Name- Jay Shah
Nikhil Raina

Homework #7

CSCI-462

Question-1 compute two public key and one common key for DHKM.

$p = 467$, $\alpha = 2$

1. $a = 3$, $b = 5$

Alice sends a key to bob. key is

$$A = \alpha^a \bmod p$$

$$A = 2^3 \bmod 467$$

$$A = 8 \bmod 467$$

$$A = 8$$

Bob sends a key to Alice. key is

$$B = \alpha^b \bmod p$$
$$B = 2^5 \bmod 467$$
$$B = 32 \bmod 467$$
$$B = 32$$

Alice sends 8 to Bob. Bob sends 32 to Alice.

$$K = \alpha^{ab} \bmod p$$
$$K = 2^{(3*5)} \bmod 467$$
$$K = 2^{15} \bmod 467$$
$$K = 32768 \bmod 467$$
$$= 78$$

Alice computes Shared with the known 32 key recieved from bob.

$$K_a = B^a \bmod p$$
$$= 32^3 \bmod 467$$
$$= 32768 \bmod 467$$
$$= 78$$

Bob computes the shared key with known & key recieved from Alice.

$$K_b = A^b \bmod p$$
$$= 8^5 \bmod 467$$
$$= 32768 \bmod 467$$
$$= 78$$

$K_a = K_b$ which proves that 78 is the shared key between Alice and bob.

2. $a = 400$, $b = 134$

Alice sends key to Bob.

$$A = \alpha^a \bmod p$$
$$= 2^{400} \bmod 467$$
$$= 137$$

Bob sends key to Alice.

$$B = \alpha^b \bmod p$$
$$= 2^{134} \bmod 467$$
$$= 84$$

Let's compute the shared key for alice and Bob.

$$k = \alpha^{ab} \bmod p$$
$$= 2^{(400 * 134)} \bmod 467$$

$= 2^{53600} \bmod 467$

$= 90$

K_a is Alice shared key with 84 recieved from bob. K_b is Bob shared key 137 recieved from Alice.

$K_a = B^a \bmod p$ $\quad$ $K_b = A^b \bmod p$

$K_a = 84^{400} \bmod 467$ $\quad$ $K_b = 137^{134} \bmod 467$

$K_a = 90$ $\quad$ $K_b = 90$

$K_a = K_b$, so 90 is the shared key for alice and bob.

3. $a = 228$, $b = 57$

Alice sends key to bob.

$A = \alpha^a \bmod p$

$= 2^{228} \bmod 467$

$= 394$

Bob sends key to Alice.

$$B = \alpha^b \bmod p$$
$$= 2^{57} \bmod 467$$
$$= 313$$

Let's find the shared key for alice and bob.

$$K = \alpha^{ab} \bmod p$$
$$= 2^{(228 * 57)} \bmod 467$$
$$= 2^{12996} \bmod 467$$
$$= 206$$

Let's find K_a and K_b, Alice computed shared key and bob computed shared key

$K_a = B^a \bmod p$

$= 313^{228} \bmod 467$

$= 206$

$K_b = A^b \bmod p$

$= 394^{97} \bmod 467$

$= 206$

$K_a = K_b$, the shared key for alice and bob is 206.

Question-2

E be eliptic curve defined ove $\mathbb{Z}_7$

$$E: \quad y^2 = x^3 + 3x + 2$$

a)

$P = (0, 3)$

$P = (0, 4)$

$P = (2, 3)$

$P = (2, 4)$

$P = (4, 1)$

$P = (4, 6)$

$P = (5, 3)$

$P = (5, 4)$

(b)

What is the group order.

$P = (0, 3)$

$2P = P + P$

$$s = \frac{3(x_1)^2 + a}{2y_1} \bmod 7$$

$$= \frac{3(0)^2 + 3}{6} \bmod 7$$

$$= 3/6 \bmod 7$$

$$= 4$$

$2P = (s^2 - x_1 - x_2 \bmod p,\ s(x_1 - x_3) - y_1 \bmod p)$

$2P = (2,3)$

$3P = 2P + P = (5,4)$

$4P = 3P + P = (4,6)$

$5P = 4P + P = (4,1)$

$6P = 5P + P = (5,3)$

$7P = 6P + P = (2,4)$

$8P = 7P + P = (0,4)$

$9P = 8P + P =$ neutral element

This group has order 9.

(c) $P = (0, 3)$

$2P = P + P$

$2P = (2, 3)$

$3P = 2P + P = (5, 4)$

$4P = 3P + P = (4, 6)$

$5P = 4P + P = (4, 1)$

$6P = 5P + P = (5, 3)$

$7P = 6P + P = (2, 4)$

$8P = 7P + P = (0, 4)$

$9P = 8P + P =$ neutral element

α has order 9 and is primitive element.

Question-3

given eliptic curve E ove Z_{29} point $P = (8, 10)$

$$E: \quad y^2 = x^3 + 4x + 20 \mod 29$$

Calculate K.P multiplication.

1. $K = 9$

$$9P = (1001)_2 P$$

$$1::P = (8, 10)$$

$O :: 2P = 2(8,10)$

$= (0, 22)$

$O :: 2P + 2P = 2(0,22)$

$(4P) = (6,17)$

$O :: 4P + 4P + P$

$= 2(6,17) + (8,10)$

$= (4, 10)$

2. $K = 26$

$20P = (10100)_2 P$

$1 :: P = (8, 10)$

$0 :: 2P = 2(8, 10)$

$= (0, 22)$

$1 :: 2P + 2P + P$

$= 2(0, 22) + (8, 10)$

$= (20, 3)$

$1 :: 5P + 5P = 2(20, 3) = (17, 19)$

$1 :: 10P + 10P + P$

$= 2(17, 19) + (8, 10)$

$= (19, 13).$

Question-4

Alice private key is $a = 6$

Bob's public key $B = (5, 9)$

Curve defined by

$$y^2 \equiv x^3 + x + 6 \bmod 11$$

Let's calculate the session key.

private key Alice $a = 6$

public key Bob $B = (5, 9)$

session key $T_{AB} = aB = 6B$

B is $(1)_2$ B = (5, 9)

2B = B + B = (10, 9)

3B = 2B + B = (7, 2)

6B = 3B + 3B = (2, 7)

⇒ Session key is (2, 7).