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 (2):

Mathematical Model and Applications of Public Key Encryption

Introduction

This lecture builds on the foundational concepts of public-key cryptography introduced earlier, focusing on its formal representation and the mechanisms that ensure confidentiality and authentication.
Students will examine the mathematical model of secrecy, where a plaintext message is transformed into ciphertext using the recipient's public key and then recovered using the corresponding private key.
The lecture also explores how the same key pair can support digital signatures, enabling message authentication and integrity verification.
Finally, we discuss the combined use of public and private keys to achieve both confidentiality and authentication, along with practical applications such as encryption/decryption, digital signatures, and secure key exchange.

Learning Outcomes

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

- **Explain the Mathematical Model of Secrecy:** Describe how plaintext is encrypted with a public key and decrypted with a private key, ensuring confidentiality against unauthorized access.
- **Demonstrate Digital Signature Mechanisms:** Illustrate how using a sender's private key for encryption provides authentication and verifies message integrity.
- **Analyze Dual-Use Encryption for Confidentiality and Authentication:** Evaluate how double encryption—first with the sender's private key and then with the receiver's public key—delivers both data secrecy and source verification.
- **Identify Key Applications:** Discuss major applications of public-key cryptosystems, including encryption/decryption, digital signatures, and session key exchange, and compare the roles of RSA, Elliptic Curve, Diffie–Hellman, and DSS algorithms.

Mathematical Representation of Data Privacy

To examine the core components of a public-key encryption system, consider the illustrated figure below.
Suppose a sender **A** creates a plaintext message $X=[X_1,X_{2...},X_M]$ where each X_M is a character from a finite alphabet.
The intended recipient **B** generates a corresponding key pair: a **public key (PU_b)** and a **private key (PR_b)**.
The private key remains known only to **B**, while the public key is openly available so that **A** can use it to encrypt the message.

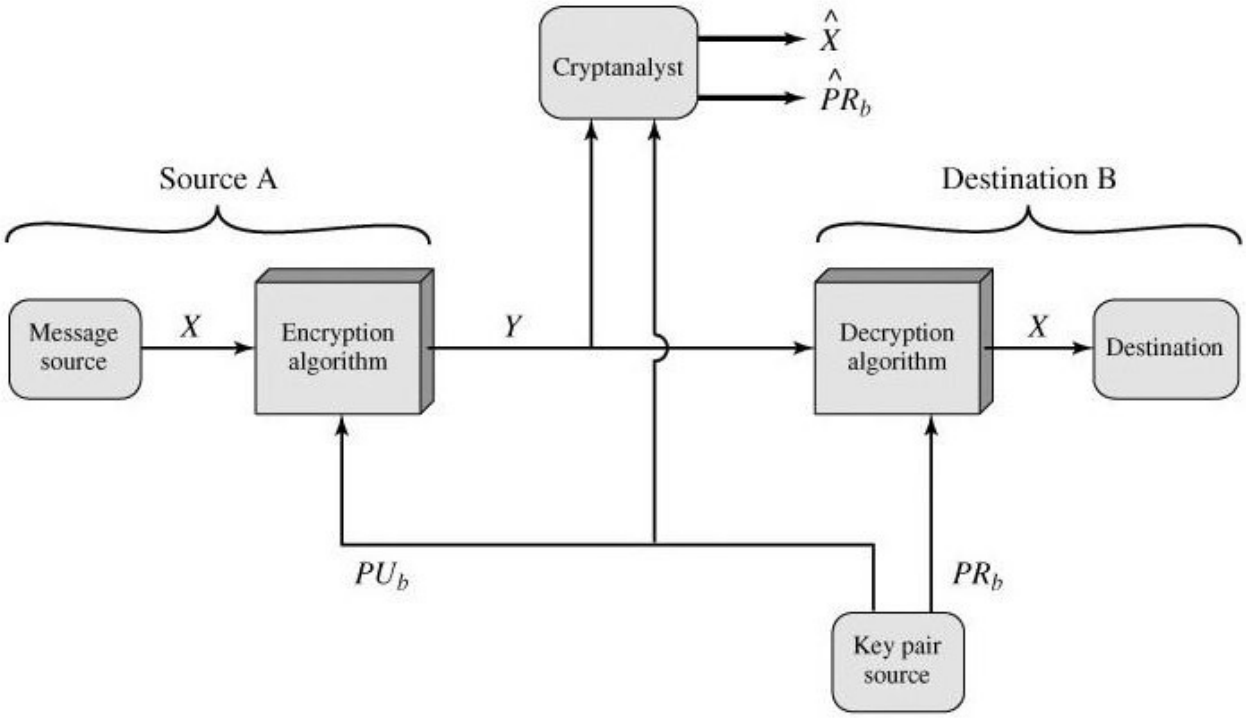

Figure (1): Public-Key Cryptosystem: Secrecy

With the message X and the encryption key PU_b as input, it forms the ciphertext $Y = [Y_1, Y_2,, Y_N]$:

$Y = E(PU_b, X)$

The intended receiver, in possession of the matching private key, is able to invert the transformation:

$X = D(PR_b, Y)$

An adversary, observing Y and having access to PU_b but not having access to PR_b or X, must attempt to recover X and/or PR_b. It is assumed that the adversary does have knowledge of the encryption (E) and decryption (D) algorithms. If the adversary is interested only in this particular message, then the focus of effort is to recover X, by generating a plaintext estimate ($\hat{X}$) often, however, the adversary is interested in being able to read future messages as well, in which case an attempt is made to recover PR_b by generating an estimate $(\hat{PR}_b)$.

