**1.** Криптография — это наука о способах преобразования информации с целью ее защиты от незаконных пользователей. Методы решения противоположной задачи (взлом криптографической защиты) составляют предмет другой науки — криптоанализа.

Целью применения криптографических методов является защита информационной системы от целенаправленных разрушающих воздействий (атак) со стороны противника.

Основные цели криптографии:

-Обеспечение конфиденциальности данных

-Обеспечение целостности данных

-Обеспечение аутентификации

-Обеспечение невозможности отказа от авторства

**2.** Типы атак на алгоритмы шифрования

1. Атака с известным шифртекстом. Злоумышленник имеет лишь набор зашифрованных данных, алгоритм сообщений и, возможно, некоторые данные об их открытом содержании.

2. Атака с известным открытым текстом. У злоумышленника имеется набор пар "открытый текст - зашифрованный текст".

3. Атака с выбором открытого текста. Злоумышленник может выбирать определенные открытые тексты и получать соответствующие им зашифрованные

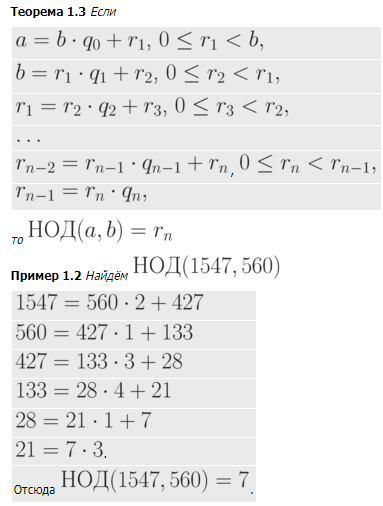
4. Адаптивная атака с выбором открытого текста. Многократно повторяемая атака с выбором открытого текста по следующему сценарию: выбор открытого текста - его шифрование - анализ результатов - выбор следующего открытого текста и т. д.

5. Атака с выбором шифртекста (простая и адаптивная). Аналогична типам 3 и 4, отличается лишь тем, что злоумышленник выбирает не открытые тексты, а зашифрованные - и анализирует результаты их расшифрования.

6. Атака с выбором открытого и зашифрованного текста. Злоумышленник может выбирать как открытые тексты, так и зашифрованные.

Криптографическая стойкость это способность алгоритма противостоять криптоанализу.

**3.** Инверсия по модулю – такое натуральное число, которое при умножении по модулю на данное число дает в результате единицу. Инверсию по модулю m можно вычислять с помощью так называемого обобщенного алгоритма Евклида



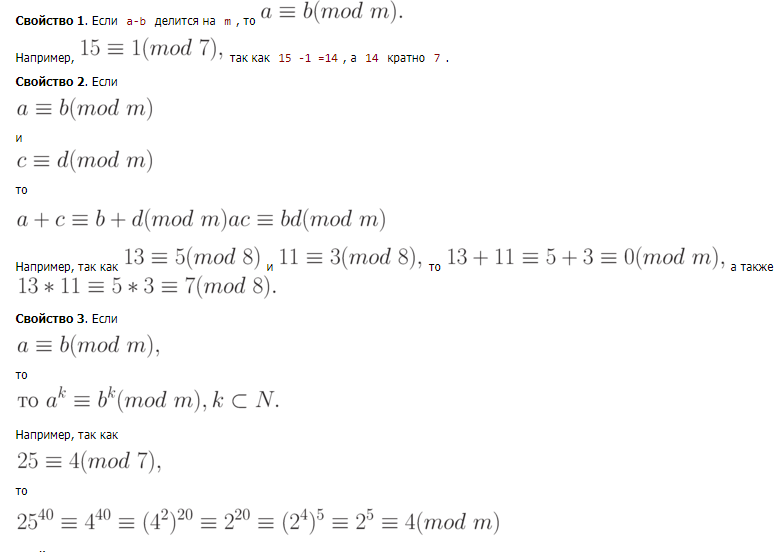
**4.** Немецкий математик Карл Фридрих Гаусс предложил *запись*

