**9 – ХЕШ ФУНКЦИИ**

**Хэширование** – преобр. вх. массива данных опр. типа произв. длины в вых. бит. строку фикс. длины: *XOR (длина всегда 8 бит)***Хэш-функция** – мат. ф, h=H(M), приним. на входе строку символов М (прообраз) перем. длины n, и преобраз. ее в вых. строку фикс. длины *l* (*хэш, дайджест, хэш-таблица*)  
1) бесключевые – завис. т. от сообщения 2) с секр. ключом**Криптогр. хэш-функция** – спец. класс хеш-ф-й, имеет разл. св-ва для решения крипт. задач:  
***Задачи:*** для аутент (хран. паролей), проверка целостности д-х, защита файлов, обнаруж. зловред. ПО, криптовалют. технологии

**Свойства хэш-функций:**\* детерминированность (неважно ск. раз вычисл H(M), M – const, один. алг == один h)  
\* дб быстрым  
\* односторонность преобразования  
\* мин. изменения в M≠M’ изм. в H(M) ≠H(M’) -->иначе **Коллизия хэш-функции**\* коллизионная устойчивость: зная M, трудно найти M’, чтобы H(M)=H(M’) – иначе I рода  
 если случайно выбраны два сообщ (M, M’) для кот. мы узнаем хешH(M)=H(M’), II рода  
**Типы хэш-ф-й:**  
\* специализированные (md2, md4, md5, sha…)  
\* на основе блоч. шифров (mdc-2, mdc-4)  
\* на основе модуляр. арифметики

**Хэш-функции на основе блочных шифров:**блоч. шифр необратим по ключу шифрования, и если исп. в ка-че ключа выход пред. шага, а в кач-ве Mi очередной блок сообщ, м. получить хорошую хэш-ф. (ГОСТ)  
НО: низкая производительность

**Мера криптостойкости** – вычислительная сложность нахождения коллизии, средство поиска коллизий – «парадокс дня рождения»

**Парадокс «дней рождений»:  
*Постулат:*** *в группе из 23+ чел с вероятность 0,5+др у двух одинаковое (нет близнецов, люди рожд. независимо, равномерно, случайно)*P(An) – вер, что в группе из n чел нет один. др  
P(An) = P(An-1) \* (m-(n-1)) / m

**Атака:  
m** – кол-во дней, **M** – мн-во людей группы, **n** – кол-во людей, люди хэшируются в их др (одно из m)  
стоит задача отыскание наим. n, при к-м хеши двух значений m будут «одним др»:  
n = (2m\* ln 100)1/2

**Особенности хэш-функций:  
MD** – Message Digest – 6 не стандартиз, преобр. вх. сообщ. [max 263] в хеш [128], в MD6 хеш[1-512]  
**SHA** – Secure Hash Algorithm – max длина сообщ как в MD, но длина хешей разная  
**ГОСТ** – России   
**SHA3** – исп. «*криптогр. губку*» - итерат. подход с произв. длиной на входе и выходе на осн. преобразования (в РБ)

 **Алгоритмы MD и SHA:**  
\* расшир вх. сообщ длиной L (итог. длина L’ кратна 512, в незаполн. 64 бита запис. двоич. L)  
 1 бит доб. к сообщ, затем доб. биты 0 … в конце длина L  
\* разбивка расшир. сообщ на блоки   
\* иниц. нач. констант  
\* обработка сообщения поблочно  
\* вывод рез.

**SHA-256:** Исходное сообщение после дополнения разбивается на блоки, каждый блок — на 16 слов.   
Алгоритм пропускает каждый блок сообщения через цикл с 64 итерациями.   
На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова.   
Результаты обработки каждого блока складываются, сумма является значением хеш-функции.   
Так как инициализация внутреннего состояния производится результатом обработки предыдущего блока, то нет возможности обрабатывать блоки параллельно.

**10 – ЭЦП**

**ЭЦП** – контрольная хар-ка сообщения, кот. вырабат. с исп. личного ключа, провер. с пом. откр. ключа, служит для контроля цел-сти и подлинности сообщения и обесп. невомзожность отказа от авторства **ЭЦП** – бинарная посл-сть символов, явл. реквизитом эл. дока, зависит от его содержания и предн. для подтверждения цел-сти и подлинности эл. дока

**Функции ЭЦП:**  
\* аутент. лицо, подписавшее собщ  
\* контрол. целостности  
\* защищать от подделок  
\* доказать авторство (если отриц)

