**Introduction to security and cryptography**

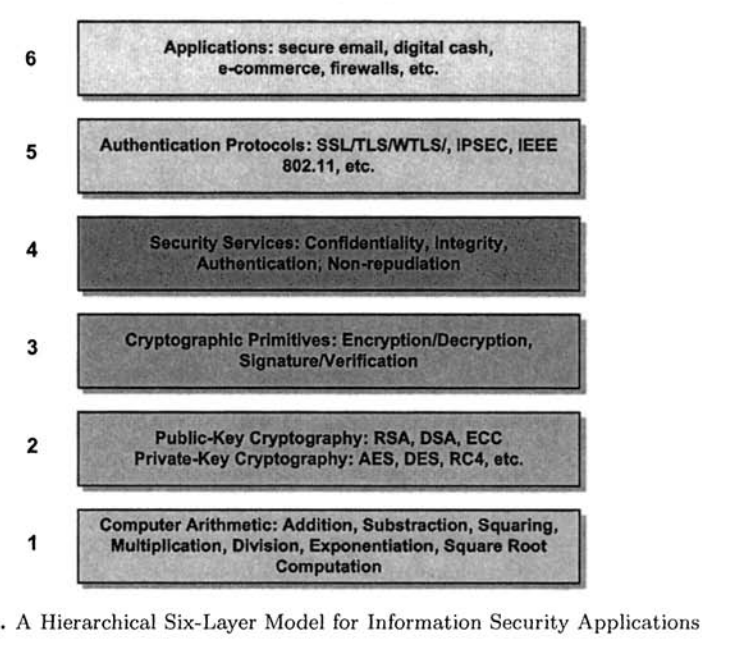
The communication between two entities is usually done through an insecure channel, which means that the information exchanged does not have any guarantee of privacy or integrity. Therefore, exchange of information should be provided by mechanisms or services that provide security. These security mechanisms or services are built using cryptographic tools.

In our Information Age, the need for protecting information is more pronounced than ever. Secure communication for the sensitive information is not only compelling for military or government institutions but also for the business sector and private individuals.

As the world becomes more connected, the dependency on electronic services has become more pronounced. In order to protect valuable data in computer and communication systems from unauthorized disclosure and modification, reliable non-interceptable means for data storage and transmission must be adopted.

As society has evolved, the need for more sophisticated methods of protecting data has increased. Now, with the information era at hand, the need is more pronounced than ever. As the world becomes more connected, the demand for information and electronic services is growing, and with the increased demand comes increased dependency on electronic systems. Already the exchange of sensitive information, such as credit card numbers, over the Internet is common practice. Protecting data and electronic systems is crucial to our way of living.

Figure 1 shows a hierarchical six-layer model for information security applications. Let us analyze that figure from a top-down point of view. On layer 6, several popular security applications have been listed such as: secure e-mail, digital cash, e-commerce, etc. Those applications depend on the implementation in layer 5 of secure authentication protocols like SSL/TLS, IPSec, IEEE 802.11, etc. However, those protocols cannot be put in place without implementing layer 4, which consists on customary security services such as: authentication, integrity, non-repudiation and confidentiahty. The underlying infrastructure for such security services is supported by the two pair of cryptographic primitives depicted in layer 3, namely, encryption/decryption and digital signature/verification. Both pair of cryptographic primitives can be implemented by the combination of public-key and private key cryptographic algorithms, such as the ones listed in layer 2. Finally, in order to obtain a high performance from the cryptographic algorithms of layer 1, it is indispensable to have an eflftcient implementation of arithmetic operations such as, addition, subtraction, multiplication, exponentiation, etc. [\FRHBOOK]



En nuestro curso se abarcan las capas 1, 2, 3 y 4.

**Cryptography**

History is filled with examples where people tried to keep information secret from adversaries. Kings and generals communicated with their troops using basic methods to prevent the enemy from learning sensitive military information. Encrypting the communication can protect it from prying eyes.

For thousands of years we have been inventing codes, and when those were broken we set about inventing better codes. *The search for the unbreakable code continues!*

The techniques needed to protect data belong to the field of cryptography. Actually, the subject has three names, cryptography, cryptology and cryptanalysis. [\TRAPE]

**Cryptology** is the all-inclusive term for the study of communication over nonsecure channels, and related problems. The process of designing systems to do this is called cryptography. Cryptanalysis deals with breaking such systcms.

