**Лаба 03**

aх ≡ 1 mod n

aх = nk +1.

1.Множество всех целых чисел (обозначим буквой Z) есть набор всех действительных чисел без дробной части: {..., -3, -2, -1, 0, 1, 2, 3, ...}.

Натуральные числа являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

Делимость – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, такое, что bq=a, то говорят, что число a делится на b. В этом случае b называется делителем числа a, а a называется кратным числа b.

Собственный делитель - Делитель a называется собственным делителем числа b, если 1<|a|<|b|, и несобственным – в противном случае.

НОД - Наибольшим общим делителем для двух целых чисел и называется наибольший из их общих делителей.

2. Основная теорема арифметики - Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей 27 = 3 \* 3 \* 3

3. Сложность решения задачи разложения больших чисел на простые сомножители, известной как проблема факторизации, определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA

4. 1, 8, 1, 1, 3 1, 1, 1

5. Каноническая форма - Порядок записи сомножителей после последнего знака равенства соответствует канонической форме.

6. аu + bv = d.

называется также реализацией «расширенного алгоритма Евклида». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.

7. натуральных чисел, не превосходящих некоторое число n и взаимно простых с n? Ответ на этот вопрос связан с каноническим разложением числа n на простые множители (см. выше основную теорему арифметики и пример 4). Так, если где p1, p2, ..., pn – разные простые множители, то число φ(n) натуральных чисел, не превосходящих n и взаимно простых с n можно точно определить по формуле Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется функцией Эйлера и обозначается φ(n).

8. Если n – простое число, а число а не кратно n, то справедливо: a ^ n = 1 mod n. Для нахождения обратных чисел по модулю

9. Модулярная арифметика так же коммутативна, ассоциативна и дистрибутивна, как и обычная арифметика

10. 1234 = 54 · 22 + 46 | 46 = 1234 – 54 · 22 54 = 46 · 1 + 8 | 8 = 54 – 46 · 1 46 = 8 · 5 + 6 | 6 = 46 – 8 · 5 8 = 6 ·1 + 2 | 2 = 8 – 6 · 1 Обратные подстановки или проход вверх начинаются от записи равенства в нижней строке правого столбца таблицы: 2 = 8 – 6 · 1. Далее вместо цифры 6 подставляется ее значение из равенства строкой выше: 2 = 8 – (46 – 8 · 5) · 1 и т. д. Полная цепочка подстановок и преобразований выглядит так: 2 = 8–(46–8·5)·1 = 8–46+8·5 = 8·6–46 = (54–46)·6–46 = 54·6–46·6–46 = 54·6 – – 46·7 = 54·6–(1234–54·22) ·7 = 54·6–1234·7+54·154 = 54·160+(-7)·1234 = 8640– –8638. Из выражения перед последним знаком равенства (выделено) следует, что для нашего примера u = -7 и v = 160 в соответствии с формой записи в (1.4).

Решето́ Эратосфе́на — алгоритм нахождения всех простых чисел до некоторого целого числа n

**Лаба 4**



Сущность подстановочного шифрования состоит в том, что, исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

**два типа** - симметричные (ключ шифрования и расшифрования один и тот же) и асимметричные (ключи шифрования и расшифрования разные)

блочные (замена (подстановка), перестановка, композиционные)

поточные (синхронные, самосинхронизирующиеся)

комбинированные

Подстановочные шифры:

**моноалфавитные** (операция замены производится только над каждым одиночным символом сообщения) цезарь

**полиалфовитные** (состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования) трисемуса, виженера

**полиграммные** (одна подстановка соответствует сразу нескольким символам исходного текста)

С точки зрения криптостойкости рассматриваемый тип шифров имеет преимущества

перед моноалфавитными шифрами. Это связано с тем, что рас-пределение частот

групп букв значительно более равномерное, чем отдельных символов.

Во-вторых, для эффективного частотного анализа требуется

боль-ший размер зашифрованного текста, так как число различных групп

букв зна-чительно больше, чем мощность алфавита.

**омофонические** (маскировка реальных частот появления символа текста с помощью омофонии, омофоны - слова которые звучат одинаково но пишутся по разному и имеют разное значение)

1. В чем заключается основная идея криптографических преобразований на основе шифров замены?

В данных шифрах операция замена производится только над каждым одиночным символом сообщения Мi. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены. Максимальное количество ключей для любого шифра этого вида не превышает N!, где N – количество символов в алфавите.