**Виды ЭЦП:**  
\* *на основе симм. ключей* (с тайным ключом) – как DES  
\* *на основе симм. систем и посредника* – две симм. с-мы: отпр-посред + посред-получ (посредник выдает обоим разный тайный ключ)  
\* *на основе асимм. систем* (с откр. ключом) – эцп как отд. элмента отсутствует, исп. ключевая инфа отправителя: откр. ключ – для зашифр, тайный – для расшифр

**ЭЦП на основе хэшей подписываемых сообщений:  
Генерация ЭЦП:   
отправитель:**\* вычисляет хэш сообщ М - H(M)  
\* вычисляет содержание ЭЦП, S по хешу H(M) с исп. закр.ключа d: S = Cd(H(M))  
\* конкатен ЭЦП + М + нек. служебная инфа (дата, t отпр…) == M’  
\* посыл. M’ получателю  
**получатель:**  
\* отдел S от М  
\* примен к М хеширование (та же ф-я)  
\* исп. откр. ключ отправителя, расшифр S (извлек из ЭЦП хеш-образ отправленного сообщ)  
 => ЭЦП м. проверить каждый, у кого есть *откр. ключ* автора  
\* провер. соответствие (=) обоих хэшов

**ЭЦП на основе RSA:**1) **генерация ключей:** Вычисл. простые p и q. Вычислить n=p\*q. Выбрать случайное е, такое, что:   
(e(p-1)(q-1))=1. Найти с пом. алг Евклида d такое, что: ed=1 mod (p-1)(q-1)  
2) Вычислить ЭЦП: sign=hd mod n, где d - закрытый ключ, h=H(M) - хеш сообщений  
3) Откр. ключ (e,n) и письмо с ЭЦП(m, sign) шлются получателю  
4) Тот вычисляет свой хеш h = signe mod n  
5) Если этот хеш совпал с полученным, то ЭЦП верна

**ЭЦП на основе DSA:** (Digital Signature Algorithm)DSA– алг. цифр. подписи  
1) Выбрать случ. х (закр ключ). y=gX mod p (откр ключ). Выбрать q>x – простой множитель (p-1)  
\* g = v(p-1)/g mod p > 1, v – любое число (1, p-1]  
2) Формирование подписи: выбрать случайное k<q, вычислить r = (gK mod p) mod q,  
s=((h+xr)/k) mod q  
3) Откр. параметры (p,q,v), откр ключ y, письмо с ЭЦП (m,r,s) отпр. получателю  
4) тот вычисл: w=s-1mod q, u1 = (H(m)\*w)mod q, u2 = (rw)mod q, a=((gu1 \*qu2)mod p)mod q  
5) Если a=r, то ЭЦП верна

**ЭЦП Эль Гамаля:  
Генерация ключ. инфы (p,g,x\*,y):**\* выбир простое p  
\* выбир g<p – первообразный корень числа p  
\* выбир х<p  
\* вычисл. y, y = gXmod p

**Зашифр:** результат – т. одна пара чисел! (не пара для к. блока)  
 это сообщение – хеш подпис. дока  
 \* выбрать k , вз-простое с (p-1)  
 S = {a, b}  
 \* a = gk mod p  
 \* b = k-1 (H(M0) – xa) mod (p-1)  
 получателю отправляют M’ = Mo||S  
**Верификация:** H(Mп) = h – вычисл. хеш полученного сообщ.  
 провер ya \* ab = gh (mod p)

**ЭЦП Шнорра: (РБ)**как Эль-Гамаль, но число p м. взять поменьше  
**Генерация ключевой инфы: (p, g, q, x\*, y)**\* p – простое число [512-1024 бит]  
\* q – простое число [160]  
\* p-1 – делитель  
\* g≠1 – любое число – gq = 1 mod p  
\* x – число <q (закр. ключ) [160+]  
\* y = g–X mod p  
**Подпись сообщения:**  
\* k – случ. число [1, q]  
\* a = gk mod p  
\* h = H(Mo || a) – созд. хеш-образ сообщ-я  
\* b = (k + xh) mod q  
\* отпр. M ’ = Mo||S, S={h,b}  
**Проверка подписи:**  
\* X = gb yh (mod p)  
\* провер рав-во h = H(Mп||X)

**Вопросы для контроля:**

1. Дать определение ЭЦП.   
**ЭЦП** – контрольная хар-ка сообщения, кот. вырабат. с исп. личного ключа, провер. с пом. откр. ключа, служит для контроля цел-сти и подлинности сообщения и обесп. невомзожность отказа от авторства **ЭЦП** – бинарная посл-сть символов, явл. реквизитом эл. дока, зависит от его содержания и предн. для подтверждения цел-сти и подлинности эл. дока

