ROYAL UNIVERSITY
OF PHNOM PENH

IC: Chapter 3d

Public-Key Cryptography and Message Authentication

Public-Key Cryptography Principles and Digital Signature

07 May 2021

by Chap Chanpiseth, Dr. Srun Sovila

Outline

1) Public-Key Encryption Structure
2) Application for Public-Key Cryptosystems
3) Requirements for Public-Key Cryptosystems
4) Other Public-Key Cryptography Algorithm
5) Digital Signature

Public-Key Cryptography Principles Overview

- Public-key encryption is as important as conventional encryption which is used ***in message authentication and key distribution***.
- **RSA and Diffie-Hellman are t**he two most used public-key algorithms
- Conventional encryption are cryptographic systems which uses ***same key*** used by sender to encrypt message and by receiver to decrypt message.

Public-Key Encryption Structure

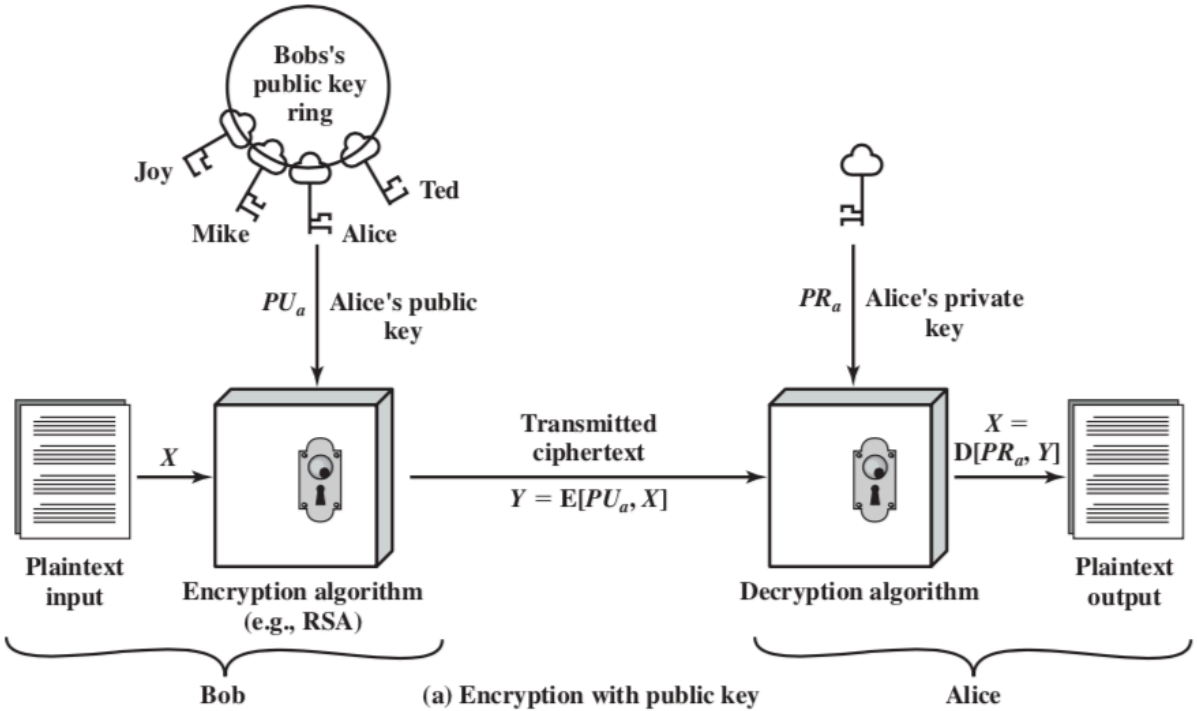
- Public-key encryption 1st publicly proposed by Diffie and Hellman in 1976 [DIFF76]
- The 1st truly revolutionary advance in encryption in literally thousands of years.
- Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns, such as are used in symmetric encryption algorithms.
- Public-key cryptography is asymmetric: the use of two separate keys
- The use of two keys are used in the areas of
    1) Confidentiality,
    2) Key distribution and
    3) Authentication.

Public-Key Encryption Structure (Cont.)

Several common misconceptions concerning public-key encryption

1) Public-key encryption is considered to be more secure from cryptanalysis than conventional encryption. *=> The security of encryption scheme: (1) the length of the key and (2) the computational work to break a cipher.*
2) Public-key encryption is a general-purpose technique that has made conventional encryption obsolete. *=> Due to computational overhead of public encryption, therefore no foreseeable likelihood that conventional encryption will be abandoned.*
3) Key distribution using public-key encryption is considered trivial, compared to the rather cumbersome handshaking involved with key distribution centers for conventional encryption. *=> Some form of protocol often involves a central agent, and the processes are no simpler or any more efficient than those required for conventional encryption.*

Public-Key Encryption Structure (Cont.)



