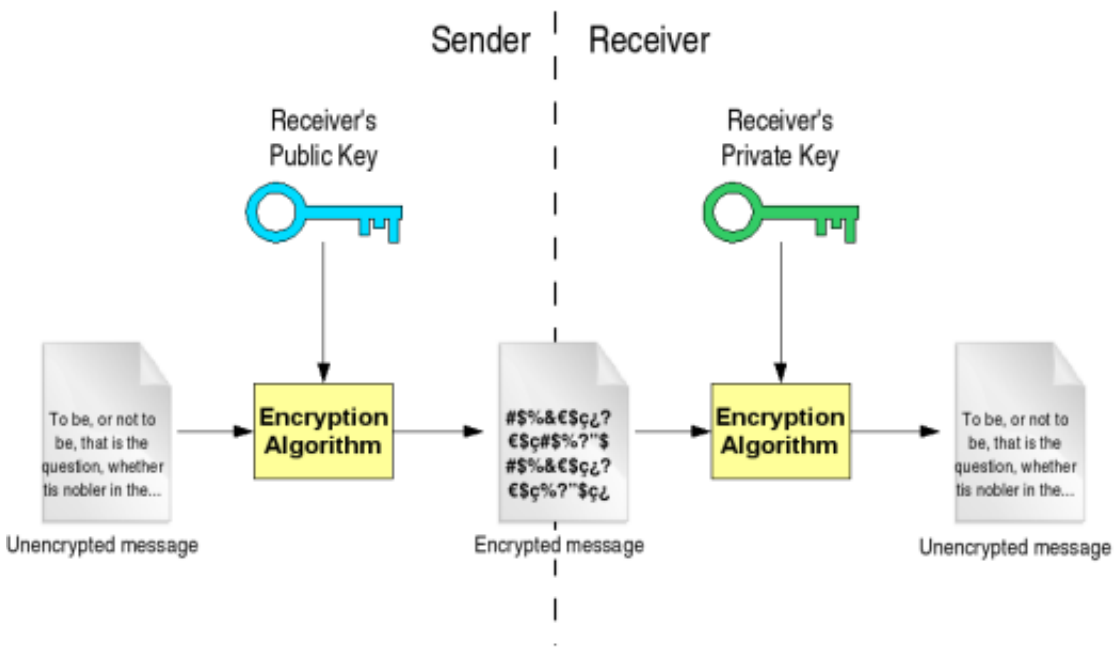
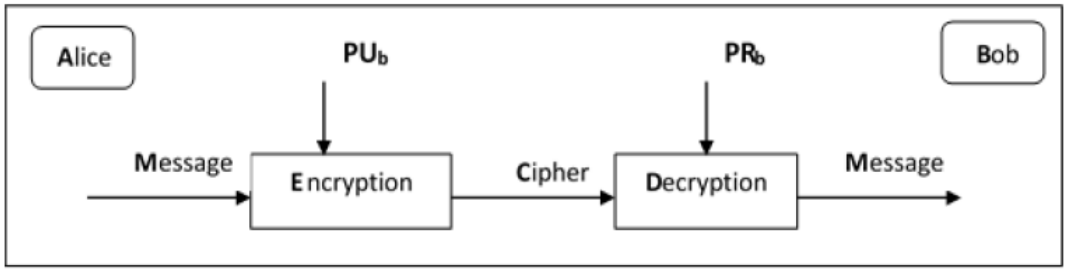
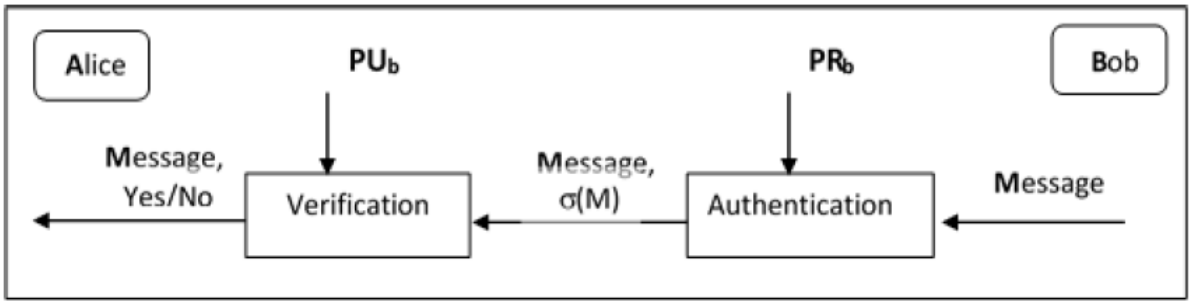
Public Key Cryptography

Asymmetric Cryptography (alsocalledPublicKeyCryptography) was a real breakthrough in cryptography. 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). The use of two keys has profound consequences in the areas of confidentiality, keydistribution, and authentication.





confidentiality



authentication.

