Cryptography

Terminologies

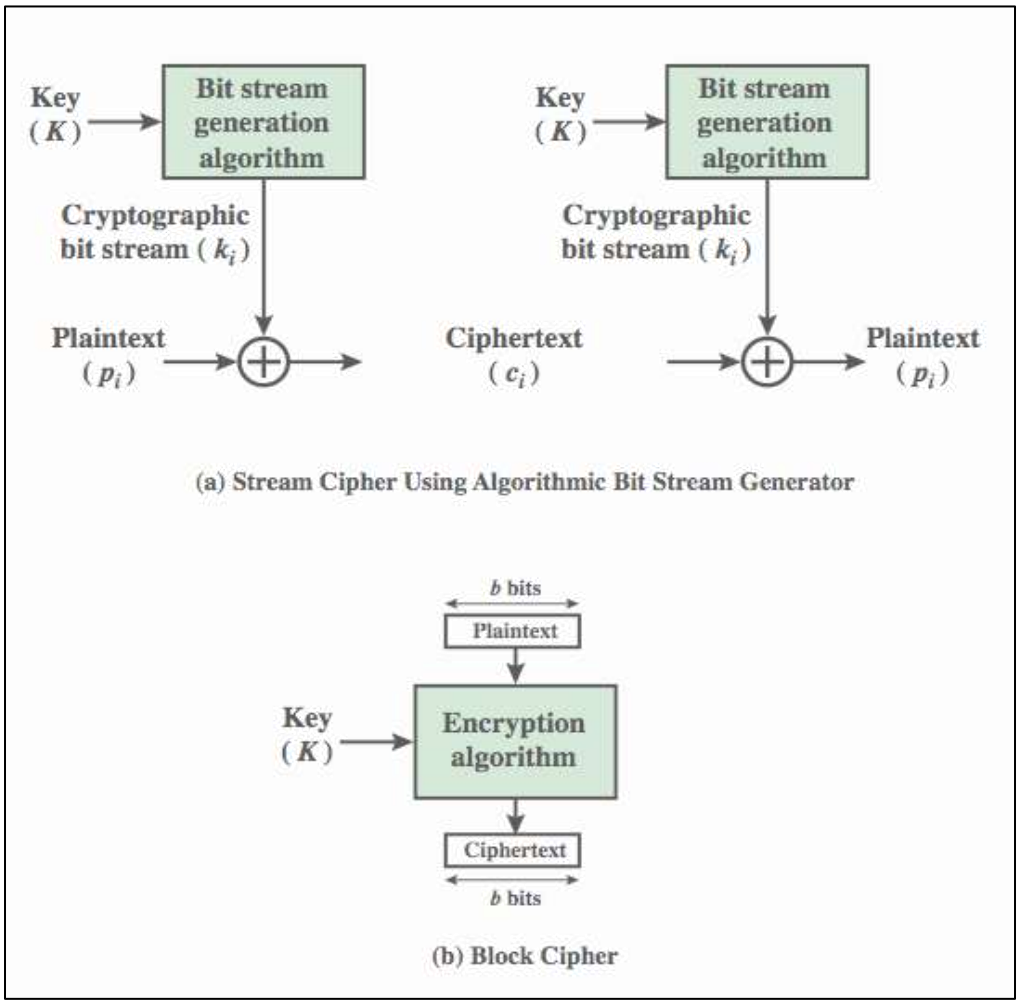
- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (codebreaking) - study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - field of both cryptography and cryptanalysis

Different Cryptographic Systems

Cryptographic system can be characterized by:

- **Type of encryption operations used**
  - **Substitution**: Substitution cipher is a data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols.
  - **Transposition**: Transposition cipher is a simple data encryption scheme in which plaintext characters are shifted in some regular pattern to form ciphertext.
  - **Product**: Product cipher is the data encryption scheme in which the ciphertext produced by encrypting a plaintext document is subjected to further encryption. By combining two or more simple transposition ciphers or substitution ciphers, a more secure encryption may result.
- **Number of keys used**
  - **Single-key/ Private key/ Symmetric key**: In the Private key approach, the same key is used for encryption and decryption.
  - **Two-key/ Public key/ Asymmetric key**: In a Public key approach, two keys are used; one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.
- **Way in which plaintext is processed**
  - **Block**: A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically, a block size of 64 or 128 bits is used.

- **Stream**: A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.



Symmetric Encryption

Symmetric encryption is also known as conventional/ private-key/ single-key encryption. Here, sender and receiver share a common key. All classical encryption algorithms are private-key approach. This was only type prior to invention of public-key in 1970's and by far most widely used.