**2.** Привести классификационные признаки и дать сравнительную характеристику разновидностям подстановочных шифров.

Цезарь, вижинер, трисемус

Полиалфавитные самые стойкие

Моноалф самые легкие

**3.** Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?

Для русского 33 -1, для бел 32 -1 (первая комбинация начальный алфавит)

**криптостойкость**) — способность криптографического алгоритма противостоять криптоанализу.

**Криптоанализ** — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа

4. Найти ключ шифра, с помощью которого получен шифртекст: ‘byajhvfwbjyyfzgjcktljdfntkmyjcnm’. Информационнаяпоследовательность

Можно криптоанализ, можно посмотреть вероятность выпадения каждого символа в тексте и подобрать соотв букву

5. Расшифровать (с демонстрацией каждого шага алгоритма) текст Сi = ‘qrscqcocqclc’, зашифрованный аффинным шифром Цезаря при N =26, а = 3, b = 5.

0 ≤ a, b< N, наибольший общий делитель (НОД) чисел a, b равен 1, т.е. эти числа являются взаимно простыми.

6. Зашифровать и расшифровать свою фамилию (на основе кириллицы), используя аффинный шифр Цезаря.

Пусть N =26, а = 3, b = 5. Тогда, НОД (3, 26) = 1, и мы получаем следующее соответствие между индексами букв:

х 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 3х+5 5 8 11 14 17 20 23 0 3 6 9 12 15 18 21 24 1 4 7 10 13 16 19 22 25 2

Преобразуя числа в буквы английского алфавита, получаем следующее соответствие для букв открытого текста и шифртекста:

А B C D Е F G Н I J К L М N O Р Q R S T U V W Х Y Z

F I L O R U Х А D G J М Р S V Y В Е Н K N Q Т W Z C

Если Мi = ‘VENIVIDIVICI’, то получение зашифрованного сообщения в деталях показывает таблица 2.2

**7.** Можно ли использовать в качестве ключевого в шифре Виженера слово, равное по длине открытому тексту? Обосновать ответ.

По длине открытого текста - можно

ну во первых такого слова вообще может и не быть

8. По какому признаку отличить текст зашифрованный шифров Плейфера?

Полиграммный шифр, шифруется по биграммам, два символа шифруются как один, провести криптоанализ, выявить совпадение пар символов (будет около 600 комбинаций для англ алфавита)

9. Имеются ли предпочтения в выборе размеров таблицы Трисемуса для виртуального алфавита мощностью 40: 4х10? 10х4? 5х8? 8х5? 2х20? 20х2?

Квадратная форма должна быть

10. Охарактеризовать основные виды атак на шифры.

Зависит от того есть ли у нас шифро текст, есть ли открытй текст, есть ли ключ.

**Атака с выбором ключа -** Криптоаналитик задает часть ключа, а на оставшуюся часть ключа выполняет атаку на основе связанных ключей.

**Атака на основе связанных ключей -** Криптоаналитик знает не сами ключи, а некоторые различия (соотношения) между ними

**Есть атака с известным шифротекстом**- Разновидности такой атаки: • полный перебор ключей (лобовая атака, brute force attack);

• атака по словарю, перебор ключей по словарю (dictionary attack); применяется часто для взлома паролей; • частотный криптоанализ – метод взлома шифра, основывающийся на предположении о существовании зависимости между частотой появления символов алфавита в открытых сообщениях и соответствующих шифрозамен в шифрограммах

**Атака с выбором шифртекста** - имеет возможность выбрать необходимое количество шифрограмм и получить соответствующие им открытые тексты. Он также может воспользоваться устройством расшифрования один или несколько раз для получения шифртекста в расшифрованном виде. Используя полученные данные, он может попытаться восстановить секретный ключ

**Адаптивная атака с выбором шифртекста -** Криптоаналитик имеет возможность выбирать новые шифрограммы для расшифрования с учетом того, что ему известна некоторая информация из предыдущих сообщений.

**Атака с известным открытым текстом (known plaintext attack).** То же, что и предыдущая, но противник для некоторых шифрограмм получает в свое распоряжение соответствующие им открытые тексты

11. Сравнить криптостойкость шифра Цезаря и шифра Виженера.

**Виженера – т.к. там большее кол-во вариатов(тяжелее взлом), т.к. сначала нужно узнать длину ключа**

**Цезаря мы просто заменяем буквы**

**https://habr.com/ru/post/271257/**

12. Охарактеризовать основные методы взлома подстановочных шифров.

