Class Fun

Date

Page No.

Q1) Alice & Bob use ElGamal scheme with common prime $q = 157$ and a primitive root $\alpha = 5$

a) Bob has public key $Y_B = 10$, Alice chooses random integer $k = 3$, What is ciphertext of $M = 9$?

$$k = Y_B^k \bmod q$$

$Y_B = 10 \quad k = 3 \quad q = 157$

$$k = 10^3 \bmod 157 = 58$$

We know,

$$C_1 = \alpha^k \bmod q = 5^3 \bmod 157$$
$$= 125 \bmod 157$$
$$= 125$$

$$C_2 = k.M \bmod q = (58.9) \bmod 157$$

$C_2 = 51$

Cipher text for $M = 9$, $C = 125, 51$

DTU/2K16/MC/13

Class Fun

Date | Page No.

b) Alice chooses new value K so M = 9 is C = (25, C_2) what is integer C_2?

Using direct algorithm, we see

K = 1 doesn't work K = 2 works

As $25 \bmod 157 = 5^2 \bmod 187 = C_1 = 25$

$\therefore K = 2$

Given M = 9

$C_2 = kM \bmod q$

$k = y_B^k \bmod q = 10^2 \bmod 157$

$= 100$

$C_2 = (100 \cdot 9) \bmod 157$

$= 900 \bmod 157$

$= 115$

$\boxed{C_2 = 115}$

PTU/2k16/MC/13

Class Fun

Date

Page No.

(Q2) Elliptic Curve over Real Numbers

$y^2 = x^3 - \frac{17}{12}x + 1$, Let $P = (1, 0)$ and $Q = (1.5, 1.5)$

Find $P+Q$ and $2P$?

$P = (1, 0)$ $\quad Q = (1.5, 1.5)$

From the addition formula

$$S = \frac{y_p - y_a}{x_p - x_a}$$

$$\frac{0 - 1.5}{1 - 1.5} = 3$$

$$x_R = S^2 - x_p - x_Q = 9 - 1 - 1.5$$
$$= 6.5$$

$$y_R = -y_p + S(x_p - x_R)$$

$$= 0.3\,(1 - 6.5)$$

$$= -16.5$$

$$P + Q = (6.5, -16.5)$$

Now, for the doubling formula :-

$$S = (3x_p^2 + a) / 2y_p$$

$$3 \times (1) + \left(\frac{-17}{12}\right) / 2(0)$$

This is not defined.

DTU/2K16/MC/13

Class Fun

Date | Page No.

Q3) Diffie Hellman technique with prime = 23 primitive root $\alpha = 5$

a) $Y_A = 8 \quad k = ?$

$Y_A = \alpha^{X_B} \bmod q$

$8 = 5^x \bmod 23$

$\log_5 8 \equiv x \bmod 23$

$x \equiv x \bmod 23 \equiv \log_5 8$

This is the discrete log problem

The solution to this equation is $x \equiv 6$

$5^6 \bmod 23 = 15625 \bmod 23$

Now, $K_2 = K = (Y_A)^{X_B} \bmod q$

$5^6 \bmod 23 = 8^6 \bmod 23$

$= 13$

Hence, $k = 13$

ii) To show 5 is primitive root :-

$\phi(23) = 22 \quad (23$ is prime)

For α to be a primitive root, we must

DTU/2K16/MC/13

Class Exm

Date

Page No.

need to check $a^2 \not\equiv 1 \bmod 23$

$5^{22} \equiv (5^2)^5 \cdot 5 = 2^5 \cdot 5 = 9 \cdot 5 \equiv -1 \bmod 23$

$5^2 \equiv 2 \bmod 23$

So, 5 is a primitive root modulo 23.

DTU/2K16/MC/13

Class Fun

Date

Page No.

Q5) $6^{472} \bmod 345$

a	b (Binary)	Exponentiation
6	111011000	1
36	11101100	1
1296	1110110	1
2851	111011	2851
501	11101	2951
1706	1110	881
856	111	881
1926	11	2836
786	1	1551
3096	0	3346

So, $6^{427} \bmod 345 = 3346$

DTU/2K16/MC/13

Class Fun

Date | Page No.

(Q6) We have N = 77

$\phi(N) = 60$

Relatively prime to 77 are :-

[1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59]

We can choose e = 13, and it is given here correct.

$d = e^{-1} \bmod \phi(N)$

$= 13^{-1} \bmod 60$

$= 37$

We are given ciphertext C = 20

plaintext $M = C^d \bmod N$

$= 20^{37} \bmod 77$

$20^{2+35} \bmod 77$

$20^2 \cdot 20^{35} \bmod 77$

$(400 \bmod 77)\ 20^{35} \bmod 77$

$15 \cdot 20^{35} \bmod 77$

$20\ (20^2)^{17} \cdot 20 \bmod 77$

$(400 \bmod 77)^{17} \cdot 20 \bmod 77$

$(15)^{17} \bmod 77$

$M = 48$