Introduction to cryptography

Cryptography is the study of mathematical techniques related to the aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. In other words, it is the mathematical foundation on which one builds a secure system. It studies the way of securely transmitting, storing and processing information. It is used to hide information by mangling with some mathematical techniques and tools. It is not only used by spies but also in telecommunication, email, banking transactions etc. Cryptography is also used for information security including digital signature which is also used for verification and authentication of messages that are sent world wide web(www).

Goals of cryptography

All the information related objectives are divided into four categories:

a) privacy/confidentiality
b) data integrity
c)authentication
d)non-repudiation

a. Privacy/Confidentiality
It is a service to keep the content of the information secured from all but those authorized to have it. There are numerous approaches for providing confidentiality ranging from physical protection to mathematical algorithms which render data unintelligible.

b. Data Integrity
It is the service that addresses the problem of unauthorized alteration of data. To assure. Data integrity one must have the ability to prevent data manipulation by unauthorized parties.

c. Authentication
It is the service related to identification which applies to both the entity and the information itself. Two parties entering a communication must identify each other. The information delivered over a channel should be authenticated with origin, data content, time sent etc. for this reason this aspect of cryptography is divided into two categories entity authentication and data origin authentication. (Remember: Data Authentication implicitly provides data integrity.)

d. Non-repudiation
It is the service that prevents the entity from denying previous commitments or action. Whenever disputes arise due to entities denying that actions were taken, means to resolve the situation is necessary.

Basic Terminologies used in Cryptography

1. Plaintext message
It is the message to be communicated.
2. Ciphertext
It is a disguised or mangled version of the plain text.
3. Encryption
Process that turns plain text into ciphertext.

4. Decryption
   Process that turns ciphertext back into plain text.
5. Cryptology
   Study of encryption and decryption algorithms.
6. Cryptography
   Application of cryptology
7. Stream Cipher
   It operates on a message symbol by symbol, bit by bit.
8. Block Cipher
   Operates on the message block wise.
9. Diagraph
   Operates on double letters.
10. Trigraph
    Operates on triple letters.
11. Polygraph
    Operates on multiple letters.
12. Transposition Cipher
    Rearrange letters, symbols or bits in the plain text.
13. Substitution Cipher
    Replaces letters, symbols or bits in the plain text without changing the order.
14. Product Cipher
    Alternate transposition and substitution cipher
15. Cryptanalysis
    The study of the process by which an enemy tries to turn ciphertext into plaintext.
16. Cryptosystem
    A system consisting of encryption and decryption algorithms.

3 ways by which enemy turns ciphertext into plaintext

1. Steal or purchase/bribe to get the key.
2. Exploit sloppy implementation to get the key.
3. Cryptanalysis

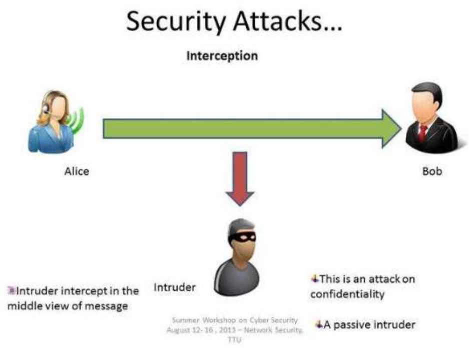
OSI Security Architecture

ITU-T (International Telecommunication Union Standard form) X.800 defines a systematic way for providing and defining security requirements known as OSI Security Architecture.
It provides three aspects of security:

a. Security Attack
b. Security Mechanism
c. Security Services

1. Security Attack
   It refers to any actions that compromises the security of information of an organization. Information security deals with preventing attacks or failing to detect the attack on information systems. There are four categories of security attacks.

a. Interruption: completely blocked / destroyed the assets of the system so that it becomes unavailable or unusable.
b. Interception:



Security Attacks...