Since a dictionary **Kriptos=hide** and **graphos=write**, cryptography is the art to write in an enigmatic mode.

“The study of mathematical techniques related to the aspects of information security, such as confidentiality, integrity and availability of the data, authentication of entity and origin, it doesn’t includes only the media to provide information security, but to a set of techniques.” Menezes & Vanstone

Modern cryptography is a field that draws heavily upon mathematics, computer science, and cleverness.

**Secure Communications**

In the basic communication scenario, depicted in Figure 1, there are two parties, we’ll call them Alice and Bob, who want to communicate with each other. A third party, Candy, is a potential eavesdropper.

When Alice wants to send a message, called the plaintext, to Bob, she encrypts it using a method prearranged with Bob. Usually, the encryption method is assumed to be known to Candy; what keeps the message secret is a key. When Bob receives the encrypted message, called the ciphertext, he changes it back to the plaintext using a decryption key.

Candy could have one of the following goals:

1. Read the message.

2. Find the key and thus read all messages encrypted with that key.

3. Corrupt Alice’s message into another message in such a way that Bob will think Alice sent the altered message.

4. Masquerade as Alice, and thus communicate with Bob even though Bob believes he is communicating with Alice.

Plaintext

Ciphertext

Decryption Key

Encryption Key

Candy

Fig. 1 Basic Communication Scenario for Cryptography

Communication Scenario for Cryptography. Which case we're in depends on how evil Candy is. Cases (3) and (4) relate to issues of integrity and authentication, respectively.

A more active and malicious adversary, corresponding to cases(3) and (4), is sometimes called Mallory in the literature. More passive observers (as in cases (1) and (2)) are sometimes named Oscar.

**Possible Attacks**

There are four main types of attack that Candy might be able to use. The differences among these types of attacks are the amounts of information Candy has available to her when trying to determine the key. The four attacks are as follows:

1. Ciphertext only: Candy has only a copy of the ciphertext
2. Known Plaintext: Candy has copy a ciphertext and the corresponding plaintext. For example, suppose Candy intercepts an encrypted press release, then sees the decrypted release the next day. If she can deduce the decryption key, and if Alice doesn’t change the key, Candy can read all future messages. Or, if Alice always starts her messages with “Dear Bob,” then Candy has a small piece of ciphertext and corresponding plaintext. For many weak cryptosystems, this suffices to find the key. Even for stronger systems such as the German Enigma machine used in World War II, this amount of information has been useful.
3. Chosen plaintext: Candy gains temporary access to the encryption machine. She cannot open it to find the key; however, she can encrypt a large number of suitably chosen plaintexts and try to use the resulting ciphertexts to deduce the key.
4. Chosen ciphertext: Candy obtains temporary access to the decryption machine, uses it to “decrypt” several strings of symbols, and tries to use the results to deduce the key.

A chosen plaintext attack could happens as follows. You want to identify an aiplane as friend or foe. Send a random message to the plane, which encrypts the message automatically and sends it back. Only a friendly airplane is assumed to have the correct key. Compare the message from the plane with the correctly encrypted message. If the match, the plane is friendly. Ig not, it’s the enemy. However, the enemy can send a large number of chosen messages to one of your planes and look at the resulting ciphertexts. If this allows them to deduce the key, the enemy can equip their plane so they can masquerade as friendly.

An example of a known plaintext attack reportedly happened in World War II In the Sahara Desert. An isolated German outpost every day sent an identical message saying that there was nothing new to report, but of course it was encrypted with the key being used that day. So each day the Allies had a piaintext-ciphertext pair that was extremely useful in determining the key. In fact, during the Sahara campaign, General Montgomery was carefully directed around the outpost so that the transmissions would not be stopped.

One of the most im portant assumptions in modern cryptography is Kerckhoff’s principle: In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used. This principle was enunciated by Auguste Kerclchoffs in 1883 in his classic treatise La Cnjptographie Militaire. The enemy can obtain this information in many ways. For example, encryption/decryption machines can be captured and analyzed. Or people can defect or be captured. The security of the system should therefore be based on the key and not on the obscurity of the algorithm used. Consequently, we always asume that Candy has knowledge os the algorithm that is used to perform encryption.