We mentioned earlier that either of the two related keys can be used for encryption, with the other being used for decryption. This enables a rather different cryptographic scheme to be

implemented. Whereas the scheme illustrated in above Figure provides confidentiality, the figure below shows the use of public-key encryption to provide authentication:

$Y = E(PR_a, X)$

$X = D(PU_a, Y)$

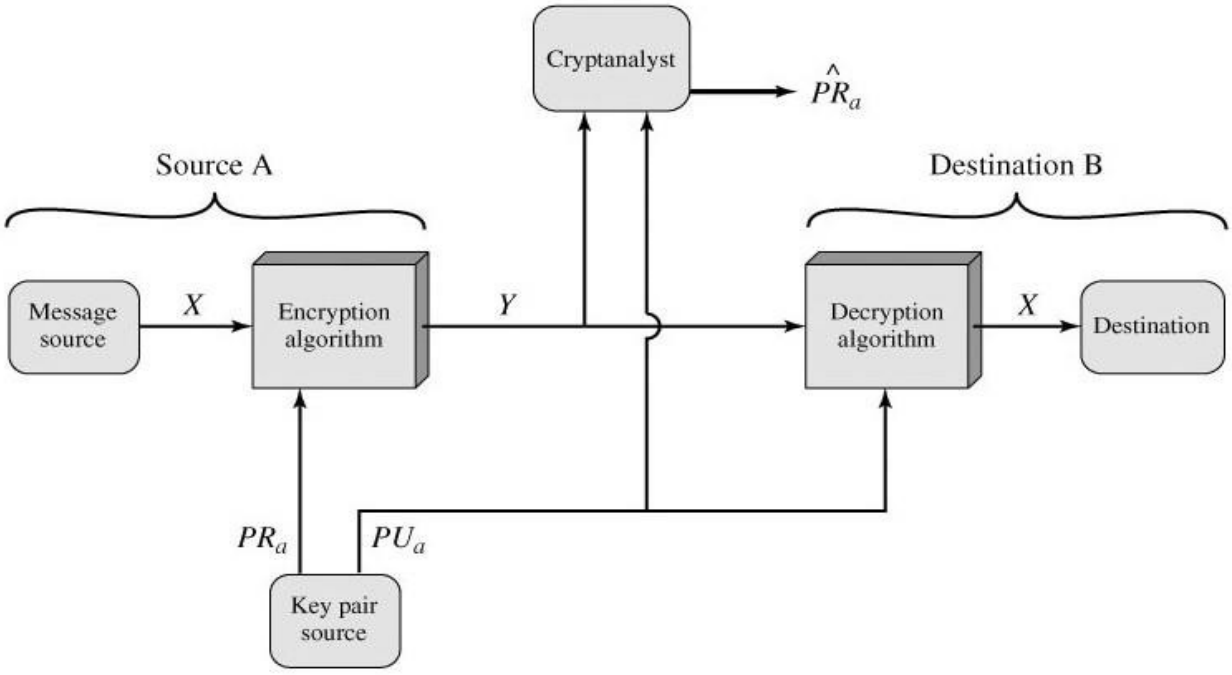

Figure (2): Public-Key Cryptosystem: Authentication

In this case, A prepares a message to B and encrypts it using A's private key before transmitting it. B can decrypt the message using A's public key. Because the message was encrypted using A's private key, only A could have prepared the message. Therefore, the entire encrypted message serves as a ***digital signature***. In addition, it is impossible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms of data integrity.

In the preceding scheme, the entire message is encrypted, which, although validating both author and contents, requires a great deal of storage. Each document must be kept in plaintext to be used for practical purposes. A copy also must be stored in ciphertext so that the origin and contents can be verified in case of a dispute. A more efficient way of achieving the same results is to encrypt a small block of bits that is a function of the document. Such a block, called an authenticator, must have the property that it is infeasible to change the document without changing the authenticator. If the authenticator is encrypted with the sender's private key, it serves as a signature that verifies origin, content, and sequencing.

It is important to emphasize that the encryption process depicted in the figure above does not provide confidentiality. That is, the message being sent is safe from alteration but not from eavesdropping. This is obvious in the case of a signature based on a portion of the message, because the rest of the message is transmitted in the clear. Even in the case of complete encryption, as shown in Figure (***Public-Key Cryptosystem: Authentication***), there is no protection of confidentiality because any observer can decrypt the message by using the sender's public key.

