптосистемы и посредника**
2. **ЭЦП DSS.**

То же, что DSA



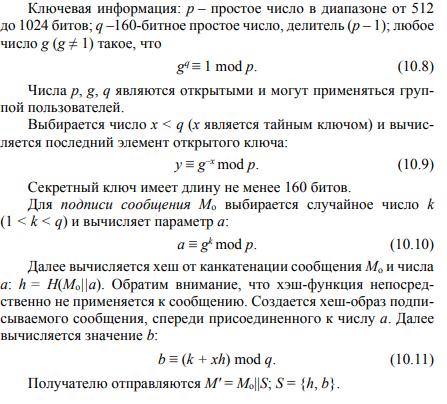


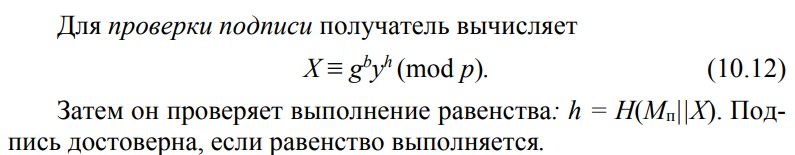


1. **ЭЦП на основе алгоритма Эль-Гамаля**
2. **ЭЦП на основе эллиптической кривой.**

**С. 170 в книге криптография**

1. **Алгоритм К. Шнорра. Стандарт ЭЦП в РБ.**

****

****

1. **Протокол Kerberos.**

**pdf**

1. **Деструктивные программы. Классификация и методы нейтрализации.**

**pdf**

1. **Оценка безопасности парольной защиты.**

**pdf**