El-Gamal

Public keys: Prime: q primitive root: α

Alice

Picks X_A, $1 < X_A < q-1$ randomly as Private key.

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

Y_A is Alice's 3rd Public Key.

Bob → Alice

1. $0 \le M \le q-1$ msg.
2. Pick random k, $1 \le k \le q-1$
3. Calculate $K = (Y_A)^k \bmod q = (\alpha^{X_A})^k \equiv \alpha^{X_A k} \bmod q$
4. Send $C = (C_1, C_2)$.

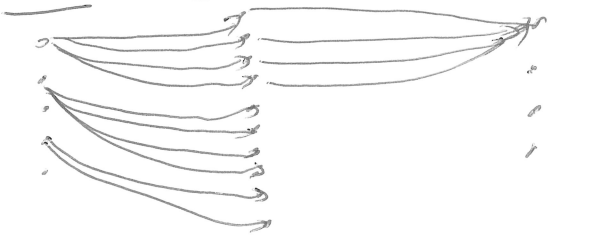
$C_1 = \alpha^k \bmod q \quad C_2 = KM \bmod q$

What Alice Does

1. Compute $C_1^{X_A} = (\alpha^k)^{X_A} \equiv \alpha^{X_A k} \equiv K \bmod q$
2. Compute $K^{-1} \bmod q$ via EEA.
3. Compute $K^{-1} C_2 = K^{-1}(KM) = (K^{-1}K)M$

$\equiv M \bmod q$

P $\quad C = P^2 \xrightarrow{\text{decrypt}}$ P



1	2	3	4	5	6
3	2	6	4	5	1

Public: $q = 7$ $\alpha = 3$

Alice $X_A = 3$ $Y_A = 3^3 = 6$

11/2/19 (2)

Bob $m = 2$

m	k	K	C_1	C_2
2	1			
2	2			
2	3			
2	4			
2	5			
2	6			

2, 4, 8, 5, 10, 9, 7, 3, 6, 1

Public $q = 11$ $\alpha = 2$

Alice $X_A = 4$ $Y_A = 2^4 \equiv \boxed{5} \bmod 11$

m	k	K	C_1	C_2	$C_1^{X_A} K$	K^{-1}	$K^{-1} C_2$
7	1	5	2	2	5	9	7
7	2	3	4	10	3	4	7
7	3	4	8	6	4	3	7
7	4	9	5	8	9	5	7
7	5	1	10	7	1	1	7
7	6	5	9	2	5	9	7
7	7	3	7	10	3	4	7
7	8	4	3	6	4	3	7
7	9	9	6	8	9	5	7
7	10	1	1	7	1	1	7