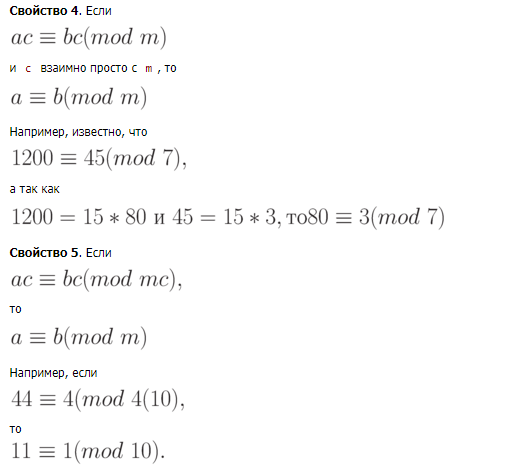
a \equiv b (mod\ m),

для двух чисел a и b, если они имеют одинаковые остатки от деления на m (читается a сравнимо с b по модулю m ). Например,

1997 \equiv 1(mod 4),\\
7k +1 \equiv 1(mod 7),\ где\ k - любое\ целое\ число.

Сравнения обнаруживают полезные для математиков и криптографов свойства, во многом похожие на свойства равенств. Эти свойства позволяют существенно упрощать арифметические вычисления, если нас интересует только *остаток от деления* на некоторое число m. Так, например, свойства сравнений полезны при расчетах в алгоритмах шифрования с открытым ключом.





**5.** Существует два типа критериев простоты: детерминированные и вероятностные

Детерминированный алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу. Вероятностный алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ

**6.** Кодированием называют универсальный способ отображения информации при её хранении, обработке и передаче в виде системы соответствий между сигналами и элементами сообщений, при помощи которых эти элементы можно зафиксировать

**Пример -** Азбука Морзе

Алгоритм - •− •−•• −−• −−− •−• •• − −−

**7.** В настоящее время общепризнанным является подразделение криптографических алгоритмов на следующие основные категории:

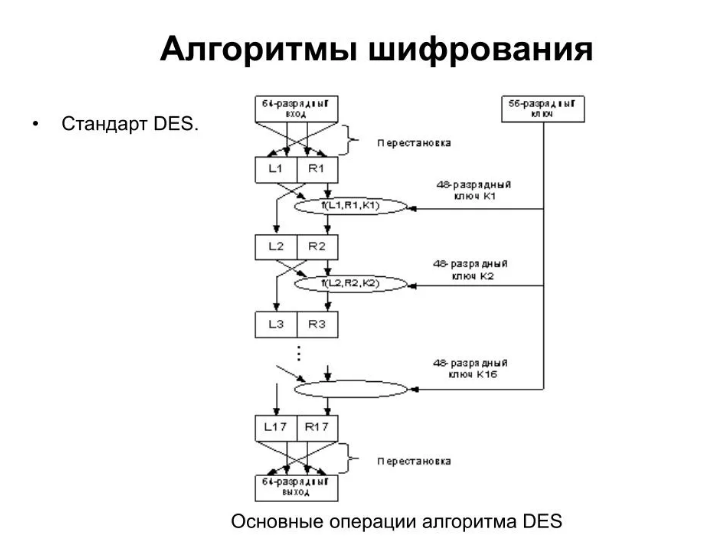
- алгоритмы шифрования с секретным ключом (симметричные)

+ блочные шифры

+ поточные шифры

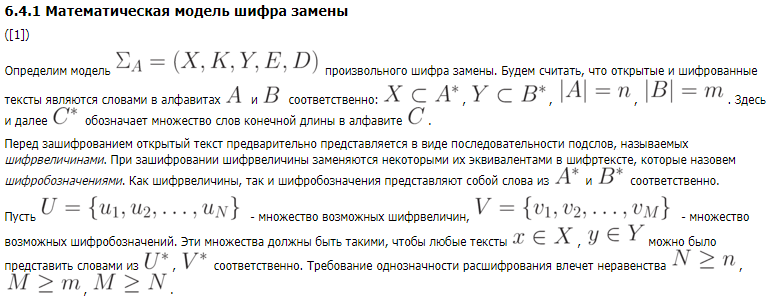
- алгоритмы шифрования с открытым ключом (асимметричные)

**Пример**



**8.** **Шифры замены, Атбаш, Цезарь, кодовое слово**

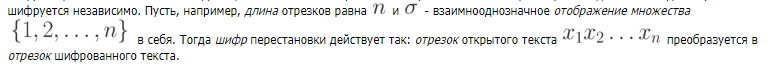
Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других "частей" открытого текста на аналогичные "части" шифрованного текста



**9. Шифры перестановки**

Простая перестановка, маршрутная перестановка, вертикальная перестановка, поворотная решетка, двойная перестановка

Ключом шифра перестановки является перестановка номеров символов открытого текста. Это, в частности, означает, что длина ключа шифрования должна быть равна длине преобразуемого текста



**10. Гамми́рование, или Шифр XOR,** — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст.

Пусть символам исходного алфавита соответствуют числа от 0 (А) до 32 (Я). Если обозначить число, соответствующее исходному символу, x, а символу ключа – k, то можно записать правило гаммирования следующим образом:

z = x + k (mod N),

где z – закодированный символ, N - количество символов в алфавите, а сложение по модулю N - операция, аналогичная обычному сложению, с тем отличием, что если обычное суммирование дает результат, больший или равный N, то значением суммы считается остаток от деления его на N.

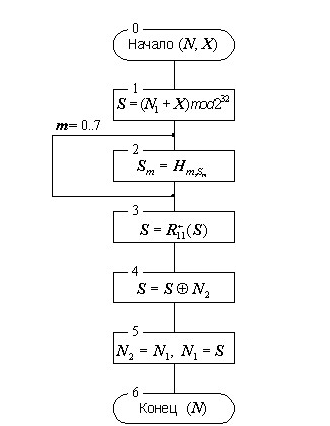
**11.** **Принципы построения блочных шифров. Схема Фейстеля.**

Перемешиванием называется использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи символов открытого и зашифрованного текста, а также ключа и зашифрованного текста.

**12.** **Алгоритм симметричного шифрования DES**.



**13.** **Алгоритм симметричного шифрования ГОСТ 28147-99**.



**14.** **Режимы выполнения алгоритмов симметричного шифрования**.

ECB, CBC, CFB, OFB

**15.** **Поточные криптосистемы**. Принципы построения. Классификация. Проблема синхронизации.

Паша Проебался…

**16.** **Поточные шифры**. Отличия от блочных. Стойкость. Методы анализа.

важнейшим достоинством поточных шифров перед блочными является высокая скорость шифрования, соизмеримая со скоростью поступления входной информации; поэтому, обеспечивается шифрование практически в реальном масштабе времени вне зависимости от объема и разрядности потока преобразуемых данных.

**17.** **Примеры поточных шифров, использующих аддитивные генераторы**.

RC4, SEAL, WAKE

**18.** **Основные методы и виды криптоанализа. Примеры**.



**19.** **Линейный криптоанализ**

Линейный криптоанализ — особый род атаки на симметричные шифры, направленный на восстановление неизвестного ключа шифрования, по известным открытым сообщениям и соответствующим им шифртекстам.

**20.** **Разностный криптоанализ**.

метод криптоанализа симметричных блочных шифров (и других криптографических примитивов, в частности, хеш-функций и поточных шифров)

**21. Схема работы ассиметричного ключа**:

1. Получатель генерирует два неразрывно связанных ключа – открытый ключ Кв и секретный ключ kв.

2 Получатель по открытому каналу отправляет свой открытый ключ Кв отправителю.

3 Отправитель зашифровывает открытый текст под управлением полученного открытого ключа получателя сообщения и получает криптограмму.

4 Отправитель отправляет криптограмму получателю.

5 Получатель расшифровывает криптограмму под управлением своего секретного ключа kв.

**22.** **RSA это криптографический** алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Стойкость данного алгоритма определяется его длиной. Надежным считается алгоритм RSA длинной не менее 1024 бит.

**23.** **Схема Эль-Гамаля** это криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. При одинаковой длине ключа криптостойкость равная RSA.

**24**. **Криптосистема Рабина это** криптографическая система с открытым ключом, безопасность которой обеспечивается сложностью поиска квадратных корней в кольце остатков по модулю составного числа. Безопасность системы обусловлена сложностью разложения на множители больших чисел. Она является доказуемо стойкой к атаке на основе подобранного открытого зашифрованного текста, но является абсолютно беззащитной перед атакой на основе выбранного шифртекста.

**25.** **Алгоритм шифрования ГОСТ 28147-89** по своей структуре аналогичен широко распространенному стандарту криптографического преобразования DES. При этом существенно увеличена длина ключа

**26.** **Протокол Ди́ффи-Хе́ллмана** это криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

**27.** **Хеш-функция это функция,** осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом.

Виды «хеш-функций»:

1. «Хеш-функции», основанные на делении

2. «Хеш-функции», основанные на умножении

3. Хеширование строк переменной длины

4. Идеальное хеширование

5. Универсальное хеширование

**28.** **Типы атак на хеш-функции**:

1. нахождение прообраза x по заданному значению y.

