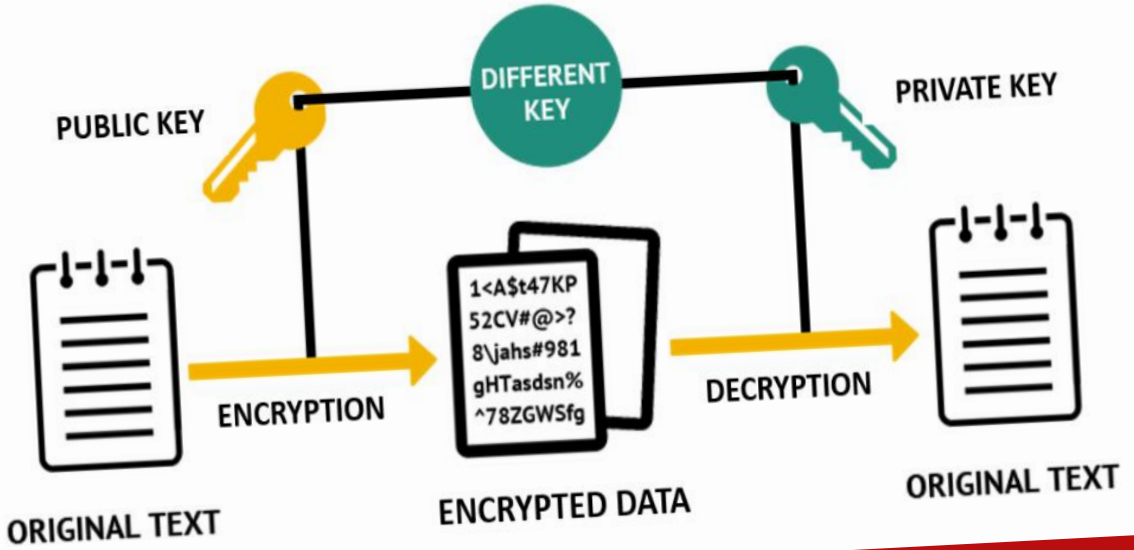
ASYMMETRIC CIPHER

NINTH LECTURE



Assist Prof. Dr. Saja J. Mohammed

2025-2024

WHY ASYMMETRIC ALGORITHMS?

The main reson that coused to introduce the asymmetric algorithms is **Key Management**: In symmetric encryption, the same secret key is used for both encryption and decryption. This means that both the sender and the recipient need to possess and securely share the same key in advance. This can be challenging when communicating over insecure channels or when there are multiple parties involved.

On the other hand, asymmetric encryption uses a pair of mathematically related keys: a public key for encryption and a private key for decryption. The public key can be freely shared, while the private key is kept secret. This eliminates the need for key distribution and allows for secure communication even if the public key is intercepted.