Криптоанализ – вероятности, полный пербор. Частота встречаемости

**Лаба 5**



Блочные и поточные – по способу шифрования

Самый простой шифр перестановки – написать слово в обратном порядке. Либо каждой букве присвоить числовое значение, потов переставить значение по другому порядку. Блочная перестановка – уже юзаем не 1 символ, а несколько символов. Сообщение разбиваем поблокам, по 2-3 символа, присваиваем числовое значение и меняем их порядок. Шифр **маршруной перестановки** – они будут потяжелее, в том плане что можно придумать различные варианты, как пример шифр эйлера, это прохождение коня по шахматному полю(ходит буквой Г)

Возможно еще блочные

**Классификация** – множественная и одинарная.

1.В чем заключается основная идея криптографических преобразований на основе шифров перестановки?

Сущность перестановочного шифрования состоит в том, что, исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки

2. Привести классификационные признаки и дать сравнительную характеристику разновидностям перестановочных шифров.

Шифры перестановки относятся к классу симметричных. Элементами текста могут быть отдельные символы (самый распространённый случай), пары, тройки букв и так далее

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.

шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Шифры простой блочной перестановки

3. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?

Русский - 32, бел - кол-во символов - 1

4. Охарактеризовать криптостойкость перестановочных и подстановочных шифров.

Перестановочные хуже, т.к. в перестановочных можно просто даже угадать подбором, увидеть закономерность в зашифрованном сообщении.Один и тот же алфавит

Подстановочные бы выбрал, т.к. есть полиалфавитные – несколько алфавитов(Вижинер)

Зависит от длины сообщения

5. Привести примеры дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной лабораторной работе.

Шифр с применением специальной решетки с дырками, которая накладывается на зашифрованный текст и по буквам в этих дырках читается шифрованное сообщение.

6. Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?

Да, Должна быть более менее квадратная

7. Охарактеризовать основные методы взлома перестановочных шифров.

Статистический анализ, как часто встречаются определенные символы

Перебор ключей малой длины, если маленькое сообщение

**Лаба 6**

Энигма – шифровальная машина.Состоит из роторов, рефлекторов и в военной версии еще и из коммутаторов для дополнительной защиты.

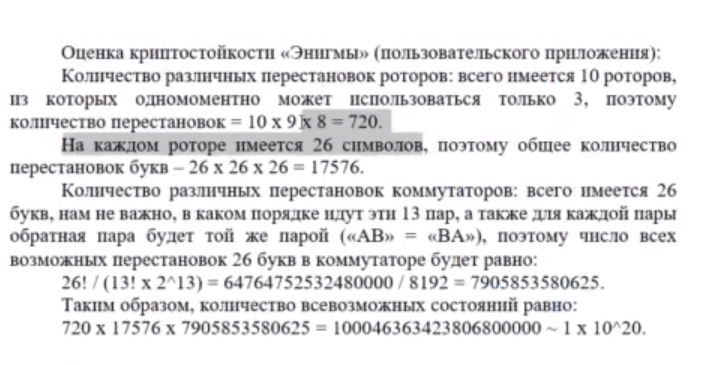
Ротор – диск, на котором содержится алфавит.

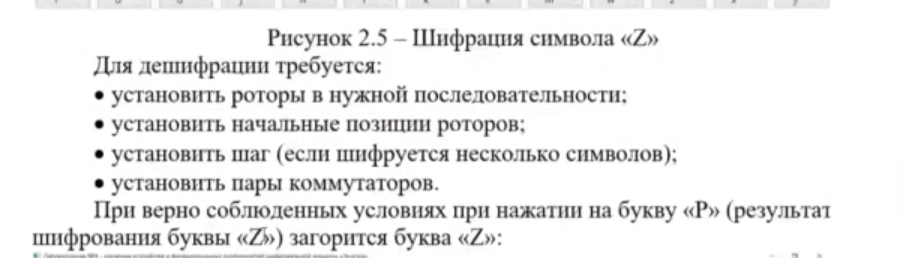
Принцип работы:

Сигнал подается с правой стороны

После каждого такого шага наш крайний правый ротор начинал двигаться, и когда он проходил целый круг, начинал двигаться другой ротор

Работает на основе Динамического шифра цезаря.





26! – наши буквы, 13! – наши пары, 2^13 – мы говорим что пары AB BA это одинаковые пары

Недостатки:

Символ не может шифроваться тем же символом

Повторение слов или частей сообщений, на основе которых можно было понять настройки машины

Чтобы расшифровать, нужно знать роторы, и их позицию, стартовую позицию, шаги и пары коммутаторов

Преимущества:

Большая криптостойкость

Если не попали по букве, то сдвиг назад вернуть нельзя, чел фактор

1. Дать пояснение к структуре шифровальных машин Энигма.

