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

Main drawback vs RSA
Ciphertext is twice as long as Plaintext,
1 Plaintext can map to many ciphertexts,
all these 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: \( Y_A = \alpha^{X_A} \mod p \)

Bob wants to send message to Alice

1. Bob picks a random value, \( k \), \( 1 \leq k \leq p-1 \).
2. \( K = Y_A^k \mod p \) \( \left[ (\alpha^{X_A})^k = \alpha^{X_Ak} \mod p \right] \)
3. Ciphertext is ordered pair \((C_1, C_2)\)

\[
C_1 = \alpha^k \mod p \\
C_2 = \left( K \times M \right) \mod p
\]
Alice receives C1, C2

1. \( K = C1^{x_A} \mod p \)
   \((2^k)^{x_A} = 2^{x_A + k} \mod p \)

2. Calculates \( K^{-1} \mod p \) via EEA.

3. \( M = (K^{-1} \times C2) \mod p \)
   \( \overline{K^{-1} \times k \times M = 1 \times M \mod p} \)