Public Key Cryptography

The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography.

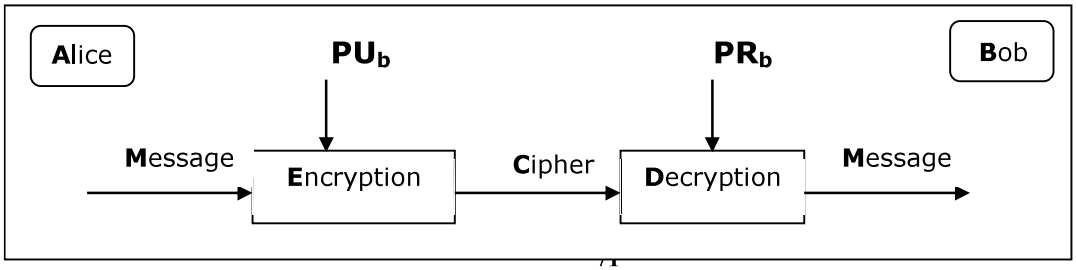
Asymmetric Cryptography (also called Public-Key Cryptography) was a real breakthrough in cryptography. The major change between asymmetric cryptography and the 'traditional' symmetric cryptography is that, in asymmetric cryptography, the key for the encryption is not the same as the key for the decryption. Each user has 2 keys: a Public Key, which is known to all, and a Private Key, which is kept secret (private). Denote Bob's public key by PU(B), and denote Bob's private key by PR(B).

Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of ***confidentiality***, ***key distribution***, and ***authentication***

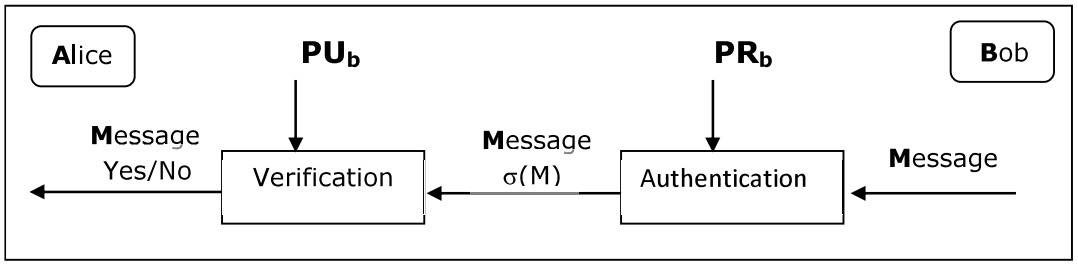
The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. ***The first problem*** is that of key distribution. Key distribution under symmetric encryption requires either (1) that two communicants already share a key, which somehow has been distributed to them; or (2) the use of a key distribution center.

The second is the authentication the way that identifies the sender.

The first use of public key cryptography is for encrypting messages to Bob. Anyone who wishes to send an encrypted message to Bob will use Bob's public key. To decrypt the message, Bob's private key is needed, and only Bob knows it.

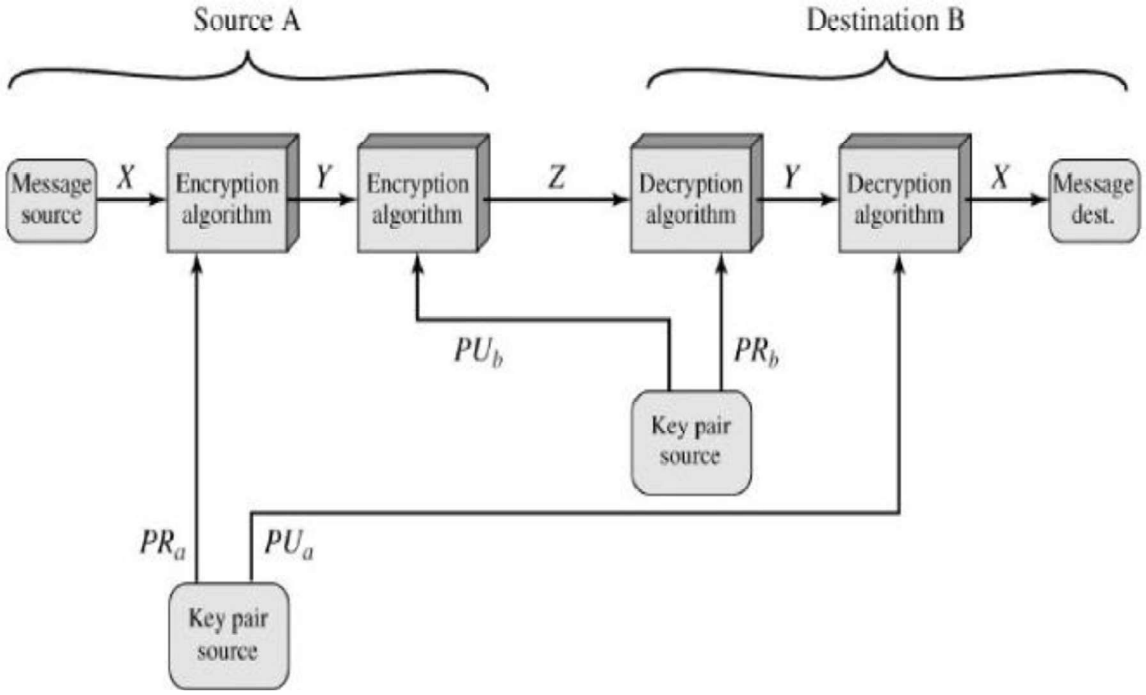


The second use of public key cryptography is for message signing by Bob. Bob's private key is used by Bob to generate a signature. Any one is able to verify Bob's signature using Bob's public key. Denote the signature of the message M by σ(M).



The encryption (or verification) algorithm and the decryption (or authentication) algorithms may or may not be the same.

However, it is possible to provide both the **authentication** function and **confidentiality** by a double use of the public-key scheme.



History of Public Key Cryptography

1976 – Diffie & Hellman published an article 'Public Key Cryptography' that presented the model. They got a patent but never used it to license the technology. They also came up with a protocol for a Key Exchange protocol based on their method.

1977 – Rivest, Shamir, and Adleman invented the RSA scheme which provides Encryption, Signature, and Key Exchange. RSA became the most popular method for public key cryptography.

Since – Many other methods implemented the public key model. For example:
El Gamal – Encryption, Signature, and Key Exchange (developed by El Gamal).
DSS – Digital Signature Standard (developed by NIST).
DH – Key exchange (developed by Diffie and Hellman).

The table below summarizes some of the important aspects of symmetric (Private-Key Cryptography) and public-key encryption. To discriminate between the two, we refer to the key used in symmetric encryption as a secret key (Private-Key Cryptography) and asymmetric (Public-Key Cryptography)

Private-Key Cryptography	Public-Key Cryptography
• The same algorithm with the same key is used for encryption and decryption • Key is shared by both sender and receiver • Also known as symmetric, both parties are equal • Provide **secrecy** • For example DES cipher algorithm.	• One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. • sender and receiver used different keys • Asymmetric since parties are not equal • Provide **secrecy**, **authentication** and **session keys**. • For example RSA cipher algorithm.