CIS 3362 11/1/24

RSA last time - 1st Public Key Crypto System

→ El Gamal → TODAY

→ Elliptic Curve Cryptography (what more people want to use)
→ next week

RSA security is based on factoring

All public key systems are based on trapdoor functions of some sort: easy to forwards, hard to undo/backwards.

easy $p \times q = n$ hard $n \rightarrow p \times q$

Discrete Log Problem

easy $b^e \bmod n$ hard I give you c, b, n, find e

$b^e = c \bmod n$

El Gamal uses the Discrete Log Problem

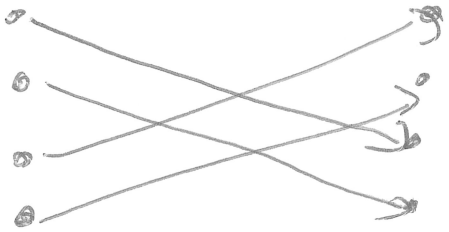
Plaintext is one number

Ciphertext is a pair of numbers

multiple ciphertexts can be valid for the same plaintext/key pair.

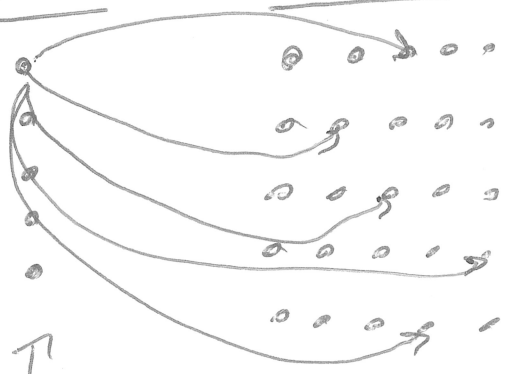
Typical Picture

Plain → Cipher



El Gamal

Plain → Cipher



n options

n^2 options

Alice creates Public keys

Public elements:
- Large Prime: q
- Primitive Root: α

Y_A (Alice's Public Key) $= \alpha^{X_A} \bmod q$

→ even though everyone can see Y_A, it is computationally infeasible to calculate X_A.

Private key: X_A

$1 < X_A < q-1$

Alice's Private Key

1. Bob wants to send $M \rightarrow$ Alice $\quad 0 \leq M < q$.
2. Bob pick random int k (lowercase) $\quad 1 \leq k \leq q-1$.
3. K (~~capital~~ capital) $= Y_A^k \bmod q$.
4. Send (C_1, C_2). $C_1 = \alpha^k \bmod q \quad C_2 = KM \bmod q$

How can Alice read the message

$$K = Y_A^k = (\alpha^{X_A})^k = \alpha^{X_A k} \equiv \alpha^{X_A k} \bmod q$$

$$K^{-1} C_2 = (K^{-1} K) m \bmod q$$

$$\equiv$$

$$M = K^{-1} \times C_2 \bmod q \rightarrow$$ Alice's goal is to find $K^{-1} \bmod q$

$$C_1 = \alpha^k \quad \text{Alice} = C_1^{X_A} \bmod q$$

$$= (\alpha^k)^{X_A}$$

$$= \alpha^{k X_A} \bmod q$$

$$= K$$

Alice's steps

1. $C_1^{X_A} \rightarrow K$
2. Calculate $K^{-1} \bmod q$
3. $M = K^{-1} \times C_2$

$q = 13$, $\alpha = 2$ (6, 11, 7)

Alice picks $X_A = 8 \rightarrow Y_A = 2^8 \bmod 13$

$= (2^4)(2^4) \bmod 13$

$= 16 \times 16 \bmod 13$

$= 3 \times 3 \bmod 13$

$= 9$

Public Info

$q = 13, \alpha = 2$

$Y_A = 9$

1. Bob wants to send $M = 6$.

2. $k = 5$

3. $Y_A^k = 9^5 = 3 \mod 13 = K$ ($9^5 \rightarrow (2^8)^5$)

4. (C_1, C_2) $\quad C_1 = \alpha^k = 2^5 = 32 \mod 13 = 6$

$C_2 = 3 \times 6 = 18 = 5 \mod 13$

Bob sends $(6, 5)$ to Alice.

Alice sets $C_1 = 6$, $C_2 = 5$

1. $C_1^{X_A} = 6^8 = 3 \rightarrow K$ ($6^8 \rightarrow (2^5)^8$)

2. $3^{-1} \mod 13 = 9$ $\quad k^{-1} \mod 13$

3. Alice $\quad 9 \times 5 = 45 \mod 13$

$= \boxed{6}$ M

Take 2 Bob uses diff k.

1. Bob wants to send $m = 6$.
2. $k = 7$
3. $Y_A^k = 9^7 = 9 = \underline{\underline{K}}$
4. (C_1, C_2), $C_1 = \alpha^k = 2^7 = 11 \mod 13$

$C_2 = 9 \times 6 = 54 \mod 13$
$= 2 \mod 13$

Bob sends Alice $(11, 2)$

Alice gets $C_1 = 11$ $C_2 = 2$

1. $C_1^{X_A} = 11^8 = 9 = K$
2. $K^{-1} \mod q$ $9^{-1} \mod 13 = 3$
3. $K^{-1} \times C_2 = 3 \times 2 = \boxed{6}$ M

We can interpret an integer in base 26 convert to a string of letters

file
C_1 C_2 → decrypt
C_1 C_2
C_1 C_2
↓

$M = 3264173_{26}$ then $_{10}$
↳ convert to base 26

0, 7, 3, 18, 17, 3 ←

A H D S R D