Chapter One
Introduction

1.1. Cryptography

Computers are now fond in every layer society, and information is being communicated and processed automatically on a large scale. Such as medical and financial files, automatic banking, video-phones, pay-tv, facsimiles, tele-shopping, and global computer networks. In all these cases there is a growing need for the protection of information to safeguard economic interests, to prevent fraud and to ensure privacy.

Cryptography is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure and modification. The *Cryptographic systems* are classified into two cryptosystems, *private-key cryptosystem* and *public-key cryptosystem*. Both are based on complex mathematical algorithms and are controlled by keys. Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security. Cryptography, over the ages, has been an art practised by many who have devised ad hoc techniques to meet some of the information security requirements. The last twenty years have been a period of transition as the discipline moved from an art to a science. There are now several international scientific conferences devoted exclusively to cryptography and also an international scientific organization, the International Association for Cryptologic Research (IACR), aimed at fostering research in the area.

1.2. Cryptographic Tools

This section describes a number of basic *cryptographic tools* (*primitives*) used to provide information security. Examples of primitives include encryption schemes, hash functions, and digital signature schemes. These primitives should be evaluated with respect to various criteria such as [5]:

1. ***Level of security****:* This is usually difficult to quantify. Often it is given in terms of the number of operations required (using the best methods currently known) to defeat the intended objective. Typically the level of security is defined by an upper bound on the amount of work necessary to defeat the objective. This is sometimes called the work factor.
2. ***Functionality:*** Primitives will need to be combined to meet various information security objectives. Which primitives are most effective for a given objective will be determined by the basic properties of the primitives.
3. ***Methods of operation:*** Primitives, when applied in various ways and with various inputs, will typically exhibit different characteristics; thus, one primitive could provide very different functionality depending on its mode of operation or usage.

4. ***Performance:*** This refers to the efficiency of a primitive in a particular mode of operation. (For example, an encryption algorithm may be rated by the number of bits per second which it can encrypt.)
5. ***Ease of implementation:*** This refers to the difficulty of realizing the primitive in a practical instantiation. This might include the complexity of implementing the primitive in either a software or hardware environment.

The relative importance of various criteria is very much dependent on the application and resources available. For example, in an environment where computing power is limited one may have to trade off a very high level of security for better performance of the system as a whole.

1.3. Cryptographic Goals

Of all the information security objectives the following four form a framework from which the others will be built: (1) privacy or confidentiality, (2) data integrity, (3) authentication, and (4) non-repudiation [5].

1. *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

2. *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

3. *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

4. *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

1.4. Cryptosystems

Cryptography is the art and science of transforming (i.e., encrypting) information under secret keys for the purpose of secrecy or authenticity. A cryptographic system, or cryptosystem, consists of encrypt and decrypt

transformations together with a set of keys that parameterize the transformations. The encrypt function scrambles data into what appears as gibberish; the decrypt function restores the original data. The original data is referred to as plaintext or cleartext, and the scrambled data is ciphertext. Because the keys are not hard-wired into the functions, the same functions can be used with different keys. The decrypt key must be kept secret to prevent an eavesdropper from decrypting intercepted ciphertext; the transformations themselves may be public.

The strength of a cryptosystem refers to its ability to withstand attack by someone who intercepts ciphertext. A system is breakable if it is possible to systematically determine the secret key or plaintext of an intercepted ciphertext message. The process of attempting to break a cryptosystem is called cryptanalysis.

A system's strength depends on the number of its possible keys and its underlying mathematics. If the key length, which is typically expressed as a number of bits, is too short, a system may be broken by an exhaustive search, that is, by systematically trying all possible keys until one is found that produces known or meaningful plaintext. For example, if the key length is 32 bits, there are about 4 billion possibilities. Assuming that 1 million keys can be checked per second, all 4 billion could be checked in about an hour. Even if the key length is long enough that an attack by exhaustive search is infeasible, a cryptosystem may be vulnerable to a shortcut solution that exploits the system's underlying mathematics or some trapdoor [6]. Examples of shortcut methods are factoring and differential cryptanalysis.

The one-time pad is unbreakable because it is impossible to deduce any information about the key or plaintext from an intercepted ciphertext. The one-time pad and systems that stimulate it are called stream ciphers.