Public-Key Encryption Structure (Cont.)

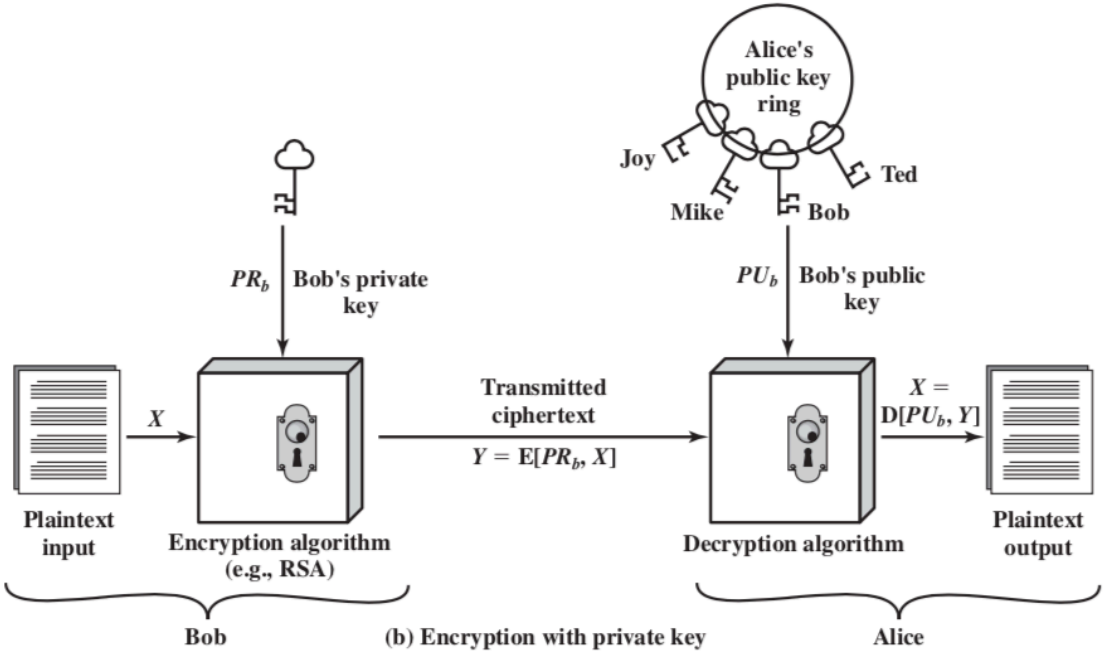


Figure 3.9 Public-Key Cryptography

Public-Key Encryption Structure (Cont.)

The public key of the pair is made public for others to use

- The private key is known only to its owner.

A general-purpose public-key cryptographic algorithm relies on

- One key for encryption and
- Another related key for decryption.

Public-Key Encryption Structure (End)

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 ***the public key*** in a public register or other accessible file.
   - The companion key is kept private.
   - Each user maintains a collection of public keys obtained from others.
3) If Bob wishes to send a private message to Alice
   - Bob encrypts the message using Alice's public key.
   - Upon receiving the message, Alice decrypts it using her private key.
   - No other recipient can decrypt the message because only Alice knows Alice's private key.

Application for Public-Key Cryptosystems

- Public-key systems are characterized by the use of a cryptographic type of algorithm with two keys, one held private and one available publicly.
- Depending on the application, the sender uses either the sender's private key, the receiver's public key, or both to perform some type of cryptographic function.
- The public-key cryptosystems could be classified into ***three categories:***
  1) ***Encryption/Decryption:*** The sender encrypts a message with the recipient's public key.
  2) ***Digital Signatures:*** 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.
  3) ***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.

Application for Public-Key Cryptosystems (Cont.)

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

Table 1: Applications for Public-Key Cryptosystems

- Some public-key algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications.
- The Digital Signature Standard (DSS) and elliptic-curve cryptography will be briefly discussed in the next few slides.

Requirements for Public-Key Cryptosystems

A public-key cryptosystem depends on a cryptographic algorithm based on two related keys.

Diffie and Hellman lay out the conditions that such algorithms must fulfil

1) It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
2) It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext: $C = E(PU_b, M)$
3) It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$
4) It is computationally infeasible for an opponent, knowing the public key, PU_b, to determine the private key, PR_b.
5) It is computationally infeasible for an opponent, knowing the public key, PU_b, and a ciphertext, C, to recover the original message, M.
6) Either of the two related keys can be used for encryption, with the other used for decryption.
   - $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b,M)]$ =>*This requirement is useful but not necessary.*

Public-Key Cryptography Algorithms

- The RSA scheme is one of the most widely used approach to public-key encryption.
- RSA is a block cipher
  - The plaintext and ciphertext are integers between 0 and n - 1 for some n.