Клавиатуру, набор вращающихся дисков – роторов, – которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состояла из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

Энигма состоит из 5 основных блоков:

- панели механических клавиш, 1 (дают сигнал поворота роторных дисков);

- трех (или более) роторных дисков, 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;

- рефлектора, 3 (имеет контакты с крайним слева ротором);

- коммутационной панели, 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);

- панели в виде электрических лампочек, 5; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифровани

2. На основе каких шифров строится машина Энигма?

Как мы отмечали выше, Энигма строится на основе подстановочных шифров, подобных на шифр Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра Энигмы лежит динамический шифр Цезаря.

3. Дать пояснение к принципам зашифрования сообщений.

4. Дать характеристику криптостойкости шифровальной машины Энигма.

Если говорим про военную энигму, то у них криптостойкость выше нашей машины, т.к. у нас 13 пар роторов, а у них был 10 пар роторов и 6 свободных букв, у нас количество возможных комбинаций будет 26!/(13!\*2^13),

Зависит от кол-ва роторов, кол-во символов, кол-во пар

5. Дать характеристику (с численными оценками) криптостойкости машины-симулятора на основе разработанного приложения.

У нас есть 10 роторв, используем мы 3

6. Пояснить основные принципы расшифрования сообщений Энигмы.

Нужно поставить роторы

7. Ваши предложения по модификации известных аналогов Энигмы?

**Лаба 7**

Перестановки не влияют на криптографию. Правый блок проходит через функцию f с приминением ключа 48 бит. На выходе получаем блок в 32 бита, который xor с левым блоков 32 бита далее мы меняем эти блоки местами и так происходит 16 раз. Ключ 56 а используем по 48, т.к. ключ должен расширяться до 16 ключей по 48 бит

Фунция F – приходит блок в 32 бита, далее этот блок проходит через блок расширения, в итоге мы получаем 48 битовый блок, затем xor с ключом затем мы получаем новый блок в 48 бит, который разделяется на 8 блоков по 6 бит. Каждый подблок проходит через бокс подстановки. По итогу этот бокс получает 6 битовый блок и в мы получаем из него 4 битовый блок. Затем все складываем в новый 32 битовый блок который затем проходит через перестановку

Ключ: мы берем наш 64 битовый ключ, но суть в том, что каждый 8 бит – проверочный бит. мы не учитываем в итоге мы получаем лишь 56 бит. Так мы выделяем значащие биты. Затем мы делим на 56 битовый блок на два блока по 28 бит. Типа каждый раунд мы сдвигаем наши 28 бит на n бит влево. Затем складываем эти два блока, затем 56 битовый ключи проходит через сжимающую перестановку и получаем на выходе блок в 48 бит

010001 01=1 1000=8 10=1010  
Алгоритм блочный симметричный.  
  
Слабый ключ- состоит только из 0 и единиц.  
Полуслабый ключ - при котором разные ключи дают одинаковый результат при шифровании.  
  
Вопросы:  
2. Главным различием блочных и поточных шифров является то что в блочных шифрах для шифровании всех порций используется один и тот же ключ, а для поточных ключи разной длины  
3. Раундом называют один из последовательных шагов обработки данных в алгоритме блочного шифрования.  
4. Даже само название сети фейстеля означает что она имеет ячеистую топологию. Можно сказать что одна ячейка соответсвует одноу раунду зашифрования или расшифрования. Каждый входной блок шифруемого сообщения делится на два одинаковых по размеру это на левый и правый. Далее в каждом раунде выполняется преобразовании в соответствии с представлением ячейки Фейстеля  
5. Простейшие операции: Лежит операция xor : A+B(mod n). Помимо этой операции в ГОСТ и Blowfish предусмотрена операция сложения более по модулю 2^n  
6. Сложение по модулю 2^n увеличивает криптостойкость для блочных шифров.  
7. Лавинный эффект это понятие которое часто применяется к блочным шифрам . Это свойство которое обозначает что изменение малого количества бит во входном текста или ключе приводит к значительному изменению значений выходных битов  
12. Существует несколько алгоритмов для тройного деса.  
DES-EEE3 Шифруется 3 раза с тремя разными ключами  
DES-EDE3 операции шифрования расшифрования с различными ключами  
DES-EEE2 используется для того что бы зашифровывать только 2 ключа совпадают  
DES-EDE2 используется два одинаковых числа  
13. На стойкость блочного шифра оказывают влияние размер самого блока, размер ключа и количество раундов шифрования.  
14. Метод дифференциального криптоанализа - метод криптоанализа в блочных шифрах который основан на изучении преобразования разностей между шифруемыми значениями на разных раундах шифрования  
15. Линейный криптоанализ - называется методом криптоанализа который соотносит известные пары открытого текста и шифротекста для получения ключа.  
17. Ну тот же des используется доя зашиты финансовой информации, тройнойдес используется при обработки кредитных карт