There are two requirements for secure use of symmetric encryption:

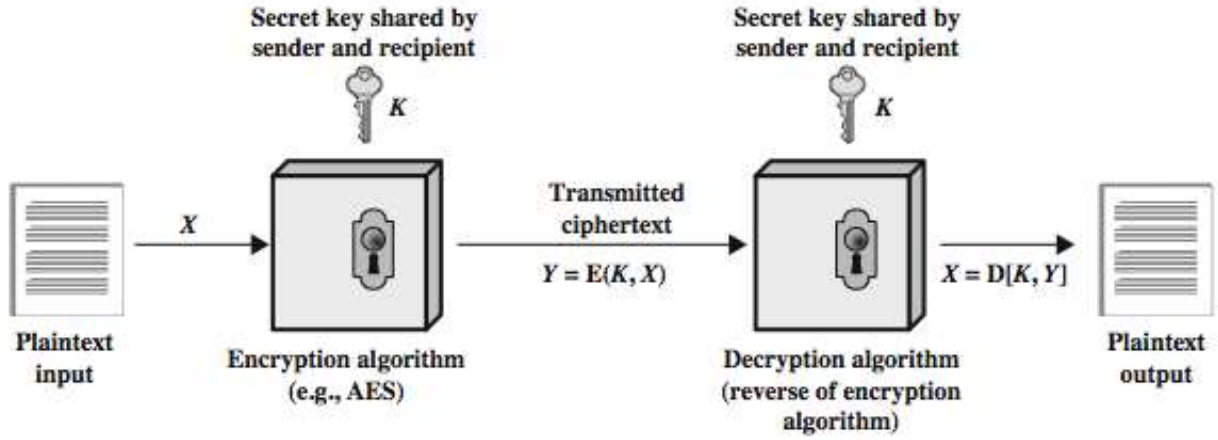
- a strong encryption algorithm
- a secret key known only to sender / receiver

Mathematically,

$Y = E(K, X)$

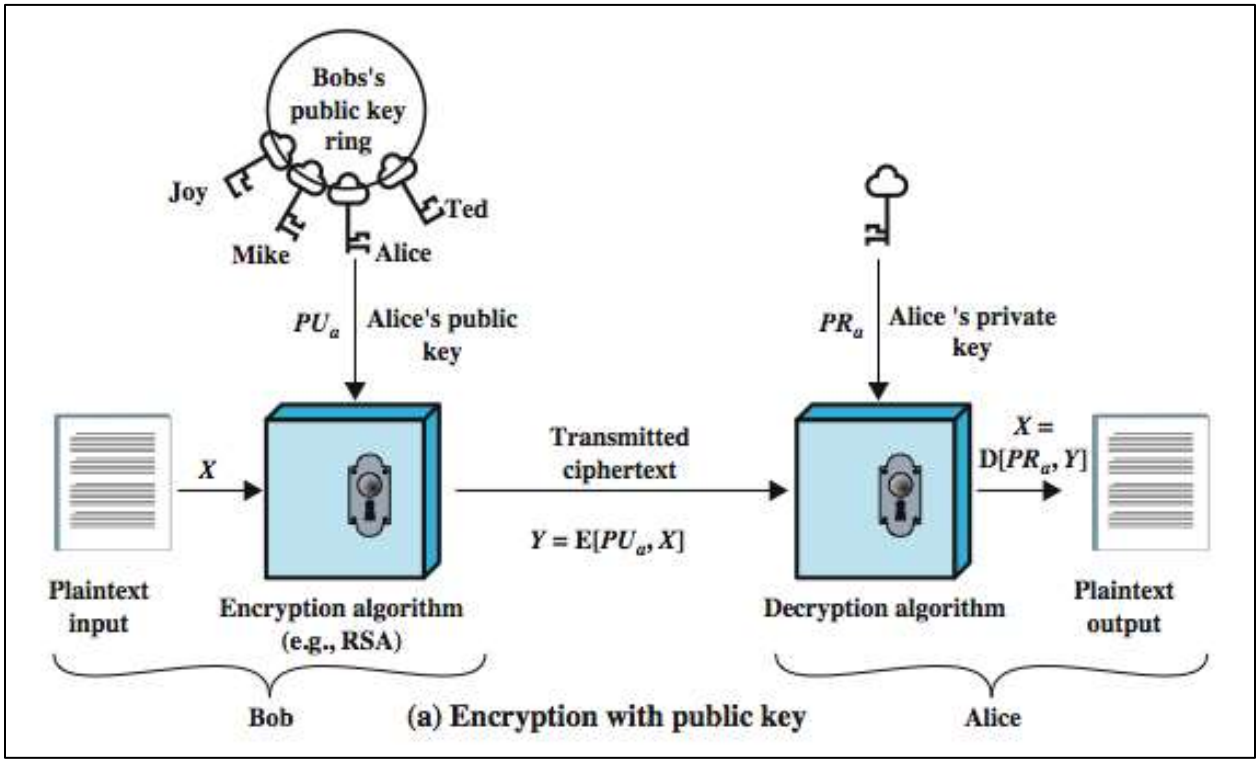
$X = D(K, Y)$

assuming encryption algorithm is known and implying a secure channel to distribute key.



Public Key Cryptography

Traditional **private/secret/single key** cryptography uses **one** key that is shared by both sender and receiver. If this key is disclosed, communications are compromised. Public key cryptography uses **two** keys – a public & a private key. It uses clever application of number theoretic concepts to function. The approach complements **rather than** replaces private key cryptography.



