جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

قسم الامن السيبراني

Department of Cyber Security

Subject:

Public key encryption

Class:

third

Lecturer:

Asst. Lecturer Qusai Al-Durrah

Lecture (1):

Introduction to public key encryption

Introduction:

Modern society relies heavily on digital communication and the exchange of sensitive data such as online banking transactions, electronic medical records, and cloud-based services. These activities demand robust methods for ensuring confidentiality and authenticity. **Public Key Cryptography**—also called asymmetric cryptography—addresses two major challenges faced by traditional symmetric encryption:

1. **Key Distribution:** Eliminates the need for a secure channel to share a single secret key.
2. **Digital Signatures:** Provides a mechanism to verify the sender's identity and prevent repudiation of messages.

Activity (1) - Hand-Raising Question:

Who can give me a real-life example where secure communication and authenticity are essential?

Learning Outcomes:

By the end of this lecture, students will be able to:

- **Define and Differentiate:** Clearly define *public key cryptography* and explain how it differs from *symmetric (secret-key) encryption*.
- **Explain Key Generation and Usage:** Describe the process of generating a public/private key pair and illustrate how each key is applied in encryption and decryption.
- **Analyze Security Functions:** Discuss how public key systems ensure **confidentiality**, enable **authentication**, and provide **digital signatures** for message integrity and non-repudiation.
- **Evaluate Strengths and Limitations:** Critically assess the advantages and potential drawbacks of public key encryption when compared with conventional symmetric methods

Principles of Public-Key Cryptosystems

The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. The first problem is that of key distribution.

key distribution under symmetric encryption requires either:

1- that two communicants already share a key, which somehow has been distributed to them;

2- the use of a key distribution center.

Whitfield Diffie, one of the discoverers of public-key encryption (along with Martin

Hellman, both at Stanford University at the time), reasoned that this second requirement negated the very essence of cryptography: the ability to maintain total secrecy over your own communication.

If the use of cryptography was to become widespread, not just in military situations but for commercial and private purposes, then electronic messages and documents would need the equivalent of signatures used in paper documents. That is, could a method be devised that would stipulate, to the satisfaction of all parties, that a digital message had been sent by a particular person?

This is a somewhat broader requirement than that of authentication

- ***Diffie and Hellman*** *achieved an astounding breakthrough in 1976 by coming up with a method that addressed both problems and that was radically different from all previous approaches to cryptography, going back over four millennia.*

Components of a Public-Key Cryptosystem

Public-key (asymmetric) algorithms use **two related keys**: one for encryption and a different, but mathematically linked, key for decryption.

Key Characteristics

- It is **computationally infeasible** to determine the private (decryption) key from knowledge of the algorithm and the public (encryption) key.
- In some algorithms (e.g., RSA), **either key** can be used to encrypt, with the other used to decrypt.

