на основе процедуры шифрования (По принципу размещения символов)

1. подстановочные

1. моноалфавит

2. Полиалфавит

3. полигамные

4. амофонические

2. перестановочные

1. Одиночной перестановки

1. простая

2. блочная

2 Множественной престановки

3. Машрутная перестоновка

4. Вертикальной перестановки

по принципу формирования шифртотекста

1. блочные

2. поточные

на основе типа ключа (по назначению ключа)

1. симметричные (с тайным ключом)

2. ассиметричные (с открытым ключом)

7 des

**Симметричные криптосистемы** — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Само название конструкции Фейстеля (сеть) означает ее ячеистую топологию. Формально одна ячейка сети соответствует одному раунду зашифрования или расшифрования сообщения.

В основе криптостойкости блочных шифров лежит идея К. Шеннона в представлении составного шифра таким образом, чтобы от обладал двумя важными свойствами: рассеянием и перемешиванием

Рассеивание подразумевает, что каждый символ (символ или бит) в зашифрованном тексте зависит от одного или всех символов в исходном тексте

Идея относительно перемешивания заключается в том, что оно должно скрыть отношения между зашифрованным текстом и ключом

Каждый 8-й бит исходного 64-битного ключа отбрасывается. Эти 8 битов, находящих в позициях 8, 16, 24, 32, 40, 48, 56, 64, изначально добавляются в исходный ключ таким образом, чтобы каждый байт содержал четное число единиц. Это используется для обнаружения ошибок при обмене и хранении ключей по известным алгоритмам избыточного кодирования. Один избыточный бит в ключе DES формируется, как видим, в соответствии с кодом простой четности. Этот код позволяет в кодовом слове (в нашем случае – в каждом байте ключа) обнаруживать ошибки, количество которых нечетно.

Из-за того, что первоначальный ключ изменяется при получении подключа для каждого раунда алгоритма, определенные

первоначальные ключи являются слабыми. Вспомним, что первоначальное значение разделяется на две половины, каждая из которых сдвигается независимо. Если все биты каждой половины равны 0 или 1, то для всех раундов алгоритма используется один и тот же ключ. Это может произойти, если ключ состоит из одних 1, из одних 0, или если одна половина ключа состоит из одних 1, а другая – из одних 0.

Полуслабые ключи - некоторые пары ключей при зашифровании переводят открытый текст в идентичный шифртекст. Иными словами, один из ключей пары может расшифровать сообщения, зашифрованные другим ключом пары

**8 псп**

Период ПСП, смысл генератора

потоковый - симметричный

Период ПСП - через сколько вернётся на исходное состояние

период (2^n)-1

зависит от начальной последовательности

неприводимый - не замыкается, совпадает с 2^n-1

приводимый - когда не совпадает 2^n

синхронные - не зависят от сообщения

асинхронные - зависят от сообщения, ключ формируется на основе сообщения

случайные числа (последовательности) – последовательность элементов, каждый из которых не может быть предсказан (вычислен) только на основе знания предшествующих ему элементов данной последовательности;

псевдослучайные числа – последовательность элементов, полученная в результате выполнения некоторого алгоритма и используемая в конкретном случае вместо последовательности случайных чисел.

**9 рюкзак**

ассиметричный

задача о рюкзаке - Дано множество предметов общим числом z различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению S?

криптостойкость - плохая, зависит от кол-ва элементов, которые нужно уложить в ранец.Секретная лазейка.

секретная лазейка - зная числа а, a^-1 и n («секретную лазейку»), можно восстановить сверхвозрастающую последовательность по нормальной последовательности. Важно то, что числа а и n («секретная пара») не обязательно должны быть теми же, что использовались при создании системы легальным пользователем.

Сверхвозрастающая последовательность - в которой каждый последующий член больше суммы всех предыдущих.

Ранцевый (рюкзачный) вектор S = (s1, . . ., sz) – это упорядоченный набор из z, z ≥ 3, различных натуральных чисел si

Односторонней функцией называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, т. е., зная х, легко вычислить f(x), но по известному f(x) трудно найти подходящее значение x.

