CIS 3362 11/1/2021

(1) El Gamal

(2) rsa2.py (Webcourses)

Public Elements

q = prime #

α = generator/primitive root

Alice (Key Generation)

Private key: $X_A < q-1$

Calculate $Y_A = \alpha^{X_A} \bmod q$

Public key = $\{q, \alpha, Y_A\}$

Bob to send message to Alice

Plaintext: $M < q$

1. Bob picks random integer, k, $k < q$.
2. Calculate $K = (Y_A)^k \bmod q$
3. Calculate $C_1 = \alpha^k \bmod q$
4. Calculate $C_2 = K \cdot M \bmod q$

Send to alice ordered pair (C_1, C_2)

Alice receives (C_1, C_2)

1. Calculate $K = C_1^{X_A} = (\alpha^k)^{X_A} = (\alpha^{X_A})^k = Y_A^k = K$
2. Calculate $K^{-1} \bmod q$. 3. $M = (K^{-1}) \cdot C_2 \bmod q$

$p = 17$ $\alpha = 7$

$X_A = 6$

$Y_A = 7^6 \equiv (7^2)^3 \equiv 15^3 \equiv (-2)^3 = -8 \equiv 9 \pmod{17}$

$\boxed{Y_A = 9}$

Bob

$M = 12, \quad k = 3$

$K = 9^3 \bmod 17$

$= 9^2 \times 9 \bmod 17$

$= 13 \times 9 \bmod 17$

$= 15 \bmod 17$

$C_1 \equiv 7^3 \equiv (-2)(7)$

$\equiv -14 \equiv 3 \bmod 17$

$C_2 = K \cdot M = 15 \times 12$

$= (-2)(-5) = 10 \bmod 17$

$B \to A : (3, 10)$

Alice 1. $3^6 \equiv (3^3)^2 \equiv 27^2$

$\equiv 10^2 \equiv \boxed{15 \bmod 17}$

2. $17 = 1 \times 15 + 2$

$15 = 7 \times 2 + 1$

$15 - 7 \times 2 = 1$

$15 - 7(17 - 15) = 1$

$8 \times 15 - 7 \times 17 = 1$

$15^{-1} \equiv 8 \bmod 17$

3. $K^{-1} \times C_2$

$= 8 \times 10$

$= 80$

$\equiv \boxed{12 \bmod 17}$

$k = 8$

$K = 9^8 \bmod 17$

$= 1$

$C_1 = \alpha^k = 7^8 = 16$

$C_2 = 1 \times 12 = 12$

$B \to A \quad (16, 12)$

Alice 1. $16^6 \equiv 1$

2. $1^{-1} \equiv 1$

3. $K^{-1} \times C_2$

$= 1 \times 12$

$= \boxed{12}$

$p = 17 \quad d = 7 \quad Y_A = 9, \; X_A = 6$

Bob picks $k = 13$

$M = 12$

1. $K = Y_A^{\,k} = 9^{13} = 8$ ✓

2. $C_1 = 7^{13} = 6$ ✓

3. $C_2 = KM = 8 \times 12 = 96$
$\equiv 11 \bmod 17$

$B \rightarrow A \quad (6, 11)$

Alice: 1. $C_1^{\,X_A} = 6^6 = 8 = K$ ✓

2. $K^{-1} \bmod 9$
$8^{-1} \bmod 17$
$17 = 2 \times 8 + 1$
$1 \times 17 - 2 \times 8 = 1$
$K^{-1} = -2 = 15$ ✓

3. $K^{-1} \times C_2$
$= 15 \times 11$
$= 165 \equiv 12 \bmod 17$ ✓