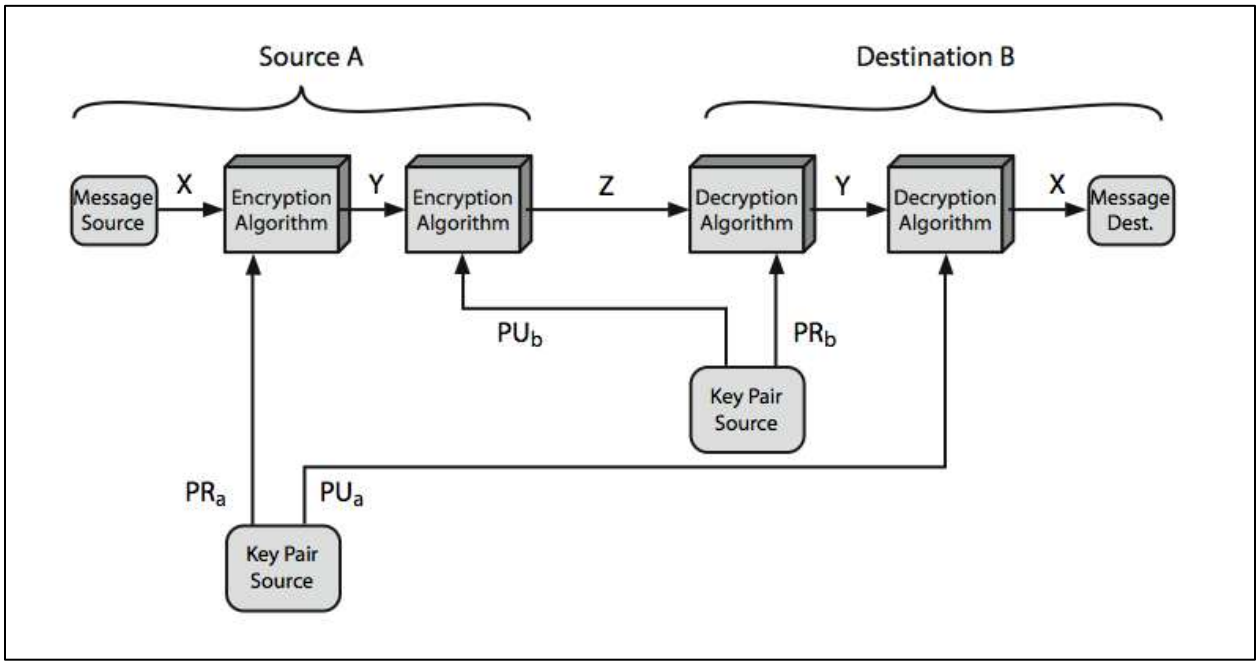
Public key cryptography was developed to address two key issues:

- **key distribution** – how to have secure communications in general without having to trust a KDC with your key
- **digital signatures** – how to verify a message comes intact from the claimed sender

Public-key/two-key/asymmetric cryptography involves the use of **two** keys:

- a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
- a related **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**

It is **asymmetric** because those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures.



Feistel Cipher Structure

Most **symmetric block** encryption algorithms in current use are based on a structure referred to as a Feistel block cipher. A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits.

Feistel's method (developed in 1973) is a practical application of Claude Shannon's proposal in 1945 to alternate **confusion** and **diffusion** functions in the product cipher. It is worth It is worth commenting that modern symmetric cipher is based on Feistel's structure which in turn is developed on Claude Shannon's suggestions. Thus, today's wide used symmetric encryption is dated back to more than half a century. In particular, Feistel proposed the use of a cipher that alternates substitutions and permutations. The terms **diffusion** and **confusion** were introduced by Claude Shannon to capture the two basic building blocks for

any cryptographic system. Shannon's concern was to thwart cryptanalysis based on statistical analysis. Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key. **The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible** in order to thwart attempts to deduce the key. **Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key** as complex as possible, again to thwart attempts to discover the key. So successful are diffusion and confusion in capturing the essence of the desired attributes of a block cipher that they have become the cornerstone of modern block cipher design.

The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- **block size** - increasing size improves security, but slows cipher
- **key size** - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds** - increasing number improves security, but slows cipher
- **subkey generation algorithm** - greater complexity can make analysis harder, but slows cipher
- **round function** - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption** - more recent concern for practical use
- **ease of analysis** - for easier validation & testing of strength

Cryptanalysis

Cryptanalysis is a process of finding vulnerabilities in cryptographic algorithms and using these weaknesses to decipher the ciphertext without knowing the secret key (instance deduction). Sometimes the weakness is not in the cryptographic algorithm itself, but rather in how it is applied that makes cryptanalysis successful. There are two general approaches, they are Cryptanalytic Attack and Brute Force Attack.

Cryptanalytic Attack

- ✓ **Cypher Text Only Attack**: In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success
- ✓ **Known Plaintext Attack**: The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further

secret information such as secret keys and code books. The term "crib" originated at Bletchley Park, the British World War II decryption operation.

- ✓ **Chosen Plaintext Attack**: A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

Brute Force Attack

Brute force attack is to simply try every key. It is the most basic attack, proportional to key size.

Unconditional and Computational Security

- **Unconditional security**: No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext.
- **Computational security**: Given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken.