ELGAMAL CRYPTOSYSTEM

ELGAMAL CRYPTOSYSTEM

- Besides RSA and Rabin, another public-key cryptosystem is ElGamal. ElGamal is based on the discrete logarithm problem.

- In **cryptography**, the **ElGamal encryption** system is an asymmetric key **encryption algorithm** for public-key **cryptography** which is based on the Diffie–Hellman key exchange. It was described by Taher **Elgamal** in 1985

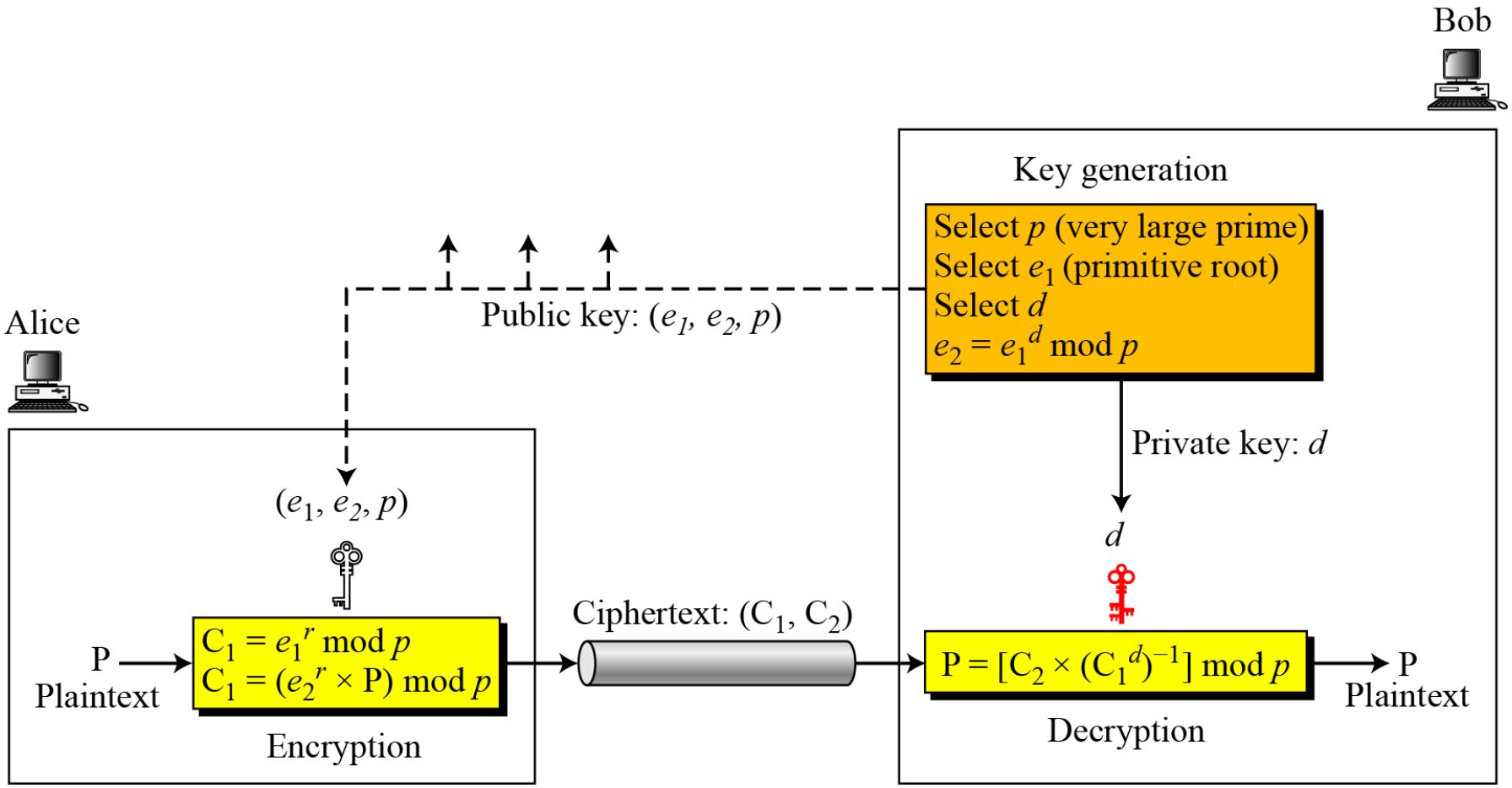
ELGAMAL ENCRYPTION CONSIST 3 COMPONENTS:

1)KEY GENERATOR

2)ENCRYPTION

3)DECRYPTION

Key generation, encryption, and decryption in ElGamal



Generate Keys

Agent X chooses

I. A large prime p
II. A primitive element g modulo p
III. A (possibly random) integer d with $2 \leq d \leq p-2$.
IV. Computes $e = g^d \bmod p$
V. Posts public key (p, g, e).
VI. Private key is d.

Encryption

1. Agent Y encrypts a short message M (M < p) and sends it to Agent X like this:
2. Agent Y chooses a random integer k (which he keeps secret).
3. Agent Y computes **$Y1 = g^k \bmod p$** and **$Y2 = M * e^k \bmod p$**
4. Agent Y sends his encrypted message (Y1, Y2) to Agent X

Decryption

When Agent X receives the encrypted message (Y1, Y2), he decrypts (using the private key d) by computing

- **Plain text = $Y2 * (Y1^{d})^{-1} \bmod p$**

EXAMPLE:

Here is a trivial example. Bob chooses p = 11 and g or e1 = 2. and d = 3 e2 or e = 8. So the public keys are (2, 8, 11) and the private key is 3. Alice chooses r or k = 4 and calculates C1 and C2 for the plaintext 7.

Plaintext: 7

$C_1 = e_1^{\,r} \bmod 11 = 16 \bmod 11 = 5 \bmod 11$

$C_2 = (P \times e_2^{\,r}) \bmod 11 = (7 \times 4096) \bmod 11 = 6 \bmod 11$

Ciphertext: (5, 6)

Bob receives the ciphertexts (5 and 6) and calculates the plaintext.

$$[C_2 \times (C_1^{\,d})^{-1}] \bmod 11 = 6 \times (5^3)^{-1} \bmod 11 = 6 \times 3 \bmod 11 = 7 \bmod 11$$

Plaintext: 7

TASK:

- *Here is a trivial example. Bob chooses p = 13 and g = 2. and d = 3 . So the public keys are (p,g,e) and the private key is 3. Alice chooses r = 7 and calculates C1 and C2 for the plaintext 4.*

- *Bob chooses p = 23 and e1 = 7. and the private key is 9. Alice chooses random integer k = 3 . calculates C1 and C2 for the plaintext 20.*