**Лаба 8**

Поточные шифры:  
RSA  
p и q простые числа которые генерируют n  
n в совместимости с таким числом как e которое так же является простым ключом  
d генерируется при помощи е и фи называется секретным ключом.  
Пример дешифрования к нам пришли {5,3,3} . Для того что бы дешифровать мы эту 5 возводили в степень d и искали бы модуль от числа 3337 . Если бы мы шифровали то мы 199 возводили бы в степень е и искали бы по модулю 3337. Все веселье в том, что у нас есть два ключа и только при помощи закрытого ключа мы можем расшифровать текст зашифрованный при помощи открытого ключа.  
Ну как говорили люди уже сдававшие до меня у нас есть такие так называемые Боб, Алиса, Ева . Предположим что Боб хочет послать Алисе сообщение m. Алгоритм шифрования в котором мы сначала берем текст и зашифровываем его при помощи открытого ключа Алисы . Алиса принимает зашифрованное сообщение берет свой закрытый и с помощью его расшифровывает сообщение. Плюс в том что если Ева захочет преобразовать наше сообщение обратно она не сможет это сделать даже имея все открытые ключи и зашифрованное сообщение. Это плюс  
Минус что при изменении даже 1 символа в битовой последовательности все будет нарушено и мы не получим наше сообщение.  
  
Схема на практике не юзается так как при одних и тех же входных значениях мы получим один результат  
  
ПСП на основе регистров сдвига  
Есть число 84320 которое делало генератор 1...8 нулевой биты нулевой соединятся с ближайшим xor а так же бит 2 3 4 соединяются с xor. Как делается ну рассказал а как генерируется ну есть приводимы и неприводимые 84320 является приводимым так как в конце вычисления мы получаем 255 а это 256-1 равняется 255 тоесть порядок его 255 это находится 2 в степени количество все регистров минус еденица . Есть так же неприводимые 420 к примеру 420 так как его порядок 6 а два в шестой степени это куда больше чем у нас получается. Если они неприводимы то мы проверяем битовую последовательность пока не получим значение в нулевом  
  
Беру значения возле xor и последнее значение суммирую беру по модулю двойки и в зависимости от того что получилось но или еденица ставлю это на первое место а остальные биты сдвигаю вправо  
  
Алгоритм BBS  
Начальное значение x^2mod(n) где n как и в rsa считается произведением чисел p и q но в это случаем при делении чисел p и q на 4 мы должны получать остаток 3; число x должно быть взаимно простым с n;  
  
Алгоритм RC4  
Алгоритм RC4 формируется на основе ключа ну к примеру у нас формируется ключ он состоит из 6 битов понятно чти это битовая последовательность из нулей и едениц. Есть какие то 16 символов от 0 до 15 в этом случае для них генериуется ключ так как он по 6 битов тоесть каждые 6 битов вставляются и формируется таблица и проходим весь алгоритм который представлен ниже  
  
Ответы на вопросы:  
  
1. Особенность потоковых шифров в том что мы букву бит сообщение шифруем по отдельности  
2. Шифры делятся на синхронные и асинхронные. В синхронных ключ никак не зависит от открытого текста а в асинхронных (самосинхронизирующиеся) там ключ вычисляемый. В синхронных преимуществом является то что так как у нас ключ не вычисляемый то будет меньше ошибок так как если у нас исказится бит то изменится и ключ и мы получим неверные данные. Синхронные шифры вроде подвержены атаке на отдельные биты шифротекста  
3. Он должен обладать свойством что на основании каких то элементов этой последовательности мы не можем вычислить абсолютно все что нам нужно ведь это должны быть какие то случайные числа быть.  
4. Часто реализуемые алгоритмы псп реализуются на основе конгруэнтного генератора. Генераторы не используются для криптографии так как у их низкая криптостойкость и но они используются при моделировании

**Лаба 9**

Для генерации двух ключей: тайного и открытого используются два больших случайных простых числа, p и q. Для максимальной большей криптостойкости нужно выбирать p и q равной длины. Рассчитывается произведение: n = pq. Этой есть один из трех компонент ключа, состоящего из чисел n, e, d. Затем случайным образом выбирается второй компонент ключа(открытый ключ или ключ зашифрования, e, такой что e и (p-1)(q-1) являются взаимно простыми числами; вспомним, что (p-1)(q-1) = φ(n) – функция Эйлера.

d -1 = e(mod φ(n)).