It is, however, possible to provide both the authentication function and confidentiality by a double use of the public-key scheme (*Public-Key Cryptosystem: Authentication and Secrecy*):

$$Z = E\,(PU_b\,,\,E\,(PR_a\,,\,X)\,)$$

$$X = D\,(Pu_a\,,\,D\,(PR_b\,,\,Z)\,)$$

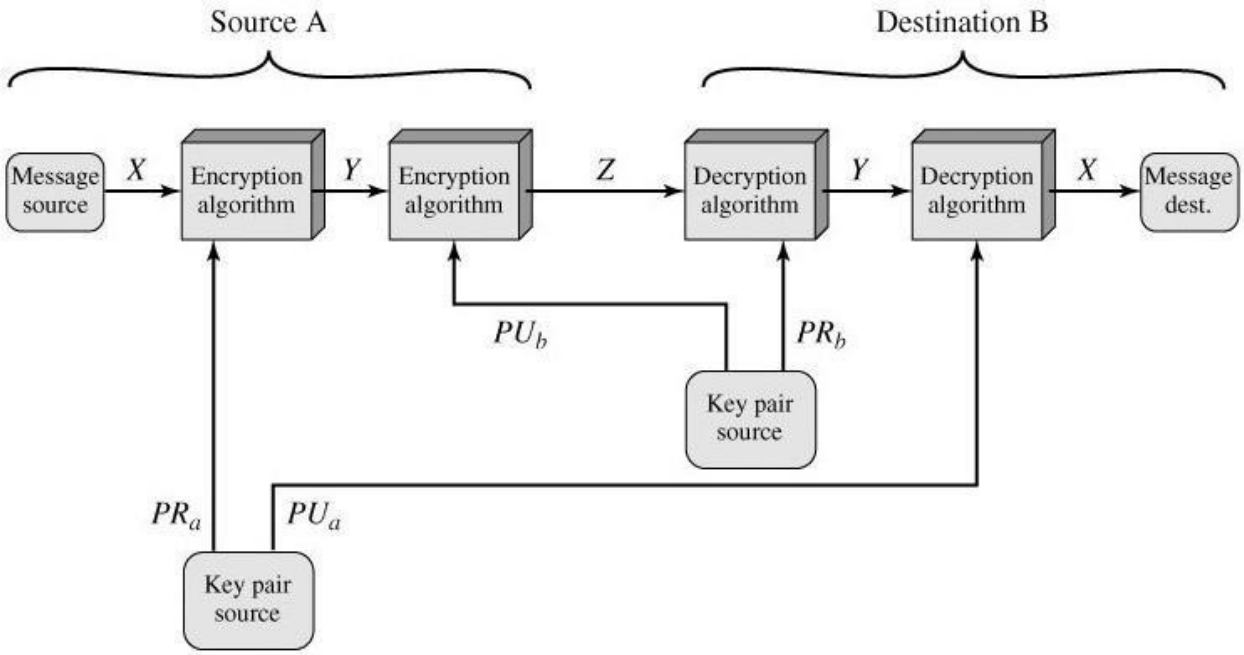

Figure (3): Public-Key Cryptosystem: Authentication and Secrecy

In this case, we begin as before by encrypting a message, using the sender's private key. This provides the digital signature. Next, we encrypt again, using the receiver's public key. The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided. The disadvantage of this approach is that the public-key algorithm, which is complex, must be exercised four times rather than two in each communication.

Applications for Public-Key Cryptosystems

Before proceeding, we need to clarify one aspect of public-key cryptosystems that is otherwise likely to lead to confusion. Public-key systems are characterized by the use of a cryptographic algorithm with two keys; one held private and one available publicly. Depending on the application, the sender uses either the sender's private key or the receiver's public key, or both, to perform some type of cryptographic function. In broad terms, we can classify the use of public-key cryptosystems into three categories:

- **Encryption/decryption**: The sender encrypts a message with the recipient's public key.
- **Digital signature:** The sender "signs" a message with its private key. Signing is

achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

- **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

Table1: Applications for Public-Key Cryptosystems

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

Encryption/Decryption: Indicates whether the algorithm can encrypt and decrypt data (i.e., convert plaintext to ciphertext and back).

- **Yes**: The algorithm supports secure message confidentiality.
- **No**: The algorithm is not designed to perform encryption tasks.

Digital Signature: Refers to the ability to sign data cryptographically to ensure authenticity, integrity, and non-repudiation.

- **Yes**: Can be used to sign digital messages or documents.
- **No**: Not applicable for signature operations.

Key Exchange: Indicates if the algorithm is used for securely exchanging cryptographic keys over an insecure channel.

- **Yes**: Supports secure key negotiation (e.g., generating a shared secret).
- **No**: Not suitable for this purpose.

Homework Assignment 2 (google classroom):

Explain how double encryption in a public-key cryptosystem can achieve both authentication and confidentiality. Use a simple example to illustrate your answer, and mention one drawback of this approach.

Instructions:

- Write **200–300 words**.
- Submit your answer as a **Word or PDF** file via Google Classroom.
- **Deadline:** One week after the lecture.

Evaluation Criteria:

1. Clarity in describing encryption and decryption order.
2. Correct identification of both authentication and confidentiality roles.
3. Logical explanation of efficiency drawbacks and practical implications.