Interception

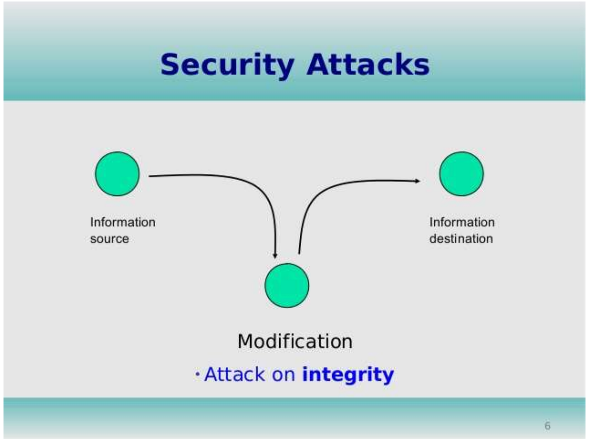
Intruder intercept in the middle view of message

This is an attack on confidentiality

A passive intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

c. Modification:



Security Attacks

Modification

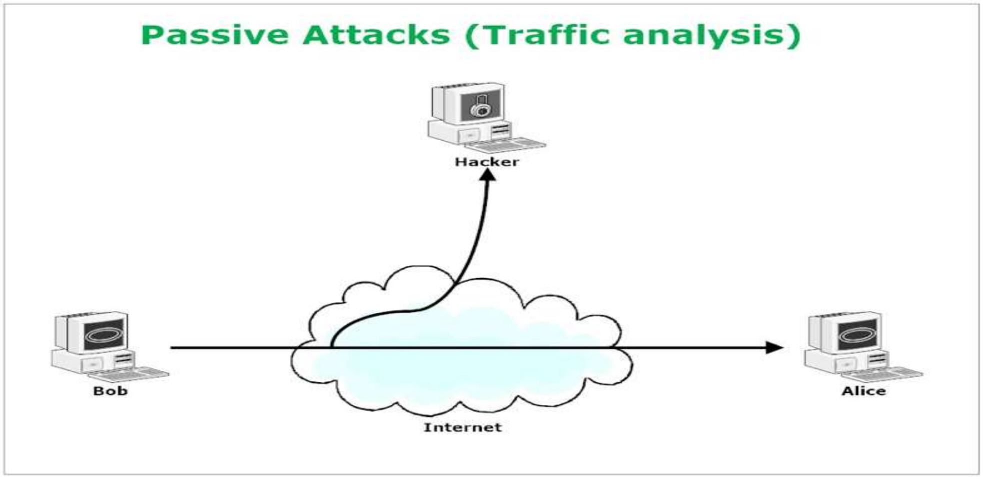
- Attack on **integrity**

d. Fabrication:

An authorized party enters counterfeit objects into the system which can be considered as an attack on integrity.

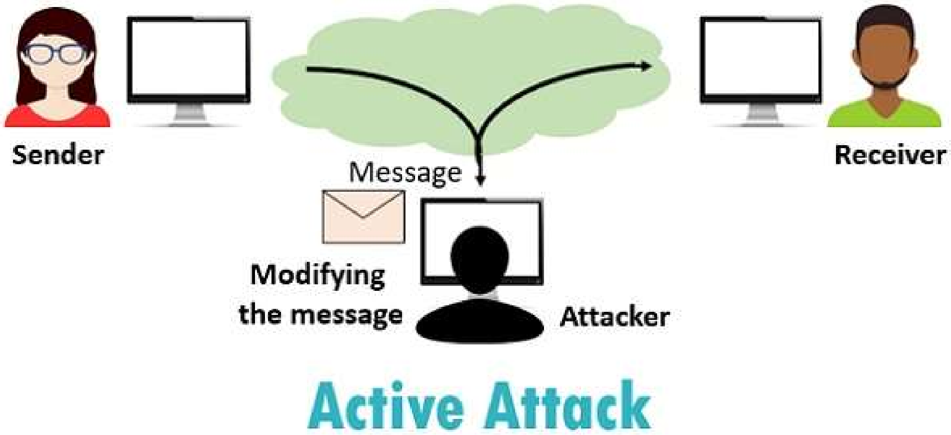
Generally, there are two types of attacks: passive attack (e.g.: interception) and active attack (e.g.: modification).

Passive attacks are of nature of monitoring the transmission. The primary goal of the opponent is to obtain the information being transmitted. Passive attack may be done by message release or traffic analysis.