Шифрование - ci = (mi)^e mod n

Расшифрование - mi = (ci)^d mod n

**Эль-гамаль**

Генерация ключевой информации. Выбирается простое число, р. Выбирается число (g, g < p), являющееся первообразным корнем числа р – очень важный элемент с точки зрения безопасности алгоритма (см. ниже). Далее выбирается число х (х < p) и вычисляется последний компонент ключевой информации: y =g х mod р.

Владельцу сформированной ключевой информации, состоящей из 4 чисел, может посылаться некоторый шифртекст, созданный с использованием открытого ключа получателя: p, g, y. Расшифрование шифртекста получатель производит своим тайным ключом: p, g, х.

Блок шифртекста (ci) состоит из двух чисел: аi и bi: ai = g k mod p, (8.7) bi = (y k \*mi) mod p.

8 – можно

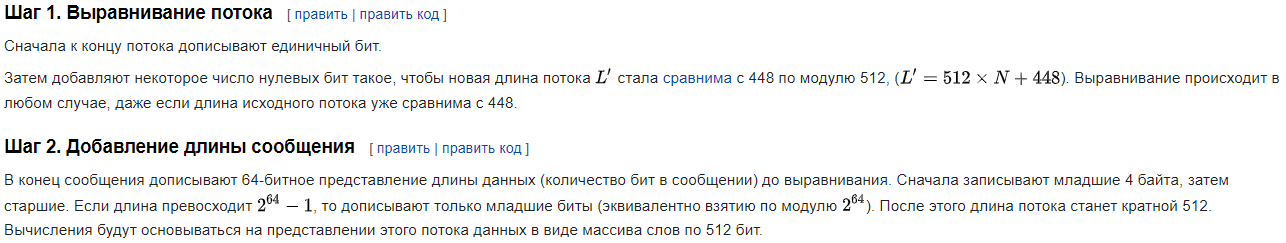
9- 

**Лаба 10**

2 – на выблре p q, чем более большие числа, тем больше криптостойксоть

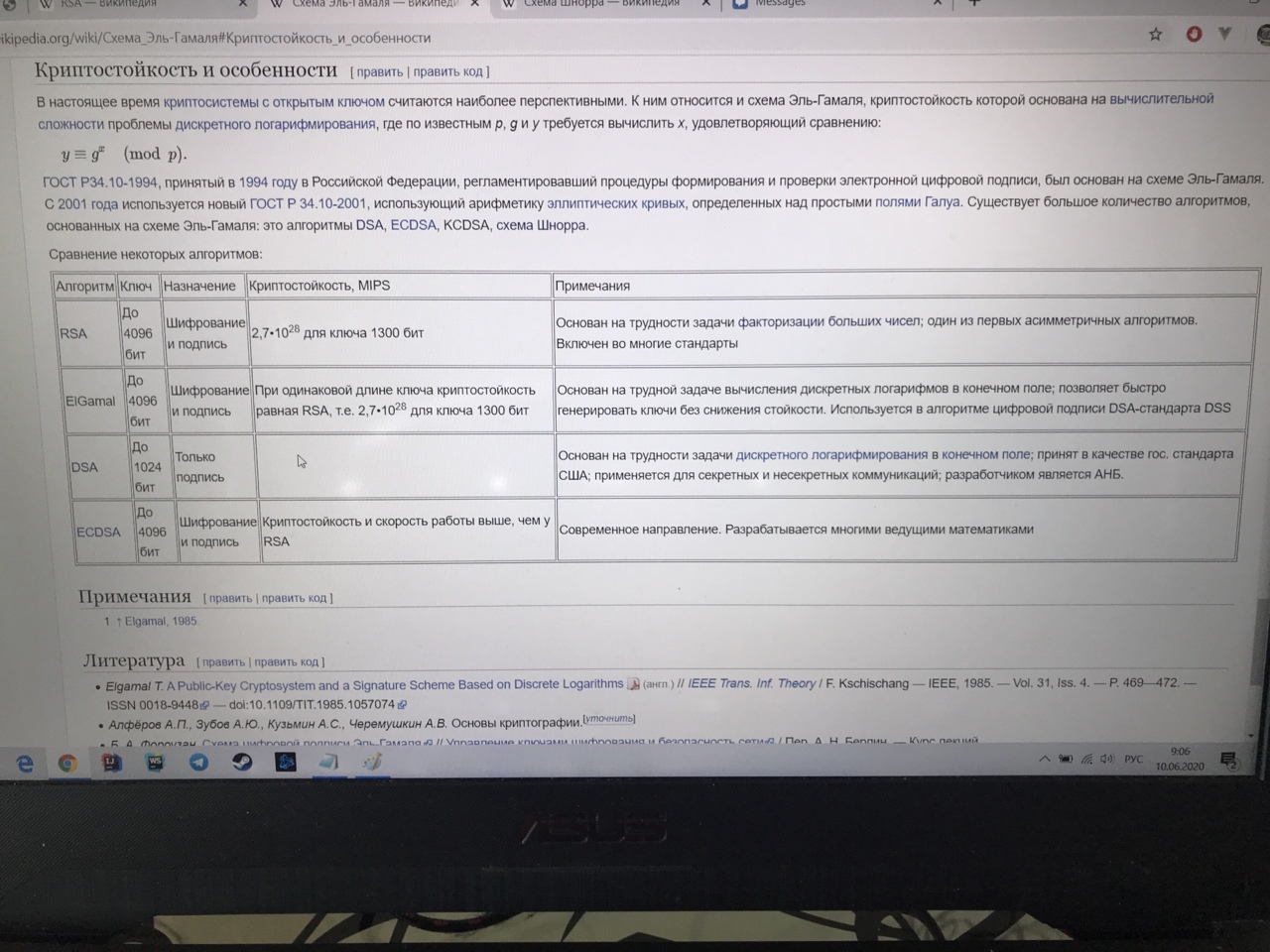
3- Первообразным корнем по модулю n (primitive root modulo n) называется такое число g, что все его степени по модулю n пробегают по всем числам, взаимно простым с n

**Лаба 11**



Хэширование:  
1)Хеш-функция - преобразует последовательность символов произвольной длины в последовательность символов определенной длины.  
2)Однонаправленность хеш-функций - это то что у нас значения могу хэшироваться только в одну сторону.  
3) Коллизии - это когда могут встречаться одинаковый наборы хэшей при разных наборах символов.  