2. Охарактеризовать основные функции ЭЦП.   
\* аутент. лицо, подписавшее собщ  
\* контрол. целостности  
\* защищать от подделок  
\* доказать авторство (если отриц)

3. В чем заключаются сходства и различия между собственноручной и электронной подписью.   
ЭЦП – бин. послед  
рукой – графический образ

4. Охарактеризовать основные способы реализации ЭЦП.   
\* *на основе симм. ключей* (с тайным ключом) – как DES (один ключ для заш и расш)  
\* *на основе симм. систем и посредника* – две симм. с-мы: отпр-посред + посред-получ (посредник выдает обоим разный тайный ключ)  
\* *на основе асимм. систем* (с откр. ключом - RSA) – эцп как отд. элмента отсутствует, исп. ключевая инфа отправителя: откр. ключ – для зашифр, тайный – для расшифр

5. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?  
\* сообщ Мо подпис. и передается в откр. виде: S = (H(Mo))d0 mod no  
\* сообщ Мо подпис. и передается в зашифр.: анал., но do,no – эл-ты тайного ключа отпр-ля,  
 перед. сообщ M’=Mo||S  
 *расшифр*: H(Mo) = (S)eo mod no, потом сравн с H(Mп)

6. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы ЭльГамаля, схемы Шнорра, а также на основе DSA.   
rsa – много времеин тратится на модульную арифметику

**11 – ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ**

**ЭК над действительными числами:  
Эллипт. кривые** – матем. объект, кот. мб определен над любым полем  
**Эллипт. кривая** **над вещ. числами** – мн-во точек, описываемых *уравнением Вейерштрасса*:   
y2 = x3 + ax + b, при этом константы (a b – вещ. числа) д. удовл: 4a3 + 27b2 ≠ 0 (искл. особые кривые или с особыми точками)

Частью ЭК явл. **бесконечно удаленная точка** (идеальная) – О   
**Группа** – непустое мн-во, элем. к-го явл. точками ЭК и облад. **свойствами**:  
\* единичный элем. – бесконечно удаленная точка О  
\* обр. величина точки R – точка, симметр. относ Ох  
\* сложение: сумма трех P, Q, -R точек ≠ 0, леж. на одной прямой равна P + Q + (-R) = О

**Законы сложения точек ЭК:**\* прямая, проход. через R и –R, явл. вертикальной прямой, кот. не пересекает ЭК ни в какой третьей точке. Если R=(x, -y), то R+(-R) = R+(x,y) = O  
\* P + Q + R: пусть P, Q – две разные точки ЭК, если провести ч/них прямую, она пересечет ЭК в –R, кот. отображ. относительно Ох в точку R, равную сумме точек P + Q  
\* Если P=Q, то *удвоение точки*: P+P=2P ==> принцип умножения точки Р на ц.ч. n – опред. как сумма n точек Р: nP = P+P…+P

**Рациональные числа** x и y – к. точка на плоскости задается парой коорд x,y

Пусть ЭК задается уравнением с параметрами а = 2, b = -5  
4a3+27b2 = ≠ 0  
P + Q = R  
P(x1,y1), Q(x2, y2), R(x3,y3)  
λ = ( у2 – у1)/( х2 – х1) P≠Q  
λ= (3(х1) 2+а)/2 у1 P=Q  
x3= λ 2 – х1 – х2  
у3= λ (х1–х3 ) – у1

λ - **угловой коэф. секущей**, провед. через точки P, Q, при P=Q секущая превращ. в касательную  
**Задача логарифмирования** – для заданный n и P сущ. алгоритмы вычисления Q=nP. Если же известны Q и P, а нам надо определить n

**ЭК над конечными полями:  
Конечное поле** – GF(p) мн-во конеч. числа элементов: мн-во ц.ч. по модулю p (простое число)  
**ЭК над полем Fp** – Ep(a,b) те же уравн, что ЭК над вещ. числами, но mod p  
O – бескон . удаленная точка, a b – вещ. числа

1) пусть ЭК задается E13(6,-9). Проверяем 4a3 + 27b2 (mod p) ≠ 0. Исходя из этого координаты точек дб ограничены квадратом нек. чисел mod 13 (y2)  
02 mod 13 = 0…  
252 mod 13 = 1  
числа справа – **квадратичные вычеты** по модулю 13  
Подставим 0: y2 = x3 + ax + b = 03 + 6\*0 – 9 (mod 13) = 4  
т.е. y=+-2, смотрим на табл вычетов (строки с 4 справа), опред. точки ЭК: (0,2). (0,11)  
соответствий нет – на ЭК нет точек с заданным х

