VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

B.Tech. Winter Semester 2024-25
School Of Computer Science and Engineering (SCOPE)

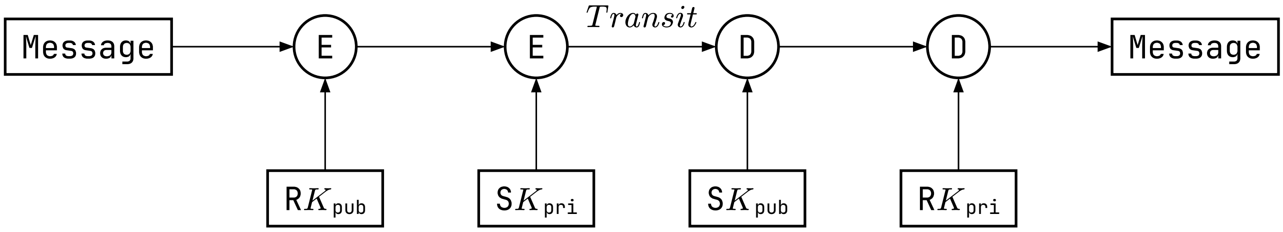
Notes
Cryptography and Network Security

Apurva Mishra: 22BCE2791

Date: CAT - II

Contents

1 Module 3: Asymmetric Encryption Algorithm and Key Exchange



1.1 Principles

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes

1.2 RSA

1.2.1 Steps

1. Choose two large primes:

$$\begin{gathered} P, Q \\ N = P * Q \end{gathered} \tag{1}$$

2. Choose public and private key:

$$\begin{gathered} K_{\text{pub}} \mid K_{\text{pub}} \text{ is not factor of } \phi(N) \\ K_{\text{pri}} \mid (K_{\text{pri}} * K_{\text{pri}}) \bmod \phi(N) = 1 \end{gathered} \tag{2}$$

3. Encrypt:

$$CT = PT^{K_{\text{pub}}} \bmod N \tag{3}$$

4. Decrypt:

$$PT = CT^{K_{\text{pri}}} \bmod D \tag{4}$$

1.3 ElGamal

1.4 Elliptic Curve cryptography

1.5 Homomorphic Encryption and Secret Sharing

1.6 Key distribution and Key exchange protocols

1.7 Diffie-Hellman Key Exchange

1. Choose public numbers such that:
   - g is primitive root of n
   - g, n are primes

$$g, n \tag{5}$$

2. Choose private numbers:

$$\begin{aligned} x_A \mid x < n \\ y_B \mid y < n \end{aligned} \tag{6}$$

3. New public values:

$$\begin{aligned} A = g^x \bmod n \\ B = g^y \bmod n \end{aligned} \tag{7}$$

4. Generate Keys User side:

$$\begin{aligned} K_A = B^x \bmod n \\ K_B = A^y \bmod n \\ K_A == K_B \end{aligned} \tag{8}$$

1.8 Man-in-the-Middle Attack

2 Module 4: Message Digest and Hash Functions

2.1 Requirements for Hash Functions

2.2 Security of Hash Functions

2.3 Message Digest (MD5)

2.4 Secure Hash Function (SHA)

2.5 Birthday Attack

2.6 HMAC