Коллизии первого рода: подразумевает, что для заданного сообщения M должно быть практически невозможно подобрать другое сообщение N, для которого хэш сообщения M равен хэшу сообщения N.  
Коллизии второго рода это когда возможно подобрать пару сообщений(M,M') которые имеют одинаковые хэши.  
4)Парадокс дней рождения используется для рассмотрения вероятности возникновения коллизий.  
Сам парадокс гласит что есть группа из 23 человек вероятность совпадения дней рождения хотя бы у двух 50%..  
7)Базовые алгоритмы семейств SHA и MD производят хэширование в несколько стадий:  
-расширение входного сообщения  
-разбивка расширенного сообщения на блоки  
-инициализация начальных констант  
-обработка сообщения поблочно (основная процедура хеширования)  
-вывод результата  
В алгоритмах MD входные сообщения преобразуются в хэш длиной 128 бит, кроме MD6 там от 1 до 512 а в алгоритмах SHA входные сообщения преобразуются в хэш длиной 160 бит  
  
РАЗЛИЧИЯ. Ну для различий можно смотреть MD5 и SHA-1 так как они оба произошли от MD4. У MD5 будет выше скорость выполнения но у его 128 битный выход , а алгоритм SHA1 имеет 160 битный выход но выполняется дольше. SHA-1 лучшем чем MD5 потому что ниже вероятность появления коллизий.  
11) Лавинный эффект говорит о том, что если изменить даже один символ во входном сообщении это сильно изменит конечный хэш.  
12)Алгоритм SHA-3 построен по принципу криптографической губки. Криптографическая губка - это класс алгоритмов с конечным внутренним состоянием, на вход которых поступает двоичная строка произвольной длины, и которые возвращают двоичнующ строку произвольной длины.  
  
