Information Security Principles

Contribution by Dr V. Stathopoulos

- Confidentiality
- It has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of Information Security.
- Confidentiality is a requisite for maintaining the privacy of the people whose personal information the organization holds.
- Integrity
- data can not be created, changed, or deleted without authorization or the assurance that information can only be accessed or modified by those authorized to do so.
- Availability
- the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. The opposite of availability is denial of service (DOS).

Communication Privacy within the Security Context

- For every application-to-application communication, there are some specific security requirements
  - *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
  - *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
  - *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
  - *Non-repudiation:* A mechanism to prove that the sender really sent this message.
- Encryption not only protects data from theft or alteration, but can also be used for user authentication.

- There are, three types of cryptographic schemes
  - secret key (or symmetric) cryptography,
  - public-key (or asymmetric) cryptography, and
  - hash functions

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

- Secret key cryptography (confidentiality)
  - the key must be known to both the sender and the receiver; that, in fact, is the secret.
  - The biggest difficulty with this approach, of course, is the distribution of the key.
  - Secret key cryptography algorithms that are in use today
    - *Data Encryption Standard (DES) or improved named as Triple-DES (3DES)*
    - *Advanced Encryption Standard (AES)*
    - others...
- Public key cryptography (confidentiality, non-repudiation)
  - PKC depends upon the existence of so-called *one-way functions*, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute

- Public key cryptography
  - the key must be known to both the sender and the receiver; that, in fact, is the secret.
  - In PKC, one of the keys is designated the *public key* and may be advertised as widely as the owner wants. The other key is designated the *private key* and is never revealed to another party.
  - It is straight forward to send messages under this scheme.
    - A wants to send B a message. A encrypts some information using B's public key;
    - B decrypts the ciphertext using his private key.
    - This method could be also used to prove who sent a message; A encrypts plaintext with A’s private key;
    - when B decrypts using A's public key, he knows that A sent the message and A cannot deny having sent the message (*non-repudiation*).

- RSA (Rivest–Shamir–Adleman)
- Diffie–Hellman
- Digital Signal Algorithm

- *Hash functions are well-suited for ensuring data integrity*
  - *Indeed, any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender.*

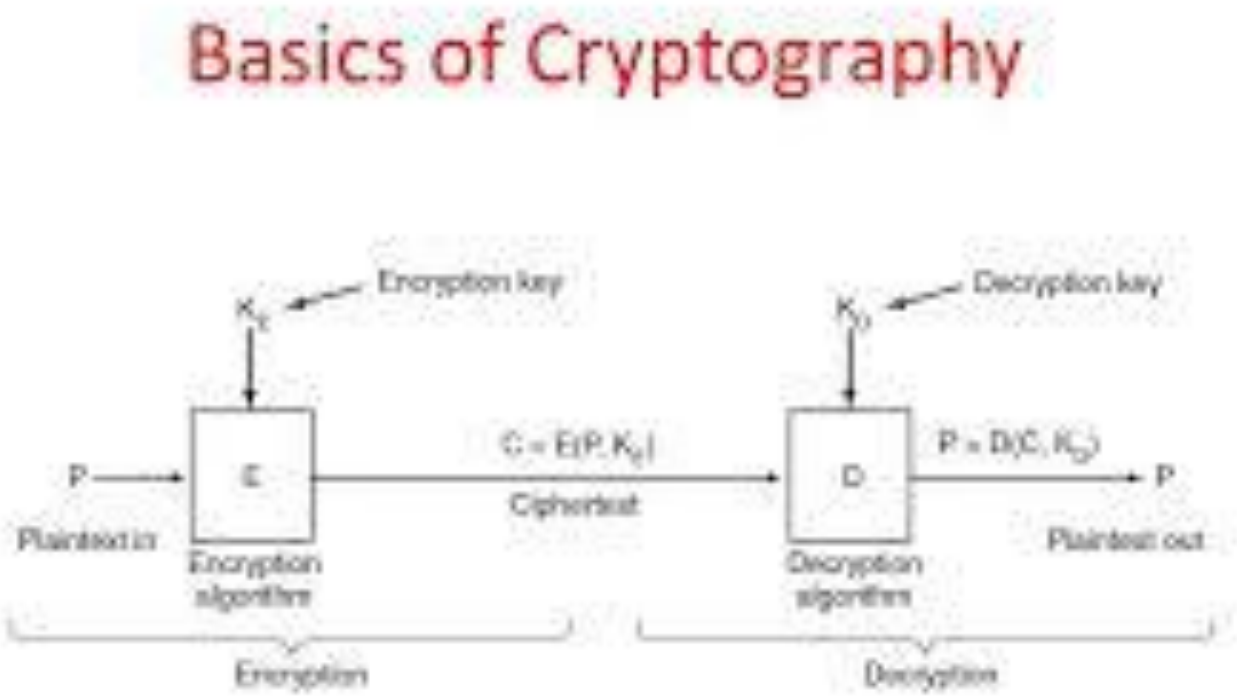
- Secret key cryptography is ideally suited to encrypt messages

- Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography

Public-Key Cryptography

- A message called ***plaintext P*** is encrypted into ***ciphertext C***
- Using an ***encryption key*** K_E To the encryption E function leads to $C= E(P, K_E)$
- On the other side we will decrypt the received C by the decryption function D and the ***decryption key*** K_d. $P= D(C, K_d)$
- ***Public-Key cryptography***: The encryption key is public, the decryption key is secret
- Encryption includes relatively low complexity operations
- Decryption has relatively very high complexity operations
- The RSA: *Rivest-Shamir-Adleman* cryptosystem uses multiplications of big numbers.

How the encryption functions apply to a message



Relationship between the plaintext and the ciphertext.