**10 rsa эль-гамаль**

ассиметричный

Основная теорема арифметики. Всякое натуральное число N, кроме 1, можно представить как произведение простых множителей

Задача дискретного логарифмирования формулируется так: для данных целых чисел а и b, 1 < а, b < n найти логарифм – такое целое число х, что

ax ≡ b (mod n),

Китайская теорема об остатках. В общем случае, если разложение числа N на простые множители представляет собой p1\*p2\*…\*pt (некоторые простые числа могут встречаться несколько раз), то система уравнений (x mod pi) = ai, где i= 1,2…, t имеет единственное решение: x, меньшее N.

проблемы двух алгоритвом: трудность вычисления логарифмов (дискретного логарифмирования) (эль-гамаль) и факторизация (rsa)

проблема факторизации: сложно разложить на простые множители

Первообразный корень по модулю р является таким числом, что его степени (g^i, 1 ≤i≤p-1 ) дают все возможные по модулю р вычеты (остатки), которые взаимно просты с p.

на что влияет первообразный корень (эль гамаль): чем больше, тем лучше криптостойкость (если посчитать неправильно, то потом не расшифруешь)

проблема эль-гамаля: увеличивается зашифрованная последовательность в 1.5-2 раза это плохо, потому что увеличиваются данные при передаче

криптостойкость примерно одинаковая, rsa больше используется

ассиметричная криптография: открытый и закрытый ключ

**11 хеш функции**

Хеш-функция – математическая функция, h = H(М), которая принимает на входе строку символов М переменной длины n и преобразует ее в выходную строку фиксированной длины

Хеширование - результат хеш функции

Стойкость к коллизиям первого рода: для заданного сообщения M должно быть практически невозможно подобрать другое сообщение N, для которого H(N)=H(M).

свойства хеш функции: детерминированность (переменная длина входит, постоянная длина выходит), скорость вычисления хэша должно быть быстрой, сложность обратного вычисления (однонаправленность), лавинный эффект, коллизионная устойчивость

коллизия: на входе разная строка, на выходе один и тот же хэш

коллизия 1-го 2-го рода: 1 - h(m) = m; 2 - два разных сообщения, а хеш одинаковый

парадокс дней рождений: из группы 23 вероятность 50% что два чела с одинаковыми ДР

что лучше md или sha: sha. md- взломан, медленне, шанс коллизий больше.

**12 эцп на основе rsa**

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

классификация ЭЦП:

на основе симметричных систем (с тайным ключом),

на основе симметричных систем и посредника(человек между),

на основе асимметричных систем (с открытым ключом).

Функции ЭЦП:

• аутентифицировать лицо, подписавшее сообщение;

• контролировать целостность подписанного сообщения;

• защищать сообщение от подделок;

• доказать авторство лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшими отличительными особенностям ЭЦП являются:

• ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);

• указанная бинарная последовательность зависит от содержания подписываемого сообщения. Как

вычисляет хеш (хеш-образ) сообщения М: Н(М),

вычисляет содержание ЭЦП (собственно ЭЦП, S) по хешу Н(М) с использованием своего закрытого ключа, d: S = Сd(Н(М));

передаём конкатенацию эцп и сообщения

нужно передать открытый ключ

получатель использует открытый ключ, чтобы извлечь из эцп хэш

применяем к сообщению операцию хеширования и сравниваем хеши, если они равны, то подпись верифицирована

виды эцп: Шнорра, Эль-Гамаля, на основе DSA, на основе RSA, на основе хешей подписываемых сообщений

В Беларусь ЭЦП на основе Шнора

**13 эллептические кривые**

**Эллиптические кривые** – математический объект, который может быть определен над любым полем.

Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением у2 = х^3 + aх + b (уравнение Вейерштрасса)

Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим символом

**Группа** – непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

Группа для ЭК есть непустое множество, элементы которого являются точками ЭК, обладающими следующими свойствами:

единичный элемент – это бесконечно удалённая точка О;

обратная величина точки R – это точка, симметричная относительно оси Х;

сложение задается следующим правилом: сумма трех ненулевых точек P, Q и -R, лежащих на одной прямой, будет равна P + Q + (-R) = О.

