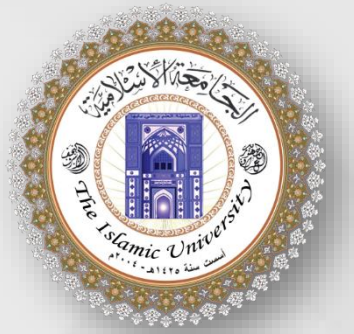


The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 12

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective :

- **Rivest–Shamir–Adleman (RSA) Algorithm.**

RSA Algorithm

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA Algorithm

Alice

Sender

Bob

Receiver

Design Target

Design Target

RSA Encipher

Communication Channel

RSA Decipher

Plaintext (ASCII code)

Ciphertext

Plaintext (ASCII code)

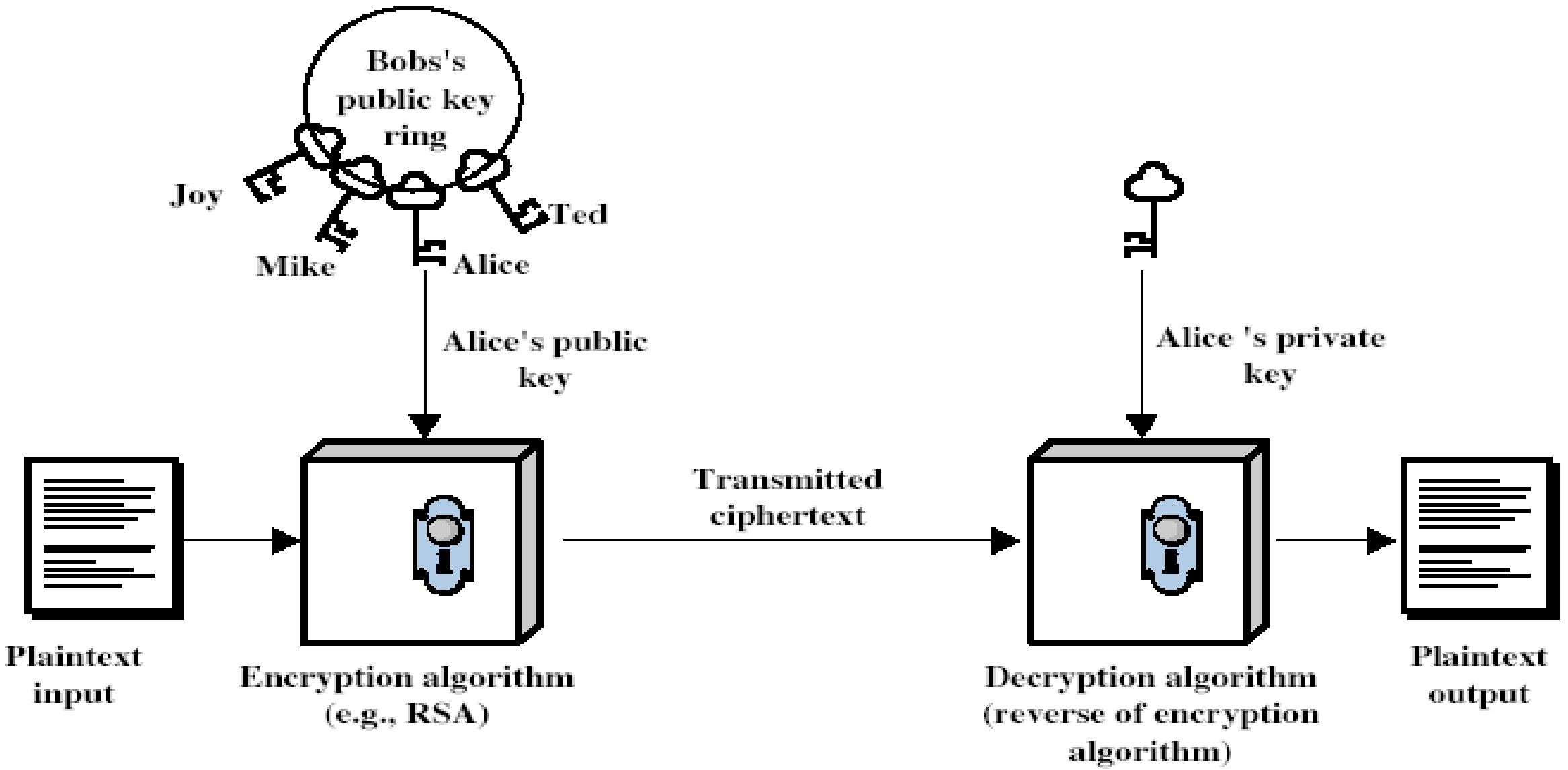
Encryption Key (Public Key)

(E,M)