Although theoretically breakable, many systems are computationally strong or practically unbreakable in the sense that the resources required to break them are unavailable or prohibitively expensive. In practice, a system need only be strong enough to provide security commensurate with the risk and consequences of breakage. Increasing security usually increases costs and decreases performance; it does not make sense to pay more for encryption than the expected loss resulting from breakage [6].

1.4.1. Private-Key Cryptosystems

There are two types of cryptosystems: private key and public key. In a *private-key cryptosystem,* the encryption and decryption keys are the same (or readily derived from each other) and are kept secret. Private-key systems are also called *secret-key* systems and *symmetric* systems. Because all publicly known cryptosystems before the late 70s were private-key systems, they are also called *traditional* or *conventional cryptosystems*.

In addition to secrecy, requirements for secure communications often include integrity and authenticity — protection against message tampering and against injection of bogus messages by a third party. Private-key cryptosystems provide authenticity because the secret key is needed to modify or create ciphertext that decrypts into meaningful plaintext. If meaningful plaintext is not automatically recognizable, a message authentication code (MAC) can be computed and appended

to the message. The computation is a function of the entire message and a secret key; it is practically impossible to find another message with the same authenticator. The receiver checks the authenticity of the message by computing the MAC using the same secret key and then verifying that the computed value is the same as the one transmitted with the message. A MAC can be used to provide authenticity for unencrypted messages as well as for encrypted ones. The National Institute of Standards and Technology (NIST) has adopted a standard for computing a MAC [6].

Private-key systems are often used during the process of authenticating users to a system. Systems that use passwords usually store those passwords in encrypted form, using the password as the key so that the ciphertext passwords cannot be decrypted. When encryption is used this way, it effectively implements a one-way function of the secret information that cannot be reversed. (If a user forgets the password between login sessions, the password must be replaced with a new one because not even the system administrator can determine the plaintext password from the ciphertext password.) Stronger forms of user authentication are possible using access tokens and smart cards that have cryptographic capabilities.

1.4.2. Public-Key Cryptosystems

In a public-key cryptosystem, or asymmetric system, each user or application has a pair of permanent or long-term keys — a public key and a private key. The public key can be freely distributed or stored in a public directory, but the private key must be known only to the user or the user's cryptographic chip. Because the public and private keys must be mathematically related, the private key cannot be derived from the public key.

The advantage of public-key systems is that they allow the transmission of secret messages without the need to exchange a secret key. To send a message, the sender obtains the receiver's public key and uses it to encrypt the message. The receiver than decrypts the message using its private key. The sender's keys are not used (they would be used in a reply) [6].

Public-key cryptosystems can provide secrecy but not authenticity. This is true because a third party, with access to the receiver's public encryption key, can inject bogus ciphertext that decrypts into meaningful plaintext. To get authenticity, it is necessary to combine a public-key cryptosystem with a public-key signature system.

1.5. Security Attacks

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

1.5.1. Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being

transmitted. Two types of passive attacks are release of message contents and traffic analysis.

The release of message contents is easily understood (Figure 1.1a). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

