9530483 مهدی علی خاصی

.1

$K = ab = 6B = 2 * 3B = 2 * (2B + B)$

$2B = B + B = (x_3,y_3) : x_1 = x_2 = 5 ; y_1 = y_2 = 9$

$s = (3x_1^2 + a)\cdot y^{-1}{}_1 = (3 \cdot 25 + 1)(2 \cdot 9)^{-1} = 76 \cdot 18^{-1} \bmod 11$

$s = 10 \cdot 8 = 80 \equiv 3 \bmod 11$

$x_3 = s^2 - x_1 - x_2 = 3^2 - 10 = -1 \equiv 10 \bmod 11$

$y_3 = s(x_1 - x_3) - y_1 = 3(5-10)-9 = -15-9 = -24 \equiv 9 \bmod 11$

$2B = (10,9)$

$3B = 2B+B = (x_3', y_3') : x_1 = 10 , x_2 = 5 , y_1 = 9 , y_2 = 9$

$s = (y_2 - y_1)(x_2 - x_1) -1 = 0 \bmod 11$

$x'_3 = 0 - x_1 - x_2 = -15 \equiv 7 \bmod 11$

$y'_3 = s(x_1 - x_3) - y_1 = -y_1 = -9 \equiv 2 \bmod 11$

$3B = (7,2)$

$6B = 2 \cdot 3B = (x''_3, y''_3) : x_1 = x_2 = 7 , y_1 = y_2 = 2$

$s = (3x^2{}_1 + a)\cdot y^{-1}{}_1 = (3 \cdot 49+1)\cdot 4^{-1} \equiv 5 \cdot 4 -1 \equiv 5 \cdot 3 = 15 \equiv 4 \bmod 11$

$x''_3 = s^2 - x_1 - x_2 = 4^2 - 14 = 16 - 14 = 2 \bmod 11$

$y''_3 = s(x_1 - x_3) - y_1 = 4(7-2)-2 = 20-2 = 18 \equiv 7 \bmod 11$

$6B = (2,7) \Rightarrow KAB = 2$

.2

a) $a = 2$ and $b = 2$ $\Rightarrow 4 * 2^3 + 27 * 2^2 = 32 + 108 = 140$
$140 = 4 \bmod 17$ $\Rightarrow 4 \mathrel{!=} 0$

b) (9, 16)

c) $17 + 1 - 2\sqrt{17} \approx 9 , 75 \le 19 \le 17 + 1 + 2\sqrt{17} \approx 26 , 25$ q.e.d.

d) In a group of size n(e.g. an elliptic curve), the order of a subgroup generated by a group element necessarily divides n. We usually choose curves so that their order n is prime; in that case, the order of a point must be either 1 (the point is the "point at infinity") or n (all other points). Thus, if n is prime, then every non-zero point is necessarily a generator for the whole curve.

.3

a. choose signature:

$s \in Z_n$

b. compute message:

$x \equiv s^e \bmod n$

c. send (x,s)

for example Oscar choose

s = 100

and send (9190, 100)

.4

a) $\alpha^x = 3^{10} \equiv 25 \bmod 31$

for (17, 5) ::

w = 17, z = 5

$t = \beta^w \cdot w^z = 6^{17} \cdot 17^5 \equiv 26 \cdot 26 \equiv 25 \bmod 31 \Rightarrow t = \alpha^x \Rightarrow$ (ok)

for (13, 5) ::

w = 13, z = 5

$t = \beta^w \cdot w^z = 6^{13} \cdot 13^5 \equiv 6 \cdot 6 \equiv 5 \bmod 31 \Rightarrow t \mathrel{!=} \alpha^x \Rightarrow$ (not ok)

b) there are p − 1, i.e. 30, different signatures for each message x.

.5

a) duo to birthday paradox => $1.2 * \sqrt{365} = 23$

b) probability of not having same birthday

$= P'(n, k) = n/n * (n - 1)/n * \ldots * (n - k + 1)/n$

=> probability of having same birthday = $1 - P' = P(n, k)$

$= 1 - \prod(1 - i / n) > 1 - \prod e^{-i/n} = 1 - e^{-\Sigma i/n}$ (i is from 1 to k – 1)

$= \mathbf{1 - e^{-k * (k - 1) / 2n}}$

c) $1.2 * \sqrt{2^n} = 1.2 * 2^{n/2}$

6.

duo to birthday paradox =>

after : $1.2 * 2^{32}$ and $1.2 * 2^{64}$ and $1.2 * 2^{80}$

the probability is greater than 0.5

after : $2 * 10^9$ and $8.4 * 10^{18}$ and $5.5 * 10^{23}$

the probability is greater than 0.1