В соответствии с этим можем сформулировать законы сложения точек эллиптической кривой:

прямая, проходящая через точки R и –R, является вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке; если R = (х, – у), то R + (х,у) = О. Точка (х,у) является отрицательным значением точки R и обозначается –R. Таким образом, по определению R + (–R) = О;

P + Q = R: пусть P и Q – две различные точки ЭК (рис. 11.1), и Р не равно Q; если проведем через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой –R; точка –R отображается относительно оси Х в точку R, равную сумме точек P и Q: P + Q = R;

Что будет, если P = Q? - В этом случае мы можем говорить об операции удвоения точки: P + Р = 2Р. Обобщив (к точке 2Р можно прибавить еще раз точку Р: 2Р + Р), сформулируем принцип умножения точки Р на целое положительное число n – определяется как сумма n точек Р: nP = P + P + P + … + P.

**Конечное поле** – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p, где p – простое число

В криптографии на основе ЭК тайный ключ – это случайное целое d , выбранное из множества {1, 2, ..., q–1}, где q – порядок подгруппы; открытый ключ – это точка Q, такая, что Q = dG, где G – базовая точка подгруппы

Как и в случае с непрерывными ЭК, теперь важным является вычисление некоторого числа d, если мы знаем P и Q для Q = dP. Это и есть задача дискретного логарифмирования для эллиптических кривых.

**направления использования ЭК в криптографии:**

в алгоритмах согласования (**передача**) ключевой информации (на основе идеи Диффи-Хеллмана),

в алгоритмах асимметричного шифрования/дешифрования сообщений,

в алгоритмах генерации/верификации ЭЦП.

При использовании ЭК зашифрование предполагает представление сообщения в виде точки Р (или представления каждого блока сообщения в виде разных точек Рi) ЭК с известной точкой G и известным Q. Соответственно **шифртекст** – это две точки на той же ЭК: С1 и C2 или Сi1 и Ci2.

какие операции можно применить к эллептическим кривым: сложение точек на эллептической кривой и умножение точки на скалярное число

коэффициент секущей: это лямбда, если у нас скалярное умножение на 2, то эти точки равны, но высчитывается по разным формулам

сложнее взломать, при одинаковой криптостойкости, длина ключа меньше

**14 стеганография**

контейнер: изображение

компоненты: контейнер, тайное сообщение, отправитель, получатель

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

При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации. «Скрытость» канала передачи тайной информации отличает стеганографии от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

Стеганографическая система обычно определяется, как некоторое множество отображений одного пространства (множества возможных сообщений, М) в другое пространство (множество возможных стеганосообщений, S, и наоборот.

**Основные компоненты стеганосистемы:**

**контейнер**, С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение, М; именно контейнер является упомянутым скрытым каналом;

**тайное сообщение,** М, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер [2, 53-56]; здесь речь может идти о невидимых цифровых водяных знаках, ЦВЗ);

**ключи или ключевая информация,** K системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом осаждения/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий (или третьи) – для предварительного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д. [2, 57, 58];

контейнер с осажденным сообщением или **стеганоконтейнер**, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

для полноты упомянем также субъектов системы: **отправителя** и **получателя**.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

**аудиостеганография**,

**видеостеганография,**

**графическая стеганография,**

**текстовая стеганография**

**Стеганографической системой** ∑ будем называть совокупность сообщений M, контейнеров C, ключей K, стеганосообщений (заполненных контейнеров) S и преобразований (прямого F и обратного F-1), которые их связывают: ∑ = (M, C, K, S, F, F^-1)

При построении стеганосистемы должны, таким образом, учитываться следующие основные положения:

свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;

противник имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;

потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Рассмотрим это на примере 24битного растрового RGB-изображения. Как известно, каждая точка кодируется 3-мя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из 3-х каналов определяет оттенок пикселя. Замена одного или даже нескольких младших бит для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.