Passive Attacks (Traffic analysis)

Active attacks involve modification of data strings or creation of a false system. These can be done by using a masquerade.



Masquerade: using a different identity for preventing exposure of one's identity/activity.
Activities: Replay, Modification, Denial of Service (DoS)

2. Security Services

It enhances the security of data processing. It is related to information transfer of an organization using security mechanisms. The most widely used security service types are discussed below:

a. X.800

It is the service provided by the protocol layer of communicating open systems which ensures adequate security of the system.

b. RFC 2828

A communication or processing service provided by the system to give specific kinds of protection to system resources.

The different security services of X.800 are:

i. Authentication: assurance of the communicating entity is the one being claimed.
ii. Access control: prevention of unauthorized use or access of resources.
iii. Data confidentiality: protection of data from unauthorized disclosure.
iv. Data integrity: assurance of data received is being sent by an authorized entity.
v. Non-repudiation: protection against denial by one of the parties in communication.

3. Security Mechanism

It deals with features designed to detect, prevent or recover from security attacks. No single mechanism that supports all the service is required. One particular element underlies many of the security mechanisms in use.

Security mechanism focus on:

a. Specific security mechanism

Encipherment, digital signatures, access control authentication, traffic padding, routing control, notarization etc.

b. Persuasive security mechanism

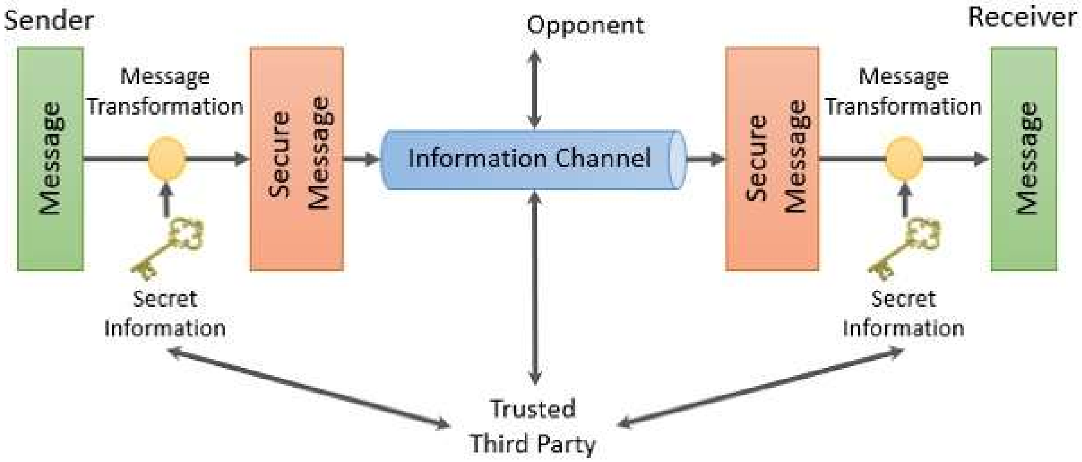
Trusted functionality, security labels, event detection, security audit trials, security recovery etc.

Generic model of secure communication

In secure communication, we use:

1. Model of N/W security
2. Model of N/W access security

1. Model of N/W security



Network Security Model

Using this model requires us to:

a. Design suitable algorithms for secure transmission.

