

CIS3362 11/4/2022

El-Gamal Cryptosystem

- based on Discrete Log Problem
(looks similar to Diffie-Hellman)

Main ~~drawback~~^{vs RSA} - Ciphertext is twice as long as

Plaintext. | Plaintext can map to many ciphertexts,
all those ciphertexts map back to the same plaintext

Public elements: Prime # p
Generator α

Secret Info: Alice picks x_A $1 < x_A < p-1$ secret

3rd public element: $Y_A = \alpha^{x_A} \text{ mod } p$

Bob wants to send message to Alice

1. Bob picks a random value, k , $1 \leq k \leq p-1$.

2. $K = Y_A^k \text{ mod } p$ $\left[(\alpha^{x_A})^k \equiv \alpha^{x_A k} \text{ mod } p \right]$

3. Ciphertext is ordered pair $(C1, C2)$

$$C1 = \alpha^k \text{ mod } p \quad C2 = \left(\frac{K \times M}{\pi} \right) \text{ mod } p$$

plaintext msg

Alice receives C_1, C_2

$$1. K = C_1^{X_A} \pmod{p}$$

$$(2^k)^{X_A} \equiv 2^{X_A k} \pmod{p}$$

2. Calculates $K^{-1} \pmod{p}$ via EEA.

$$3. M = (K^{-1} \times C_2) \pmod{p}$$

$$\underbrace{K^{-1} \times K}_{1} \times M \equiv \underline{\underline{1 \times M}} \pmod{p}$$