1. Используя методы RSA, Эль-Гамаля и Шнорра, сгенерировать ключевую информацию, используя которую вычислить значение ЭЦП для сообщения, состоящего из 24 младших бит хеша (использовать алгоритм SHA1) собственной фамилии (хеш представить десятичным числом) и выполнить процедуру верификации подписи.

Чистякова – 24 младших бита в SHA1 –84716 --> 2119 10  
H(M) = 13150279

**RSA:  
Генерация ключевой информации RSA:**1) Генерируем два простых числа: p = 5639, q = 5897  
2) вычислим n = pq = 33253183  
3) выберем число e, взаимно-простое с функцией Эйлера:  
 ф(n) = (p-1)(q-1) = 33241648   
 e = 7283  
 пара {e,n} – откр. ключ  
4) вычислим число d:   
 ed = 1 (mod ф(n))  
 d-1 = e (mod ф(n))   
 d = 29959931  
 пара {d,n} – закр. ключ

**Значение ЭЦП:**S = H(M)e mod n  
S = 21197283 mod 33253183= 8624015

**Процедура верификации подписи:**H(M) **=** Sd mod n  
H(M) = 8624015 29959931 mod 33253183= 2119  
все верно!

**Эль-Гамаля:  
Генерация ключевой информации:**Пусть p=2137  
g =2127 – первообразный корень по модулю p (g<p)  
x = 1116 – закр. ключ (случ. число [1, p-1])  
y = gX mod p = 21271116 mod 2137 = 603  
k = 7 – случ. число [1, p-1]  
a = gk mod p = 1160

**Значение ЭЦП:**H(M) **=** 13150279  
H(M0) = (xa + kb) mod (p-1)  
b = k-1 (H(M0) – xa) mod (p-1)  
b = 1831 \* (2119 – 1116\*1160) mod 2136 = 2113  
S = {1160, 2113}

**Процедура верификации подписи:**(ya \* ab ) mod p = (6031160 \* 1160 2113) mod 2137 = 1288  
gh (mod p) = 2127 2119 mod 2137 = 1288  
все верно!  
 **Шнорр:  
Генерация ключевой информации:**1) Генерируем числа:  
 p = 4721  
 q = 59  
 x = 19 (закр. ключ)   
 пара {p,q} – откр. ключ  
2) Найдем g:  
 gq = 1 mod p = 1 mod 4721  
 g = 501  
3) Найдем g-1:  
 g\*g-1 = 1 mod p  
 501 g-1 = 1 mod 4721  
 g-1 = 4476  
4) Найдем у:  
 y = ( g-1 )X mod p  
 y = 447619 mod 4721 = 2126

**Значение ЭЦП:**   
пусть k = 45  
a = gk mod p = 50145 mod 4721 = 4342  
H = H(M)+a = 21194342 (конкатенация)  
b = (k + x\*H) mod q  
b = (45 + 19 \* 21194342) mod 59 = 20  
S = {H, b} – подпись

**Процедура верификации подписи:**X = gb \* yH mod p  
X = 50120 \* 2126 21194342 mod 4721 = 4342  
Конкатенация – 21194342  
все верно!

2. Каждый выполняет (по образцу примеров 1 и 2 из методы 11) по 3 задачи (вручную) на сложение точек ЭК. ЭК и точки выбрать самостоятельно.

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

1) Пусть ЭК задается уравнением с параметрами а = 2, b = -5  
 4a3+27b2 = 4\*8 + 27\*25 = 707 ≠ 0

Пусть x1 = -3, x2 = 6  
 у 2 = х 3 + aх + b  
y1 = (–27 – 6 – 5) 1/2 = (–38)1/2 = – 6.14  
y2 = (216 + 12 – 5) 1/2 = 2231/2 = 15

Т.о., P = (-3,-6.14), Q = (6, 15) – точки эллип. кривой

λ = ( у2 – у1)/( х2 – х1) = 21.14 / 9 = 2.35 т.к. P≠Q  
x3 = λ 2 – х1 – х2 = 2.5  
y3 = λ (х1 – х3 ) – у1 = 6.785

Т.о., P+Q = R = (2.5, 6.79)

2) Пусть ЭК задается уравнением с параметрами а = 1, b = 6  
 4a3+27b2 = 4 + 27\*9 = 247 ≠ 0

Пусть x1 = 2, x2 = 2  
 у 2 = х 3 + aх + b  
y1 = (8 + 2 + 6) 1/2 = (16)1/2 = 4  
y2 = (8 + 2 + 6) 1/2 = (16)1/2 = 4

Т.о., P = Q = (2, 4)

λ= (3(х1)2+а)/2 у1= (3\*4 + 1) / 8 = 1.625 т.к. P=Q  
x3 = λ 2 – х1 – х2 = – 1.36  
y3 = λ (х1 – х3 ) – у1 = 1.46

Т.о., P+Q = R = (–1.36, 1.46)

3) Пусть ЭК задается уравнением с параметрами а = 3, b = 5  
 4a3+27b2 = 4\*27 + 27\*4 = 216 ≠ 0

Пусть x1 = 4, x2 = 2  
 у 2 = х 3 + aх + b  
y1 = (64 +12 + 5) 1/2 = (81)1/2 = 9  
y2 = (8 + 6 + 5) 1/2 = 191/2 = 4.36

Т.о., P = (4, 9), Q = (2, 4.36)

λ = ( у2 – у1)/( х2 – х1) = –4.64 / (–2) = 2.32 т.к. P≠Q  
x3 = λ 2 – х1 – х2 = – 0.6176  
y3 = λ (х1 – х3 ) – у1 = 1.7

Т.о., P+Q = R = (– 0.62, 1.7)