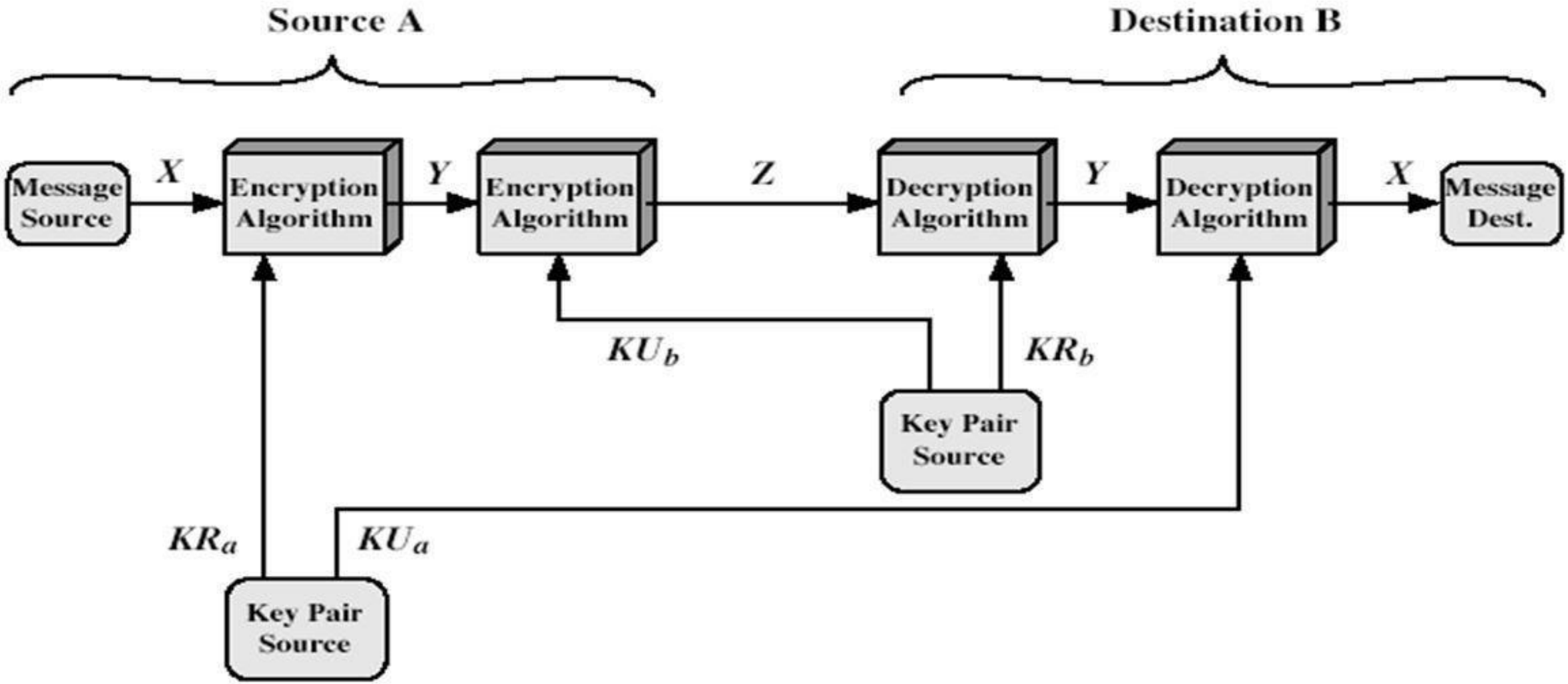
(D,M)

Decryption Key (Private Key)

Public-Key Cryptography



Public Key Cryptosystem : Secrecy and Authentication



RSA Algorithm

Encryption equation will be : $C = M^e \bmod n$

Decryption equation will be : $M = C^d \bmod n$

Where

- M → Message
- C → Ciphertext
- n → Number of Mod
- e → Encryption
- d → Decryption

RSA Algorithm

- Each user generates a public/private key pair by:
- Selecting two large primes at random **p, q** Where **p ≠ q**
- Computing their system modulus **n = p * q**
  - Note **ø(n) = (p - 1) * (q - 1)**
- Selecting at random the encryption key **e**
  - where **1< e < ø(n), gcd(e, ø(n)) = 1**
- Solve following equation to find decryption key **d**
  - **(e * d) mod ø(n) = 1** and **0 ≤ d ≤ n**
- **Publish their public encryption key: PUK = {e, n}**
- **Keep secret private decryption key: PRK = {d, p, q}**

Example 1

By using RSA find Public Key (PUK), Private Key (PRK), then Encrypt and Decrypt the message (88) if p = 11, q = 17.

Ans:-

1) p = 11, q = 17

2) n = p * q = 11 * 17 = 187

3) ø(n) = (p – 1) * (q – 1)

ø(n) = (11 – 1) * (17 – 1)

ø(n) = (10) * (16) = 160

4) e → gcd (ø(n), e) = 1

gcd (160, e) = 1

gcd (160, 7) = 1

5) (e * d) mod ø(n) = 1

(7 * d) mod 160 = 1

(7 * 23) mod 160 = 1

(161) mod 160 = 1

6) Public Key (PUK) = (e, n) → (7, 187)

7) Private Key (PRK) = (d, p, q) → (23, 11, 17)

8) Encryption : M = 88

$$C = M^e \bmod n$$

$$C = 88^7 \bmod 187$$

$$C = \left[\left(88^1 \bmod 187\right) * \left(88^2 \bmod 187\right) * \left(88^4 \bmod 187\right)\right] \bmod 187$$

$$C = [(88) * (77) * (132)] \bmod 187$$

$$C = 11$$

9) Decryption : C = 11

$$M = C^d \bmod n$$

$$M = 11^{23} \bmod 187$$

$$M = [(11^1 \bmod 187) * (11^2 \bmod 187) * (11^4 \bmod 187) * (11^8 \bmod 187) * (11^8 \bmod 187)] \bmod 187$$

$$M = [(11) * (121) * (55) * (33) * (33)] \bmod 187$$

$$M = 88$$

Homework

Q1/ By using RSA find Public Key (PUK), Private Key (PRK), then Encrypt and Decrypt the message (5) if p = 3, q = 11 and e = 7.

Q2/ By using RSA find Public Key (PUK), Private Key (PRK), then Encrypt and Decrypt the message (2) if p = 17, q = 31 and e = 7.