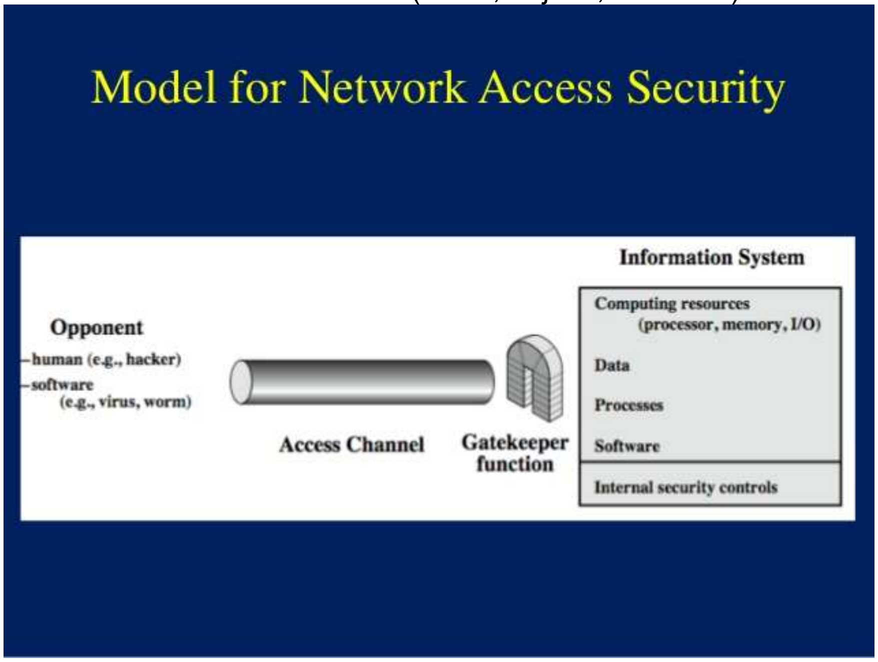
b. Develop a method to distribute and share the secret information.

c. Specify a protocol enabling the principles to use the transformation for security services.

2. Model of N/W access security

Opponents: humans (hackers, crackers)

software (worm, trojans, virus etc.)



Model for Network Access Security

Using this model, it requires us to:

a. Select appropriate gatekeeper function to identify users

b. Implement security controls to ensure only authorized access designated information resources.

c. Trusted computer system may be useful to implement this model.

