*1 задание*

**RSA:**

(младшие 24 бита SHA1-хеша фамилии Khramykh = **977b13 (16) = 9 927 443 (10)**)

P = 10009, q = 10993

N = p\*q = 110028937‬

Ф(n) = (p-1)(q-1) = 10008 \* 10992 = 110007936‬

E = 2227 (e < Ф(n) && e – вз. Просты с Ф(n))

Вычисляем D: e\*d = 1 mod Ф(n) => d – обратное по модулю => d = 8348155

Открытый ключ – (e, n) = (2227, 110028937)

Закрытый ключ – (8348155, 110028937)

S = 9927443^2227 mod 110028937 = 38721340‬

Проверяем на клиенте:

R = 38721340^8348155 mod 110028937 = 9927443

Как видно из вышенаписанного, числа у нас совпали, поэтому верификация подписи прошла успешно.

**Эль-Гамаля:**

**M = 9927443**

p = 27; x = 13, g = 5;

y = g^x mod p = 23;

берём доп ключ k = 7. К должен быть вз. простым с p-1

Шифруем:

a = g^k mod p = 5^7 mod 27 = 14

b = (y^k \* m) mod p = (5^7\*9927443) mod 27 = 10

S = (a,b) = (14, 10)

Сравнение значений:

m = g^m mod p = 5^9927443 mod 27 = 26

(23^14 \* 14^19) mod 27 = 11592836324538749809 \* 5976303958948914397184 mod 27 = 26

так как 26 = 26, то подпись верифицирована.

**Шнорра:**

**M = 9927443**

Пусть p= 3163,q=103;

g^q = 1 mod 3163;

g = 2426;

Пусть x =23;

Для возведения g-x надо найти обратное число к g по модулю 3163;

g-1 = 2977;

y = 2977^23mod 3163= 412;

Пусть k=146, тогда

a = 9927443 mod 3163= 1949;

Конкатенацией будет 99874431949

b = (146 + 23 x 99274431949) mod 103

b = 59

Подпись S={99874431949, 59}

Далее проверяем подпись для этого вычисляем

X = 2977^59 x 412^99874431949 mod 3163= 1949;

Конкатенацией будет 99874431949

Так как 99874431949 = 99874431949 следовательно подпись верифицирована.

*2. Каждый (самостоятельно!!!) выполняет (по образцу примеров 1 и 2 из приложенных материалов к лабораторной работе 11) по 3 задачи (вручную) на сложение точек ЭК. ЭК и точки выбрать самостоятельно.*

Поскольку задание носит трафаретный характер, будет обращаться серьезное внимание (при оценке) на обоснование и последовательность выполняемых операций.

Пусть ЭК задается уравнением с параметрами а = –3, b = 6.

Пусть x = 1 для точки P.

y2 = 1 - 3 + 6 = 4;

y = 2;

Пусть x = -2 для точки Q.

y2 = -8 + 6 + 6 = 4;

y = 2;

Точки Р (1, 2) и Q ( –2, 2).

λ = (2 – 2)/(1 + 2) = 0,

xR = x3 = 02 – 1 + 2 = 1,

yR = y3 = 0x(1 – 1) – 2 = –2.

P+Q=R(1, –2);

Пусть ЭК задается уравнением с параметрами а = –17, b = 24.

Пусть x = 5 для точки P и Q.

y2 = 125 – 85 + 24 = 64;

y = 8;

Точки Р (5, 8) и Q (5, 8).

λ = (3x 52 – 17)/(2 x 8) = 3,625.

xR = x3 = 3,6252 – 5 – 5 = 3,140625.

yR = y3 = 3,625x(5 – 3,140625) – 8 = –1.259766.

P+Q=R=2P(3,140625, -1.259766).

Пусть ЭК задается уравнением с параметрами а = 12, b = 9.

Пусть x = 0 для точки P.

y2 = 9;

y = 3;

Пусть x = 4 для точки Q.

y2 = 64 + 48 + 9 = 121;

y = 11;

Точки Р (0, 3) и Q ( 4, 11).

λ = (11 – 3)/(4 – 0) = 2,

xR = x3 = 22 – 0 – 4 = 0,

yR = y3 = 2x(0 – 0) – 3 = –3.

P+Q=R(0, –3)