The defferences between symmetric and asymmetric algorithms

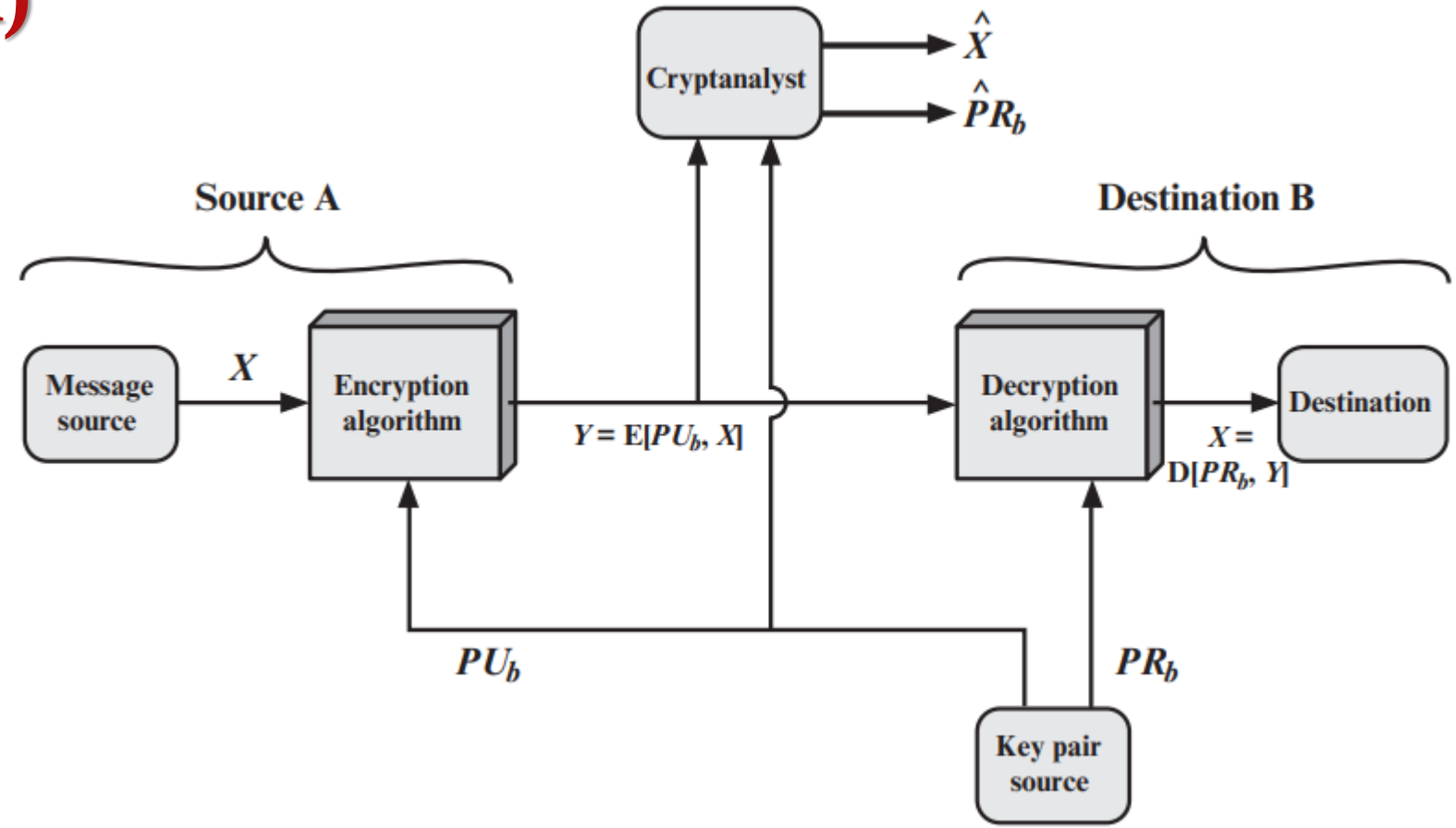
Symmetric	Asymmetric
• For Symmetric Cryptography, the same key is used for encryption and decryption	• For Asymmetri Cryptography, different keys are used for encryption and decryption
• In Symmetric Cryptography, the speed of encryption and decryption is very fast	• In asymmetric cryptography, the speed of encryption and decryption is slower
• The size of the encrypted text in symmetric cryptography is mostly like the size of the original plaintext	• In Asymmetric cryptography, the size of the text is more than the original plaintext
• Both parties should know the key in symmetric key encryption	• Only one of the keys is known by both the parties in asymmetric cryptography

ASYMMETRIC ALGORITHMS (PUBLIC KEY CIPHER)

- Asymmetric encryption algorithms use **two different keys** for encryption and decryption these key pairs are called, public and privte keys.
- To **ensure confedentaility**, **public key is** used for encryption, and **private key** is used for decryption. When consider ensuring confedentaility, we can define the key-pair as followes:
- **Public key** is a publicly shared key that used for encryption.
- **Private key** is a key used for decryption, it is kept secret and known only to the owner. Private key is derived from the public key using mathematical algorithms. Knowing the public key only must never allows getting the private key.

Note: Both the keys must belong to the **receiver.**

ASYMMETRIC ALGORITHMS (PUBLIC KEY CIPHER)



THE RIVEST-SHAMIR-ADLEMAN (RSA)

- Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman .
- A most popular example of public key algorithm.
- The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

- The algorithm can be divided into 3 steps:
  - ✓ Key generation
  - ✓ Encryption
  - ✓ Decryption

RSA ALGORITHM STEPS

Key generation ➔

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption ➔

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption ➔

Decryption by Alice with Alice's Private Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

RSA EXAMPLE:

Suppose you have the value of p=7 and q=11, generate the RSA key pair

Solution :

Compute n : n= p*q = 7* 11=77 **(can encrypt numbers from 0 to 77-1)**

Compute Ø(n): Ø(77) = (7-1)* (11-1)=6*10=60

Select value of e: where gcd(e, 60)=1 and 1<e<60

suppose e=7 (gcd(7,60)=1) 1<7<60

Public key {e,n}= {7,77}

To generate private key:

Find value of d: d= e^{-1} mod Ø (n)

= 7^{-1} mod 60

= $7^{\emptyset(60)-1}$ mod 60)

= 7^{16-1} mod 60

= 7^{15} mod 60 = 43

Ø(60)=4*3*5=(2*1)*(3-1)*(5-1)=2*2*4=16

Private key {d,n}={43,77}

RSA EXAMPLE:

To encrypt the plaintext (5) using public key{7,77}

C=p^e mod n

C= 5^7 mod 77

C = 47

To decrypt the cipher (47) using private key {43,77}:

P=c^d mod n

P=47^{43} mod 77

P= 5

RSA H.W.:

Suppose you have the value of p=3 and q=11, encrypt the plaintext 7 using RSA algorithm.

The solution :

1. Key generation:

p=3 , q=11

n=3*11=33

Ø(n)=(3-1)*(11-1)=2*10=20

…

.

.

.

.

.