

CONVENTIONAL AND PUBLIC-KEY ENCRYPTION

Conventional Encryption	Public-Key Encryption
Needed to Work:	Needed to Work:
1. The same algorithm with the same key is used for encryption and decryption	1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption
2. The sender and receiver must share the algorithm and the key.	2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security:	Needed for Security:
1. The key must be kept secret.	1. One of the two keys must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.	2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key

PUBLIC-KEY CRYPTOSYSTEM: SECRECY

There is some source A that produces a message in plaintext, $X = [X_1, X_2, \dots, X_M]$. The M elements of X are letters in some finite alphabet. The message is intended for destination B. B generates a related pair of keys: a public key, PUB, and a private key, PRb. PRb is known only to B, whereas PUB is publicly available and therefore accessible by A. With the message X and the encryption key PUB as input, A forms the ciphertext

$$Y = [Y_1, Y_2, \dots, Y_N]: Y = E(\text{PUB}, X)$$

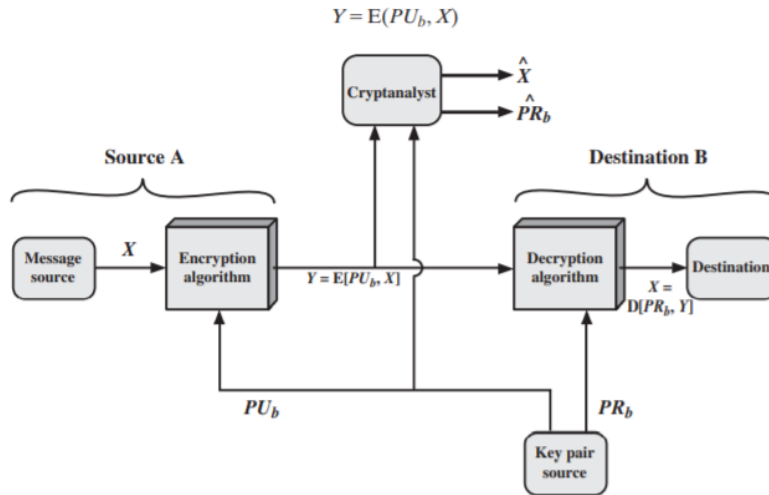


Figure 9.2 Public-Key Cryptosystem: Secrecy

Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

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 .

PUBLIC-KEY CRYPTOSYSTEM: AUTHENTICATION

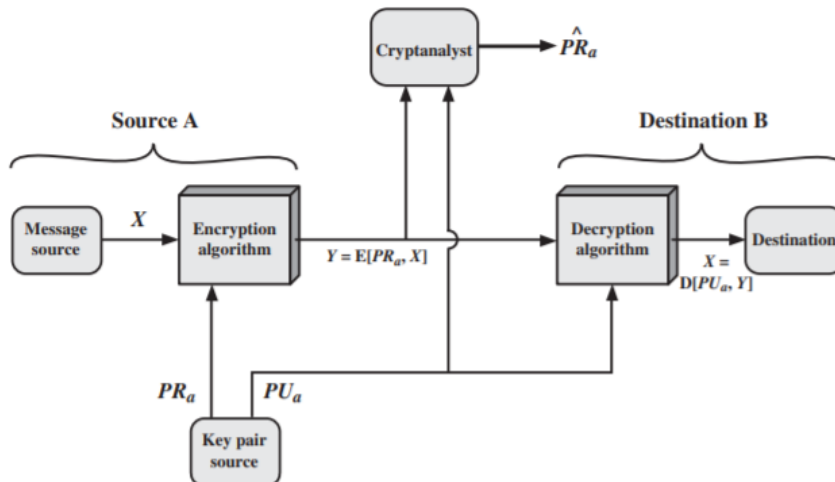


Figure 9.3 Public-Key Cryptosystem: Authentication

Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

the scheme illustrated in the above Figure provides confidentiality to provide authentication:

$$Y = E(PR_a, X) \quad X = D(PU_a, Y)$$

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.

PUBLIC-KEY CRYPTOSYSTEM: AUTHENTICATION AND SECRECY

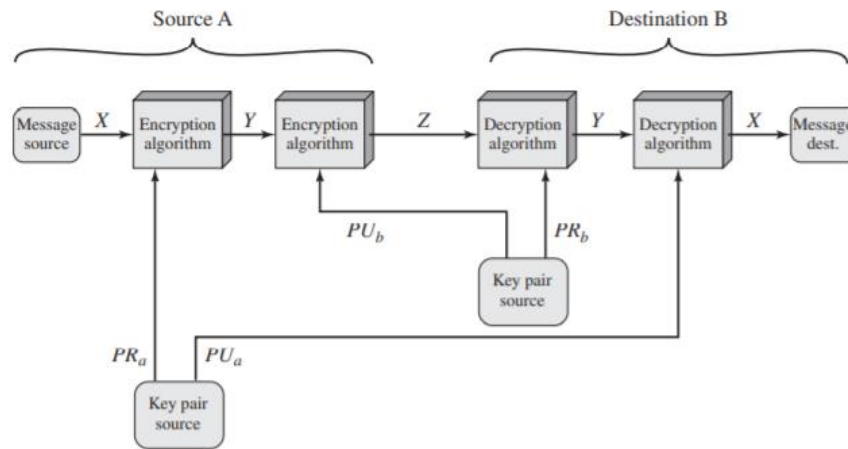


Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy

Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

It is, however, possible to provide both the authentication function and confidentiality by a double use of the public-key scheme :

$$Z = E(PU_b, E(PR_a, X)) \quad X = D(PU_a, D(PR_b, Z))$$

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

- 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.

APPLICATIONS FOR PUBLIC-KEY CRYPTOSYSTEMS

- Some algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications.
- Table indicates the applications supported by the algorithms.

Table 9.3 Applications for Public-Key Cryptosystems

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

Reference :William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006

REQUIREMENTS FOR PUBLIC-KEY CRYPTOGRAPHY

1. It is computationally easy for a party B to generate a pair (public key PUB, private key PRb).
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: $C = E(\text{Pub}, M)$
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M = D(\text{PRb}, C) = D[\text{PRb}, E(\text{Pub}, M)]$
4. It is computationally infeasible for an adversary, knowing the public key, PUB, to determine the private key, PRb.
5. It is computationally infeasible for an adversary, knowing the public key, PUB, and a ciphertext, C, to recover the original message, M. We can add a sixth requirement that, although useful, is not necessary for all public-key applications:
6. The two keys can be applied in either order: $M = D[\text{Pub}, E(\text{PRb}, M)] = D[\text{PRb}, E(\text{Pub}, M)]$

PUBLIC-KEY CRYPTANALYSIS

- A public-key encryption scheme is vulnerable to a brute-force attack. The countermeasure is the same: Use large keys

- Another form of attack is to find some way to compute the private key given the public key
- There is a form of attack that is peculiar to public-key systems. This is, in essence, a probable-message attack