То, что раньше было непрерывной кривой, теперь стало мн-вом отд. точек на плоскости ХУ, координаты к-х (x,y) – цел. числа  
Три точки нах. на 1 прямой, если сущ. прямая, соедин. их

**Умножение zP** – треб. точку P сложить саму с собой z раз (z в двоич виде). Дальше вычилс. необх. составляющие общей суммы на основе весовых (единич) разрядов двоич. числа z:  
Пусть z = 171. Это число в двоичном виде выглядит так: 10101011. В соответствии с весом «1» мы должны сложить следующие составляющие (слагаемые) общей суммы: 171P = Р + 2Р + 8Р + 32Р + 128Р

**Циклич. подгруппа** – мн-во кратных Р значений: если мы склад. два значения кратных Р, то получаем значение кратное Р  
**Порядок группы точек ЭК** – равен числу различ. точек ЭК, включая точку О  
**Генератор (баз.т.) подгруппы** – точка Р, ее порядок – это делитель порядка исх. группы (если ЭК содержит m точек, а одна из подгрупп сод. q, то q явл. делителем m):  
 p + 1 – 2(p)½ ≤ m ≤ p + 1 + 2(p)½

**Задача дискр. логарифм. для ЭК:**вычисл. d, если знаем P и Q для Q=dP  
тайный ключ – случ. ц.ч. d из мн-ва {1,2…q-1}, q – порядок подгруппы, откр ключ – точка Q=dG, G – баз. точка подгруппы  
**Криптостойкость:**  
опр. параметром L, наз. уровнем стойкости, приним. значения из {128, 192, 256}, при этом для взлома ключа надо выполнить 2L операций

**Генерация ключ. инфы:**1) входные парам l,p: 2 2l-1 < р < 2 2l , р = 3 mod 4, 0 < a < p  
2) выбир. b: 0<b<p => задана ЭК: Ep(a,b)  
3) выбир порядок q (прост.ч) и точка G, кот. задается 2 координатами, напр. G = (0,yG)  
4) случ. число [64] – вспомог. параметр (s, seed)

5) вх. парам: p, a, b, q, G  
6) генер. тайный ключ d из мн-ва {1,2…q-1}  
7) вычисл откр. ключ точка Q = dG

**Использ. в криптографии:**  
обычно исп. на этапе генерации или согласования ключ. инфы:  
\* в алг согласования (передача) ключ. инфы (на основе ДХ)  
\* в алг асимм. шифр/дешифр сообщений  
\* в алг генерации/верификации ЭЦП

**Диффи-Хеллман на основе ЭК:**  
Пусть Ep – ЭК над Fp, а Q – заранее опред. сторонами А, В точка на Е. Отправитель А выбир. тайное случ. число kA, вычисл точку Pв=kв\*Q и отправ ее получателю В. В тоже случайно выбир kв, вычисл случ kA, вычисл точку P=kA\*kв\*Q (общий ключ) и отправ результ А. А вычисл Р путем умножения Pв (получ от В) на его секретное число kA. В тоже самое

**Реализация заш/расш на основе ЭК:  
Эль-Гамаль**: сообщ представл в виде точки Р на ЭК с известной точкой G и известным Q. Шифротекст – это две точки на этой же ЭК: C1 и C2. Сторона А выбир. случ k и вычисляет с исп. откр ключа стороны В: C1=kG, C2=P+kQ. Получатель шифра вычисл: P=C2–dC1 (сложение с инверсией, (x,y) --> (x,-y)

**Реализация ЭЦП на основе ЭК:**Генерация ключей как в прошлом примере. Ключ инфа отправителя (А).  
гаем, что отправитель подписывает хеш Н(М) сообщения М.  
Генерация ЭЦП.  
1. Выбрать число k (1 < k < q), q – порядок точки G.  
2. Вычислить точку kG = (х, у), вычислить r = x mod q; при r = 0 изменить k и повторить шаг 2.  
3. Вычислить t = k -1mod q (например, на основе расш. Евклида).  
4. Вычислить s = (t \*H(M) + dr)) mod q; при s = 0 изменить k и повторить алгоритм.  
Стороне В отсылаются сообщение М и ЭЦП (числа r и s).  
Верификация ЭЦП.  
Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя:  
1. Проверить выполнение условия: 1 < r, s < q; если условие не выполняется, то легитимность подписи не подтверждается, иначе идем дальше.  
2. Вычисляются Н(М) и w = s –1 mod q.  
3. Вычисляются u1 = w Н(М) (mod q), u2 = wr (mod q).  
4. Вычисляются Gu1 + Qu2 = (x', y'), v = x' mod q.  
5. Если v = r, подтверждается легитимность подписи и целостность полученного сообщения