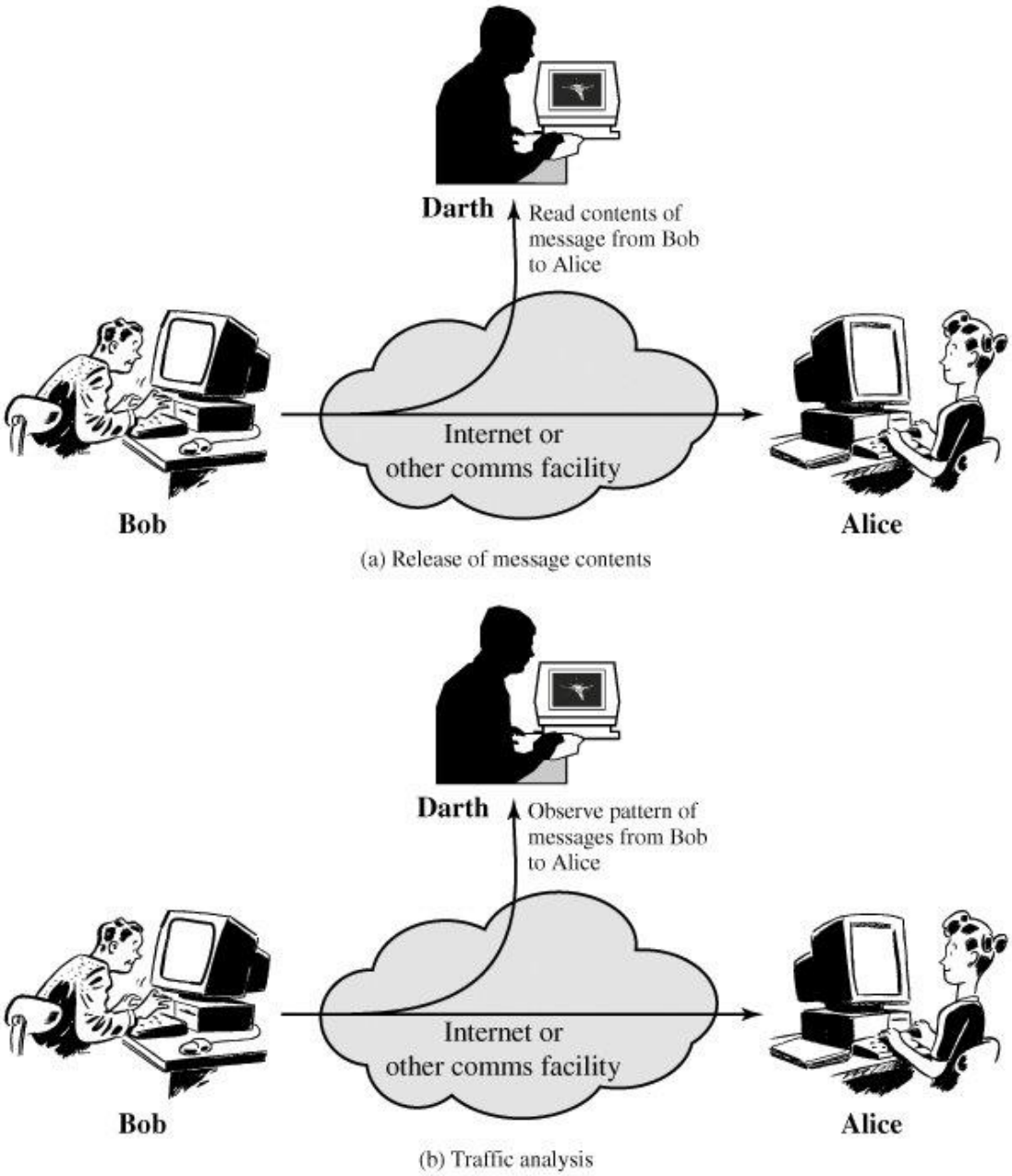

Figure 1.1. Passive Attacks

A second type of passive attack, **traffic analysis**, is subtler (Figure 1.1b). Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we