Типы хеш-функций:  
1)Специализрованные,  
2)На основе блочных шифров,  
3)На основе модулярной арифметики  
  
Свойства хэш функций:  
1)Детерминированность: независимо от того, сколько раз вычисляется хэш при использовании одинакового алгоритма, код хэш- преобразования всегда остается одинаковым.  
2)Скорость вычисления: если сам процесс вычисления не достаточно быстрый то система не является эффективной.  
3)Односторонние преобразования: что преобразование у нас идет только в одну сторону  
  
Применение хэш функций:  
1)Хранение паролей  
2)Защиты файлов  
3)Проверка целостности данных

**Лаба 12**

Электронно цифровая подпись  
RSA:  
Алиса которая создает цифровую подпись  
1)Берется открытый текст  
2)Создаем секретную подпись s с помощью секретного ключа{d,n} s= Sa(m)=m^d\*mod(n)  
3)Передаем пару {m,s} состоящую из клиента и подписи  
Боб который проверяет подлинность подписи  
1)Принимает пару {m,s}  
2)Берем открытый ключ {e,n} Алисы  
3)Вычислияем прообраз сообщения подписи m'=Pa(s)=s^e\*mod(n)  
4)Проверяем подлинность сообщения сравнивая m' и m  
  
Эль-Гамаль:  
Создание  
1)Вычисляем дайджест(хеш-сумму) сообщения M: m = h(M)  
2)Выбираем случайно число k такое, что 1 < k < p-1 и оно взаимнопростое с p-1  
вычисляем r = g^kmod(p)  
3)Вычисляем число s = (m-xr)k^-1 (mod p-1)  
4)Подписью сообщения M является пара (r,s)  
Проверка  
Имея открытый ключ (p,g,y) подпись (r,s) сообщения M проверяется следующим алгоритмом  
1) Проверка условий 0 < r < p и 0 < s < p-1  
2) Если хотя бы одно из условий не выполнилось то подпись не верна  
3)Вычисляем дайджест m = h(M)  
4)Если выполняетсяя y^r\*r^s = g^m(modp) то подпись верна  
  
Шнорр:  
Есть p-простое число от 512 до 1024; q - 160 битное простое число;  
Создание  
1)Вычисляем g^q = 1mod(p)  
2)Выбираем число (закрытый ключ) x < q и вычисляем последний элемент открытого ключа  
y = g^(-x)mod(p)  
3)Для подписи используем случайное число k (1<k<q) и вычисляем a  
a = g^k mod(p)  
4)Вычисляем хэш от канкатенации сообщения M и числа a : h= H(M0||a)  
5)Вычисляем b = (k+xh)mod(q). Отправляем получателю M' = M0||S; S ={h,b}  
Проверка  
1)Вычисялем X = g^b\*y^h(mod p)  
2)Проверяем равенство h = H(Мп||X)  
  
Вопросы:  
1) ЭЦП – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом  
электронного документа, зависящая от содержания этого документа и предназначенная для  
подтверждения целостности и подлинности электронного документа.  
2)Основыне функции ЭЦП:  
Доказать авторство того кто подписал сообщение  
Контролировать целостность сообщения  
Защита сообщения от подделок  
3)Сходства и различия собственноручной и электронной подписи  
Сходством является то, что он оба выполняют одни и те же функции.  
Отличием является, что представляет из себя бинарную последовательность.  
4)Основные способы реализации ЭЦП.  
На основе симметричных систем(с тайным ключом).(Не отличим от DES)  
На основе симметричных систем и посредника.(Создаются 2 симметричные системы в которых  
посредни выдает отправителю и получателю различные тайные ключи.)  
На основе ассиметричных систем(с открытым ключом).(Шифруется текст закрытым ключом и расширфуется  
открытым).  
6) 

**Лаба 13**

**Лаба 14**

Стеганография

Стеганографическая система (stegosystem, стегосистема или стеганосистема – в русскоязычной тематической литературе используются оба сокращения) – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.  
Метод НЗБ:  
Смотрите например мы хотим отправить 10101010 какой то наш байт у нас есть текст, музыка, виде или картинка. Чаще всего используется картинка. Сама картинка состоит из большого кол-ва символов и каждый пиксель это 3 канала RGB. Наименьший значимый бит это самый последний самый правый бит. И мы во всех пикселях всех 3 каналов обнуляем наш последний бит т.е. подготавливаем контейнер, а потом берем наше сообщение в двоичной системе и побитово записываем .  
Первые три бита в первый пиксель. Тоесть 1 бит в канал r, 2 бит в канал g и третий бит в канал b. Потом берем следующие три бита и записываем их во второй пиксель и так далее. На глаз картинка может не изменяться.