Symmetric Cryptography		Asymmetric Cryptography	
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	Key is shared by both sender and receiver	**2**	sender and receiver used different keys
3	Also known as Private-Key Cryptography symmetric, both parties are equal	**3**	Asymmetric cryptography also known as Public-Key since parties are not equal
4	Provide confidentiality	**4**	Provide confidentiality , authentication and key distribution .
5	For example DES cipher algorithm.	**5**	For example RSA cipher algorithm.

Applications for Public-Key

Cryptosystems 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

Table 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

RSA ALGORITHM

(Rivest, Shamir, Adelman)

The RSA algorithm was developed by three professors at MIT in 1977, Ron Rivest, Adi Shamir, and Leonard Adlemen, their initials give the algorithm its name. This was one of the RSA algorithms (mathematical processes) to implement the concept of public-key cryptography. The actual concept of public-key cryptography was discovered by Whitfield Diffie and Martin Hellman just one year earlier. Die and Hellman had devised a method that would allow the key to the cryptographic system to be known publicly but still have the system be a secure way to send messages. What they did not know was how to mathematically create one.

Rivest, Shamir and Adlemen took the concept of Diffie and Hellman and devised a method that uses what is known as a one-way function. A one-way function is a mathematical process that is easy to do one way but is difficult to reverse. For example, it is easy to multiply two numbers together but it is much more difficult to factor a number. This is precisely why the RSA algorithm works. Your computer can multiply two 300 digit numbers together in an extremely small fraction of a second but if you ask your computer to factor a 600 digit number that is the product of two 300 digit primes you will be waiting a long time for the result. In fact, it would take the fastest supercomputer on Earth several billion years to factor the number.

Operation of the RSA algorithm

- Key generation
- Encryption process
- Decryption process

1. ***Key generation***

- ***Primes:*** Choose 2 distinct random prime numbers : p; q
- ***Modulus:*** Compute n = p * q
- ***Predecessors***: Compute multiply their φ = (p-1) *(q-1)
- ***Public exponent:*** Choose an integer e, such that 1 < e < φ must be prime number
- ***Private exponent:*** Compute $d = e^{-1} \bmod \varphi$
  In other form can compute d as [e * d mod φ = 1]
- Publish the public encryption key : (e; n)
- Keep secret private decryption key : (d; n)

2. ***Encryption process***

$$\mathbf{C = m^e \bmod n}$$

3. ***Decryption process***

$$\mathbf{M = c^d \bmod n}$$

m = Plaintext or message

C = Ciphertext

Example 1

If the prime numbers 5, 11 are selected for p, q respectively. Find the private key and public key.

Answer

Primes: *p = 5, q = 11*

Modulus: *n = p * q = 55*

Predecessors: *φ = (p-1)* (q-1) = 4 * 10 = 40

Public exponent: *e = 3*

Private exponent: 3*d mod 40 = 1

d = 7

Example 2

If two prime numbers are selected 3, 11 for p and q respectively. How can get private and public keys to use them for encipher the message "2 4 5 7".

Answer

Step1: Keys generation

- *Primes:* P = 3 q=11
- *Modulus:* n = p * q = 3 * 11 = 33
- φ = (p-1) (q-1) = (3-1) (11-1) = (2) (10) = 20
- *Public exponent:* Choose e = 7
- *Private exponent:* $d = e^{-1} \bmod \varphi$

  Choose (d * e) mod φ =1

  d = 3

Step 2: **Encryption process**

To encrypt a message the sender has to:

- Obtain public key of recipient (e; n)
- Represent the message as an integer m in [0; n-1]
- Compute: $c = m^e \bmod n$

$C = m^e \bmod n$

$m = 2$

$C = 2^7 \bmod 33 = 29$

And so on for all other numbers (4, 5 , 7) in the same way.

Step3: Decryption process

To decrypt the ciphertext c the recipient:

- Uses his private key (d; n)
- Computes: m = cd mod n

$m = c^d \bmod n$

$29^3 \bmod 33 = 2$