#Categories of Cryptographic Systems

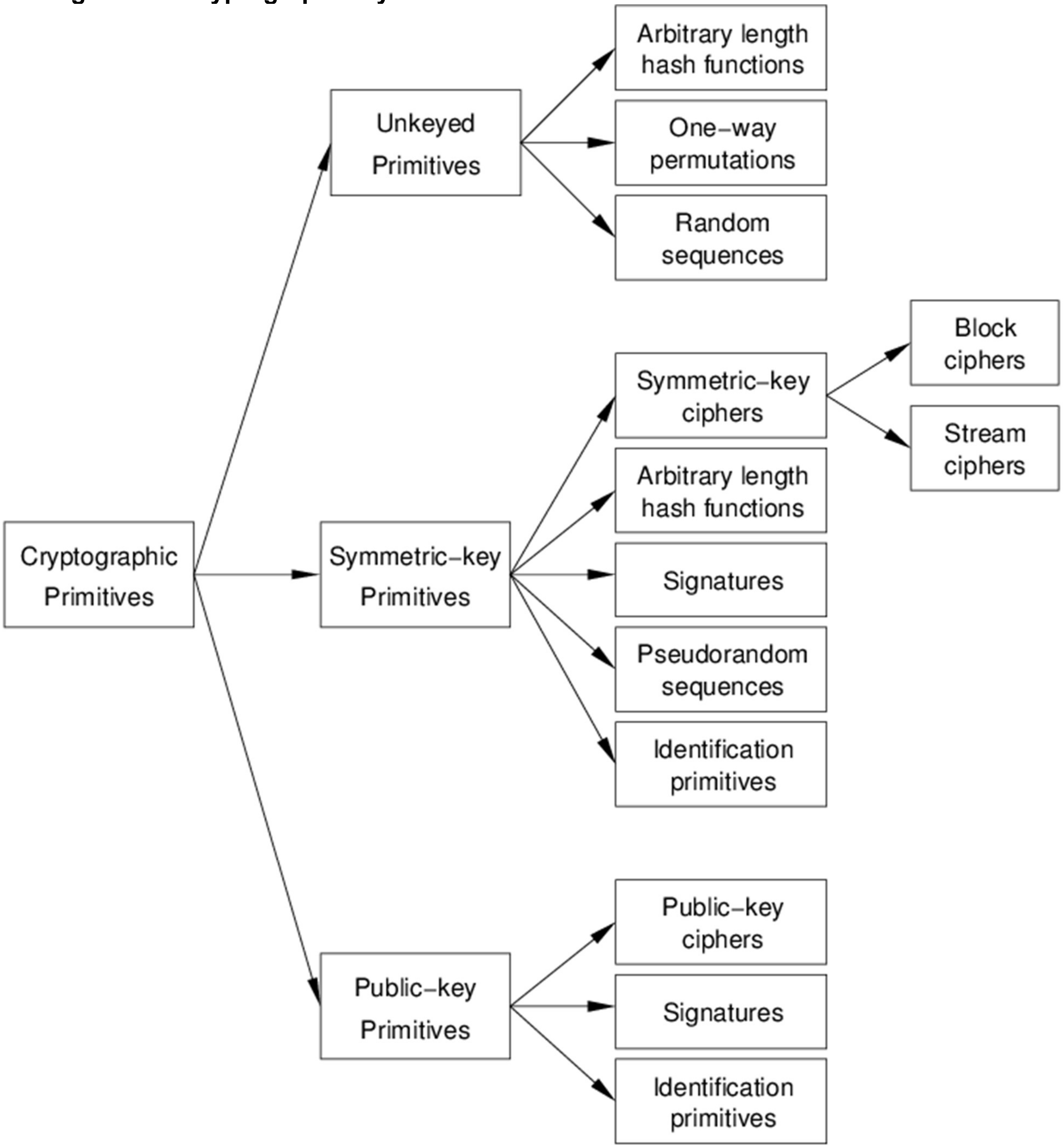


Fig. taxonomy of cryptographic systems

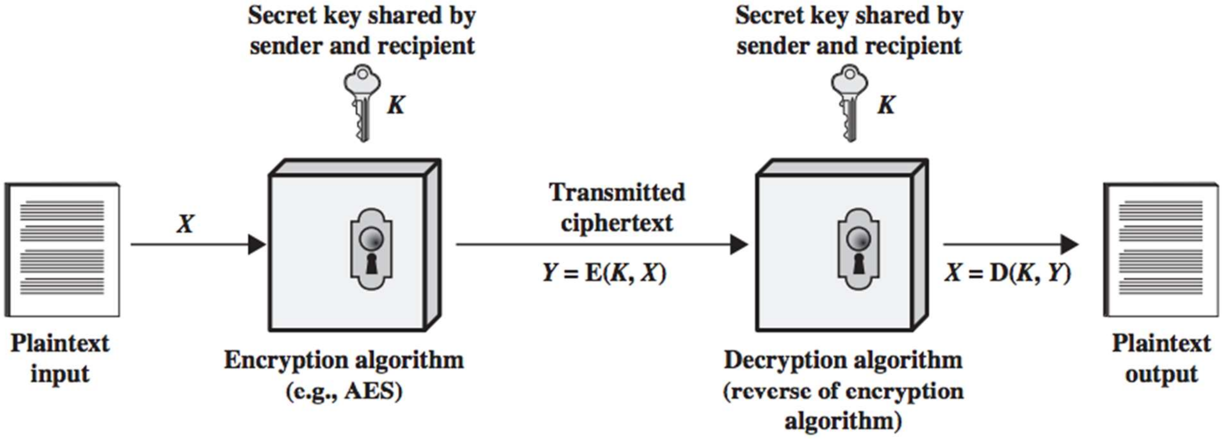
The categorization will be evaluated with respect to various criteria such as:

1. Level of security: Defined by upper bound on the amount of work necessary to defeat the objective.
2. Method of operation: A system should provide very different functionality depending upon the mode of operation of use.
3. Performance: efficiency of a system in a particular mode of operation.
4. Ease of Implementation: difficulty in realizing a system in a particular instantiation.

Conventional Encryption Model

1. Plain text
2. Encryption Algorithm
3. Secret key
4. Ciphertext
5. Decryption algorithm

The traditional or conventional encryption model uses a single private key in which the sender and the receiver share the same key. All classical encryption techniques / algorithms are private key techniques and it was the only type used widely before the invention of public key in 1970 the figure below shows the conventional encryption model.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Requirements for transmission of message through conventional encryption model

1. A strong Encryption Algorithm
2. A secret key K known to the receiver and the sender only.

Y=E (K, X)
X=D (K, X)
X is the plain text and Y is the ciphertext.

Note: if Encryption Algorithm is known, a secure channel to distribute key should be implemented.