2. нахождение прообраза xⁿ по заданному прообразу x, для которого выполняется условие h(x)=h(xⁿ).

**29. MD5** это 128-битный алгоритм хеширования. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Широко применялся для проверки целостности информации и хранения хешей паролей.

**30.** **SHA-1** это алгоритм криптографического хеширования. Алгоритм генерирует 160-битное (20 байт) хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатеричное число длиной в 40 цифр.

**31**. **ГОСТ Р 34.11-94**

При обработке блоков используются преобразования по алгоритму ГОСТ 28147—89;

Обрабатывается блок длиной 256 бит, и выходное значение тоже имеет длину 256 бит.

Определяет контрольную сумму, рассчитанную по всем блокам исходного сообщения, которая является частью финального вычисления хеша, что несколько затрудняет коллизионную атаку.

Применены меры борьбы против поиска коллизий, основанном на неполноте последнего блока.

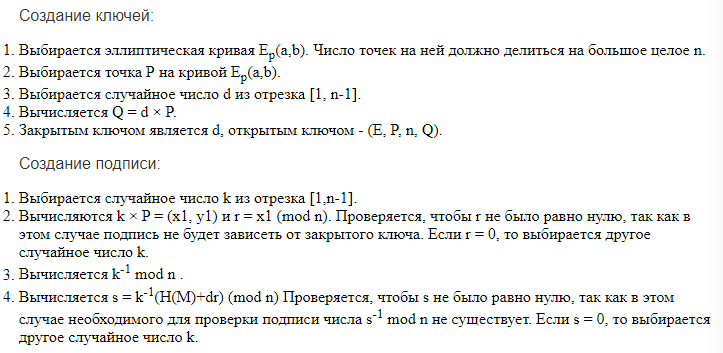
Обработка блоков происходит по алгоритму шифрования ГОСТ 28147—89, который содержит преобразования на S-блоках, что существенно осложняет применение метода дифференциального криптоанализа к поиску коллизий.

**32.** **ЭЦП** может быть полноценной заменой рукописной подписи и обладать юридической силой согласно законодательству РФ.

**33.** **DSS** - использован для генерации цифровой подписи. Цифровая подпись служит для установления изменений данных и для установления подлинности подписавшейся стороны

**34.** **ЭЦП** предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Иначе говоря, открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ. Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, как и в асимметричных системах шифрования, используются разные математические схемы.

**35.** **Эллиптические кривые**



**36. стеганография** скрывает само существование сообщения.

Невидимые чернила - проявляется только при определенных условиях (нагрев)

запись на боковой стороне колоды карт, расположенных в условленном порядке;

запись внутри вареного яйца;

«жаргонные шифры», где слова имеют другое обусловленное значение;

трафареты, которые, будучи положенными на текст, оставляют значащие буквы;

узелки на нитках и т. д.

Классическая стеганография, Компьютерная, Цифровая

**37**. **СтегоАнализ** - наука о выявлении факта передачи скрытой информации в анализируемом сообщении



**38.** **Kerberos** - использование локальной формы личной идентификации, называемой билетами, которые предоставляются сервером аутентификации. Каждый билет принадлежит определенным областям, которые определяют, к каким службам он предоставляет доступ. Эти билеты зашифрованы, и для их использования требуется несколько уровней дешифрования. Эта система билетов гарантирует, что конфиденциальная информация, такая как пароли, никогда не будет отправлена ​​по сети.

**39.** **Двусторонняя аутентификация** – это обоюдная проверка и установление подлинности, при которой информационная система также обязана подтвердить свою аутентичность перед пользователем.

**40.** **Односторонняя аутентификация** - основанная на метке времени (табл. 4.3). Если у претендента и проверяющего есть синхронизированные (в пределах погрешности) системные часы, нет необходимости посылать запрос. Претендент сразу может направить сообщение с включенной в него меткой времени, а проверяющий — сверить метку с показаниями своих часов.

**41**. **Защита информации** в эл. Платежах - При взаимодействии с POS-терминалом реквизиты пластиковой карты считываются с ее магнитной полосы встроенным считывателем. Клиент вводит собственный PIN-код, который знает только он. Элементы PIN-кода используются в общем алгоритме шифрования записи на магнитной полосе и являются электронной подписью владельца карты. Запросы на авторизацию поступают в процессинговый центр, которая обеспечивает их обработку. Процессинговым центром ведется база данных, в которой содержатся данные о банках и владельцах пластиковых карт. Далее, происходи работа со счетом владельца.