Menezes-Vanstone EC Cryptosystem

System design

1. A and B agreed to select an elliptic curve *EC*:

   $y^2=x^3+ax+b \pmod{n}$ {p:=n};

2. They also agreed to select a point G on EC

3. A and B select integers n_A and n_B {these are private keys of *A* and *B* respectively}: $n_A<n$; and $n_B < n$;

4. Users compute $P_i := n_i G$

   { public key of *i*-th user: *i*=*A, B, C*,…}

Encryption

{Suppose A wants to send message m to B via an open channel}:

m=[m(1), m(2)];

$m(1)<n$; $m(2)<n$; {m is a integer, *not* a point on E};

Comment: m is "split" onto two parts m(1) and m(2);

5. A selects a secret key $k<n$ and computes $y_0=kG$;

{"Hint/Clue"-point on EC};

6. A computes a "Mask/Screen/Veil" $[c(1), c(2)] = kP_B$;

{ c(1), c(2) are coordinates of EC point};

7. A computes

$$y_1 = c_1 m_1 \bmod n;$$

$$y_2 = c_2 m_2 \bmod n;$$ {Masking/Hiding/Veiling of m};

8. A sends to B ciphertext four integers

y=[y(0), y(1), y(2)] via open channel.

Decryption

9. *B* computes $n_B * y(0) = [c(1), c(2)]$

10. B finds inverses of c(1) and c(2) using FISH algorithm

11. *B* computes $m_1 = y_1 c_1^{-1} \bmod n$

$$m_2 = y_2 c_2^{-1} \bmod n$$

and recovers m(1) and m(2).

Numerical Example

1. Both A and B select EC: $y^2=x^3+x+6(\text{mod}11)$;

2. Both A and B agree to select generator $G=(2,7)$;

3. B selects $n(B)=8$ and pre-computes $P(B)=(3,5)$;

4. A selects a secret number $k=6<11$;

5. A pre-computes "hint/clue" $kG=6*(2,7)=(7,9)$;

6. To hide m , A pre-computes "mask/screen/veil":

   $kP(B)=6*(3,5)=(10, 9)$; {point on EC}

7. $c(1)=10$; $c(2)=9$;

8. Let plaintext *m*=91;

9. Represent *m* as *m*=(9,1)

Remark: {if m=736817, represent it as (736,817)

{*m* is NOT a point on elliptic curve *E*};

10. *A* computes $y(1)$=(10*9)mod11=2;

$y(2)$=(9*1)mod11=9;

11. *A* sends ciphertext {(7,9); 2;9} to *B* via open channel;

12. {Decryption by *B*}: [$c(1)$, $c(2)$]=8*(7,9)=(10,9);

13. $m_1 = 2 \times 10^{-1}$ mod11=(2*10)mod11=9;

$$m_2 = 9\times 9^{-1}\text{mod11=(9*5)mod11=1.}$$

Homework:

*Example*1: Send plaintext *m*=2410=(24,10) from *A* to *B*;

*Example*2: Select *t*=9 as a secret number for *A* and show how to send a plaintext *m*=2319 from *B* to *A*.