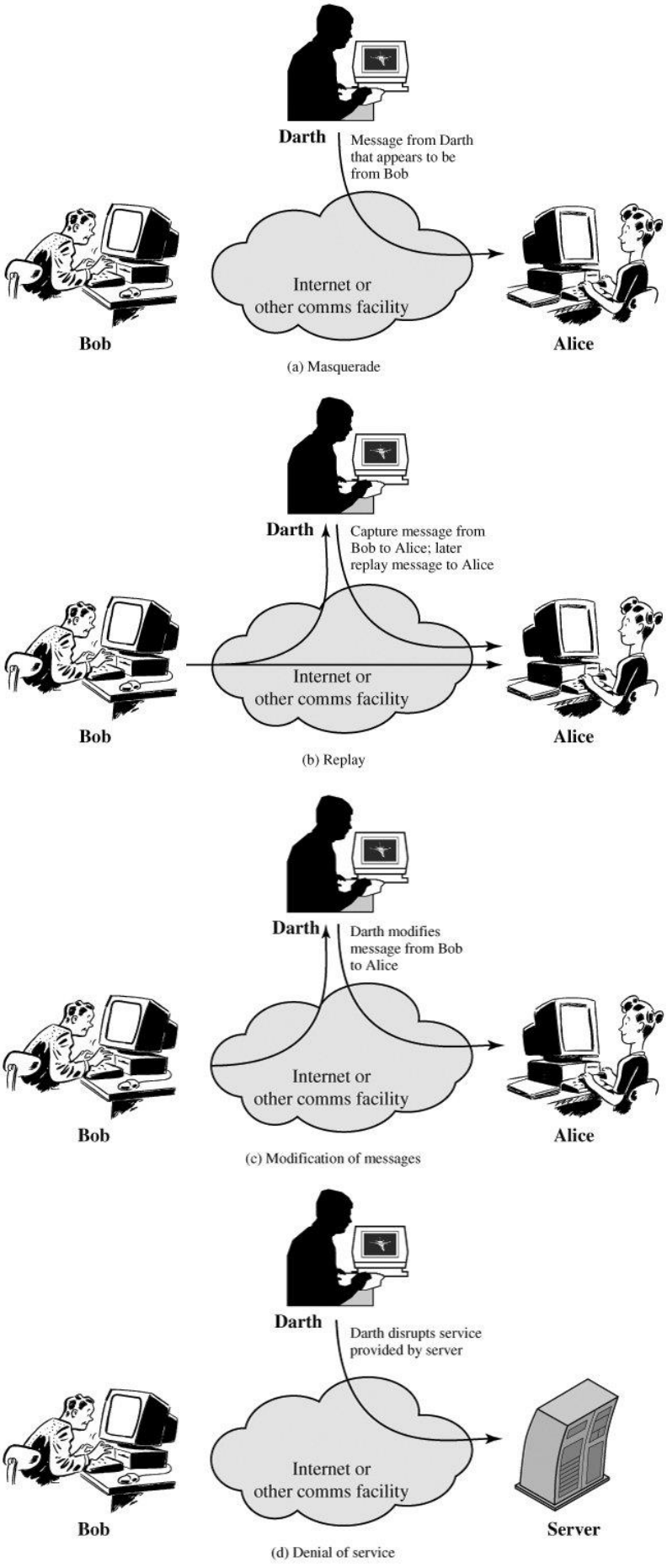

Figure 1.2. Active Attacks

had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

1.5.2. Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A ***masquerade*** takes place when one entity pretends to be a different entity (Figure 1.2a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.2b).

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.2c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The ***denial of service*** prevents or inhibits the normal use or management of communications facilities (Figure 1.2d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the

goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

1.6. A Model for Network Security

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.3. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

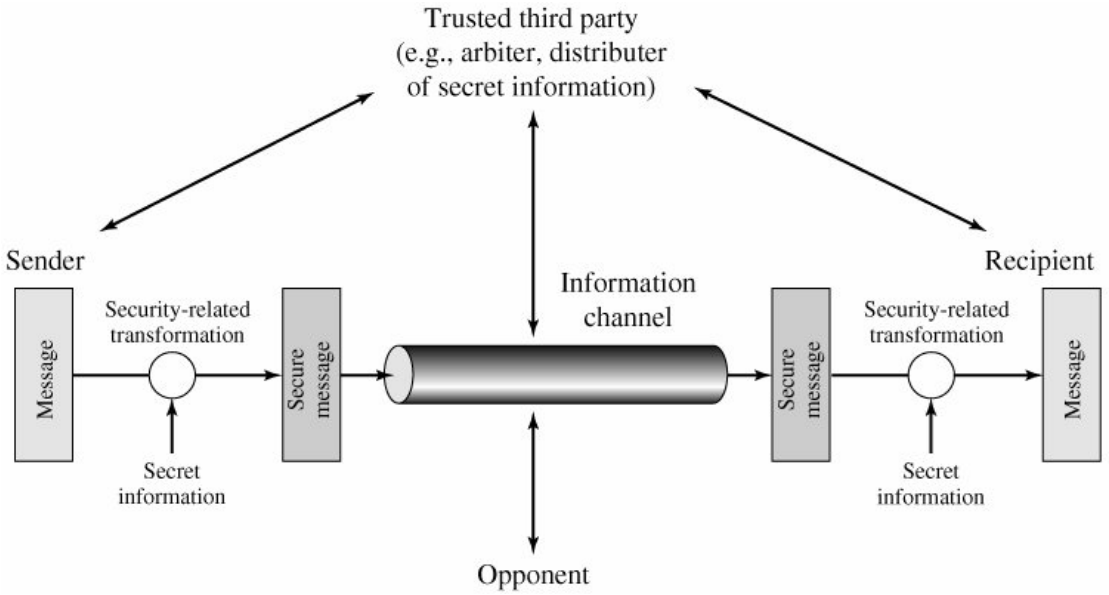

Figure 1.3. Model for Network Security

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the *encryption of the message*, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.