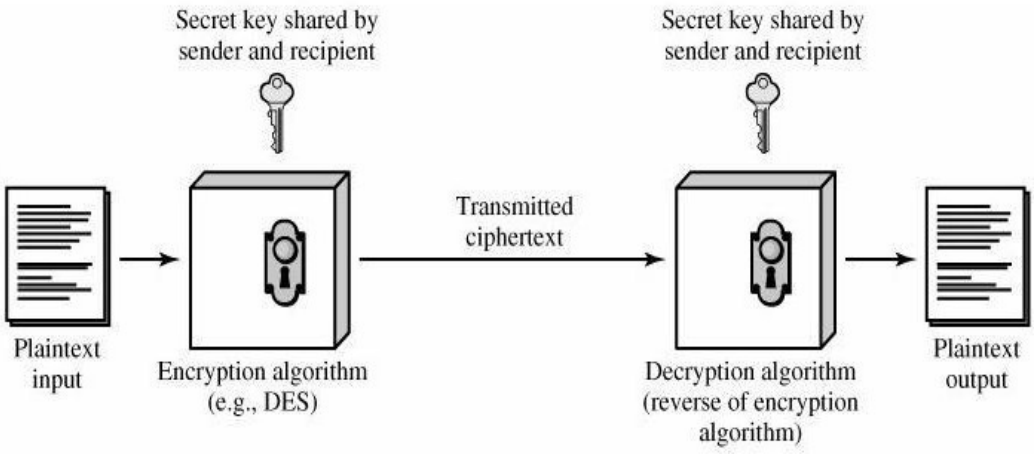
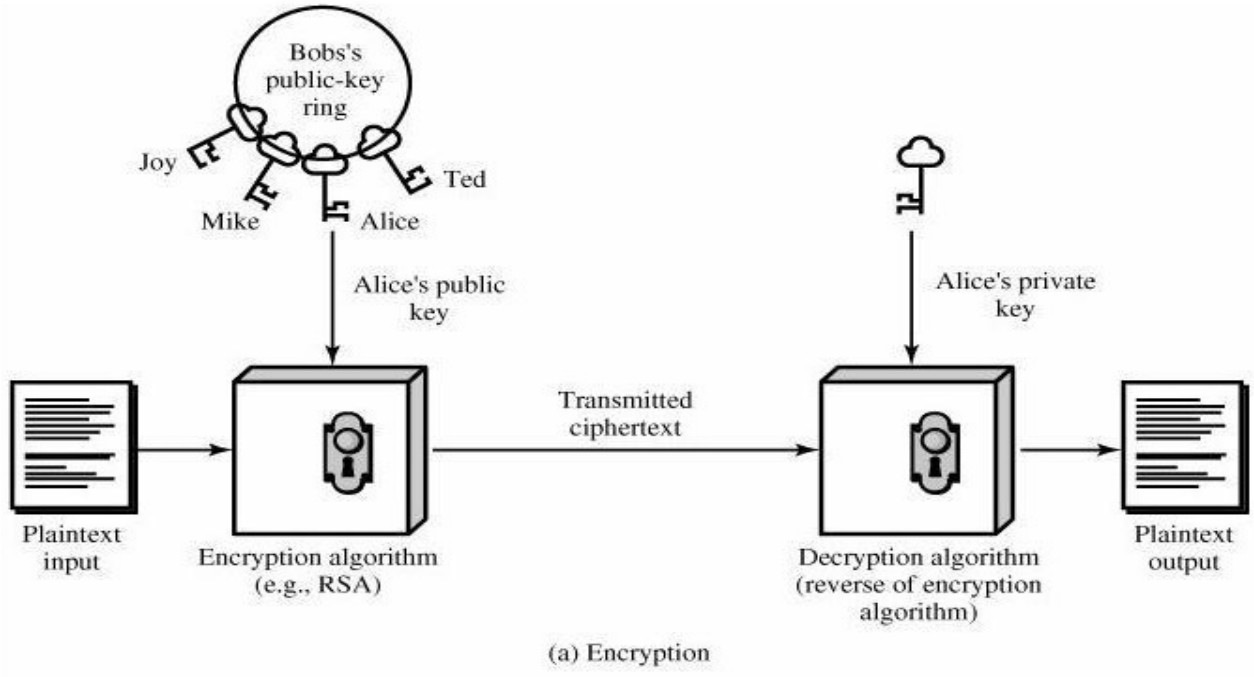


Figure (1): Simplified Model of Conventional Encryption



Figure(2): Public-Key Cryptography

- ***Plaintex***t: The original readable message that is fed into the algorithm as input.
- ***Encryption algorithm***: Transforms plaintext into ciphertext.
- ***Public and private keys***: This is a pair of keys that have been selected so that if **one is used for encryption, the other is used for decryption**. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- ***Ciphertext***: This is the **scrambled** message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- ***Decryption algorithm***: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

The essential steps are the following:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private; each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

With this model, every participant can freely obtain public keys, while each individual generates and retains their own private key, eliminating the need for private-key distribution.

As long as a user safeguards the private key, all received communications remain secure. Moreover, a system can replace its private key at any time and simply release the corresponding new public key to maintain confidentiality.

Activity (2) - Discussion (Raise Hands):

Raise your hand if you think the public key should remain secret just like the private key. Why or why not?

Conventional vs. Public-Key Encryption

The table below highlights key differences between symmetric and public-key (asymmetric) encryption.
In symmetric encryption, the single key used for both encryption and decryption is called the **secret key**.
In contrast, asymmetric encryption employs a **public key** and a **private key**. Although the private key must remain confidential, it is specifically termed "private" rather than "secret" to prevent confusion with the symmetric model's secret key.

Feature	Conventional (Symmetric)	Public-Key (Asymmetric)
Keys	Same key for encryption & decryption	Matched pair: one public, one private
Key Distribution	Secure channel required	Only public key is shared
Security Basis	Secret key secrecy	Private key secrecy
Break Resistance	Ciphertext + algorithm must not reveal key	Ciphertext + algorithm + one key must not reveal the other

Activity (3) - Group Discussion Question:

If you were designing a banking application, would you choose symmetric or public-key encryption? Raise your hand and explain your reasoning.

Homework Assignment 1 (Google Classroom):

Explain with a practical example how public key encryption solves the problem of key distribution in an insecure environment. Briefly compare this with symmetric encryption.

- **Requirements:**
  - Length: 200–300 words.
  - Format: Submit as Word or PDF file on Google Classroom.
  - Deadline: One week from the lecture date.