SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-2 NUMBER THEORY AND PUBLIC KEY CRYPTOSYSTEMS

Advantages of Public Key Cryptography

- **Enhanced Security and Confidentiality**
- Public key cryptography takes online security to the next level. With traditional methods, if someone intercepts the key to lock a message, they can unlock it.
- But with public key cryptography, your private key stays secret, ensuring only you can unlock messages encrypted with your public key.
- **Digital Signatures and Authentication**
- Public key cryptography enables the ability to confirm a message's origin and integrity without doubt. This is achieved through digital signatures. When you need to sign a digital document or message, your private key generates a distinct "stamp" that's unique to you.
- By employing your public key, others can verify this stamp, affirming your message's authenticity and untouched nature.
- **Key Distribution and Management**
- Sharing secret keys securely can be tricky, especially in large networks. Public key cryptography simplifies this by allowing you to share your public key openly while keeping your private key secret. Others can use your public key to encrypt messages they send to you.
- This means you don't need to exchange secret keys with everyone you communicate with – a big advantage for managing keys in complex environments

Common Public-key Cryptography Algorithms

- **RSA (Rivest-Shamir-Adleman)**
- RSA is like the grandfather of public-key cryptography. It's named after its creators. This algorithm uses a pair of public and private keys to encrypt and decrypt messages.
- **Diffie-Hellman**
- Diffie-Hellman is like a secret conversation in a busy room. It lets two parties agree on a secret without actually sharing it. Both sides create their own secret, then mix it with a shared number.
- **Elliptic Curve Cryptography (ECC)**
- ECC is like the sleek sports car of cryptography. It offers strong security with relatively smaller keys, making it efficient for mobile devices and constrained environments.

Applications of Public-key Cryptography

- **SSL/TLS for Secure Web Browsing**
  - SSL/TLS uses public-key cryptography to create a secure connection between your device and websites, safeguarding your sensitive information during online activities like shopping and banking.
- **Secure Email Communication (PGP/GPG)**
  - PGP and GPG utilize public key cryptography to encrypt emails, ensuring only the intended recipient with the matching private key can access the content.
- **Secure File Transfer (SFTP)**
  - SFTP employs public key cryptography to encrypt files during transfer, preventing unauthorized access and ensuring secure file sharing between devices or servers.

Limitations and Challenges

- **Computational overhead**
- Public-key cryptography, while secure, can be computationally demanding. Encrypting and decrypting messages using public and private keys requires more processing than simpler public key encryption methods.
- This can slow down data transmission and processing, especially on devices with limited resources
-