Encryption and decryption are of the following form period for

- Some plaintext block M and ciphertext block C:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

- Both sender and receiver must know the values of ***n and e***,
- and only the receiver knows the value of ***d***.

Public-Key Cryptography Algorithms (Cont.)

This is a public-key encryption algorithm with

- A public key of $KU = \{e, n\}$ and
- A private key of $KR = \{d, n\}$.

For this algorithm to be satisfactory for public-key encryption, the following requirements

1) It is possible to find values of **e, d, n** such that $M^{ed} \bmod n = M \; for \; all \; M < n$.
2) It is relatively easy to calculate $M^e \; and \; C^d \; for \; all \; values \; of \; M < n$.
3) It is infeasible to determine $d \; given \; e \; and \; n$.

Public-Key Cryptography Algorithms (Cont.)

Key Generation

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	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

Fig. 5: The RSA Algorithm

Other Public-Key Cryptography Algorithm

Two other public-key algorithms have found commercial acceptance: DSS and ECC

1) Digital Signature Standard

- The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS PUB 186, known as the DSS.
- The DSS makes use of the SHA-1 and presents a new digital signature technique, the Digital Signature Algorithm (DSA).
- Due to public feedback concerning the security of the scheme, the DSS was originally proposed in 1991 and revised in 1993, then a further minor revision in 1996.
- The DSS uses an algorithm that is designed to provide only the digital signature function.
- Unlike RSA, it cannot be used for encryption or key exchange.

Other Public-Key Cryptography Algorithm

2) Elliptic Curve Cryptography

- The vast majority of the products and standards that use public-key cryptography for encryption and digital signatures use RSA.
- The bit length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA.
- This burden has ramifications, especially for e-commerce sites that conduct large numbers of secure transactions.
- Recently, a competing system has begun to challenge RSA: elliptic curve cryptography (ECC).
- Already, ECC is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography.
- The principal attraction of ECC compared to RSA is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.

Digital Signature

A digital signature is a mathematical scheme used to validate *the authenticity and integrity* of a message, software or digital document.

- It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.

Digital Signature: Scenario 1

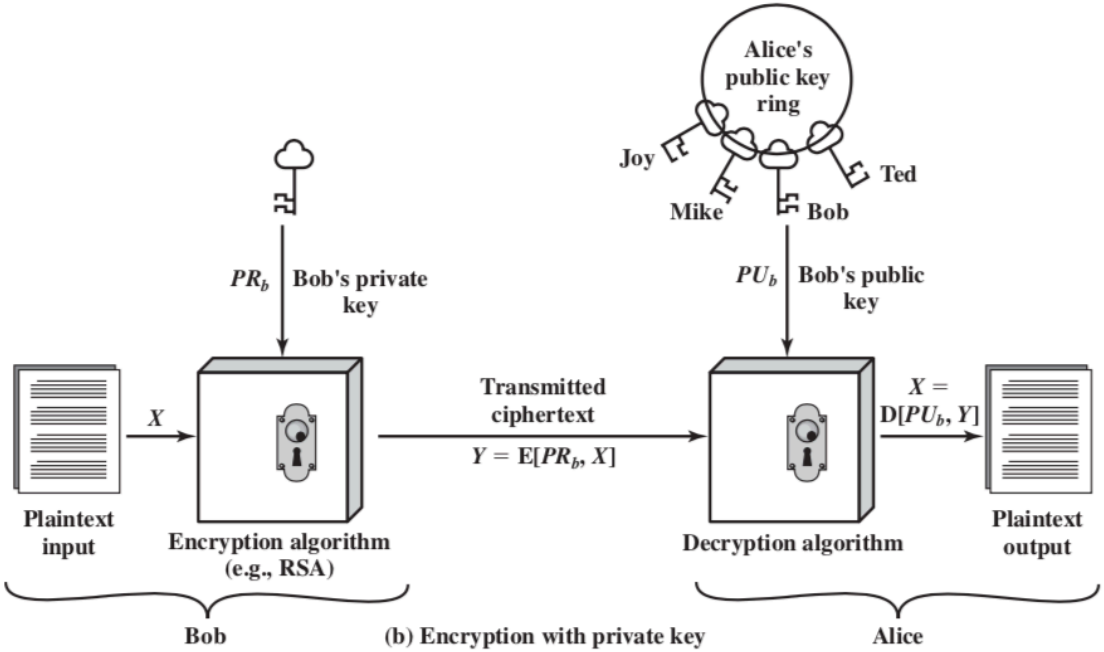


Figure 3.9 Public-Key Cryptography

Digital Signature: Scenario 1

Suppose that Bob wants to send a message to Alice

- Message confidentiality is not important
- Bob wants Alice to be certain that the message is indeed from him.
- In this case, Bob uses his own ***private key to encrypt*** the message.
- Upon receipt the ciphertext, Alice finds that she can decrypt it with Bob's public key

- Thus proving that the message must have been encrypted by Bob.
- No one else has Bob's private key, and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key.

Therefore, the entire encrypted message serves as a **digital signature**.

Digital Signature: Scenario 1 (End)

- In this scheme, the entire message is encrypted.
- Although validating both author and contents, this 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.

Digital Signature: Scenario 2

- 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***.
- A secure hash code such as SHA-1 can serve this function.

Digital Signature: Scenario 2

- Sender's private key is used to encrypt the hash code in order to generate digital signature

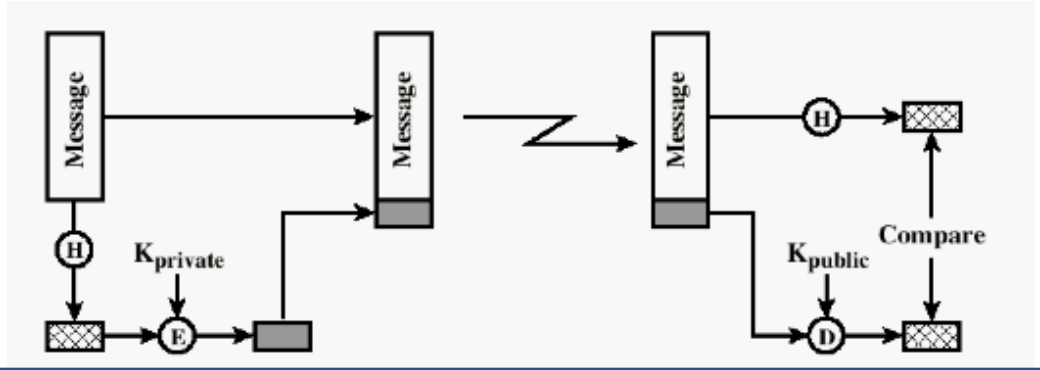
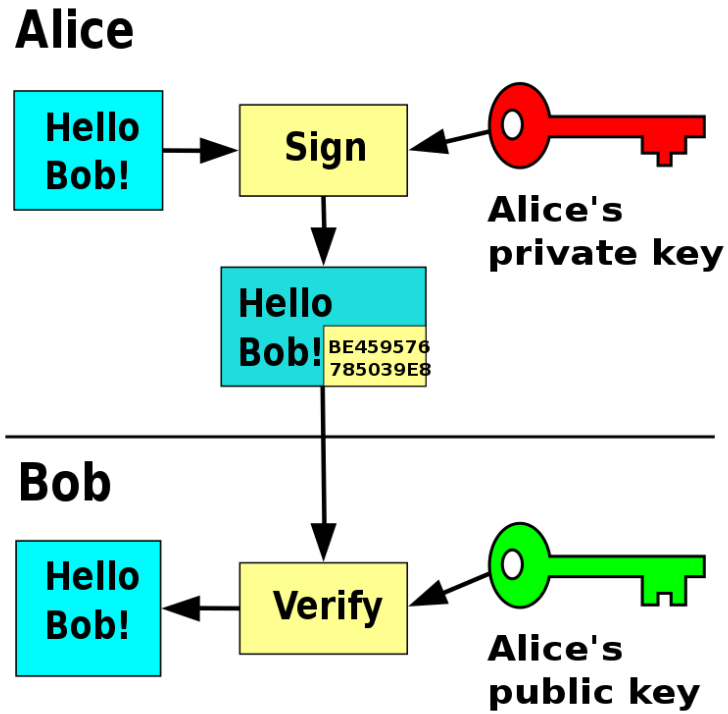


Figure 4. Using public-key encryption

Digital Signature: Scenario 2

- Alice signs a message: “Hello Bob!”
  - by appending to the original message a version encrypted with her private key.
- Bob receives both the message and signature.
  - Bob uses Alice's public key to verify the authenticity of the message, i.e. that the message decrypted using the public key, exactly matches the original message.



Note for Digital Signature

- It is important to emphasize that the encryption process just described does not provide confidentiality.
- That is, the message being sent is safe from alteration but not safe 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, there is no protection of confidentiality because any observer can decrypt the message by using the sender's public key.

References

Network Security Essentials: Applications and Standards, 4th Edition by William Stallings

Introduction to Cryptography with Coding Theory (2nd Edition) by Wade Trappe Lawrence C. Washington(2005-07-25)

Thanks for your attention !