PRACTICAL-2

Aim: Prepare report on various security attack and security mechanism.

Theory:

Security Attack:

Typical, the objective of attacking and encryption system is to recover the key in use rethink then simple text of a single to recover the plaintext of a single cipher text. Following are general approaches to attack a conventional encryption scheme.

1. **Brute-Force:**

   Attack In the brute-force method or exhaustive-key-search method, Eve tries to use all possible keys. We assume that Eve knows the algorithm and knows the key domain (the list of all possible keys). Using the intercepted cipher, Eve decrypts the cipher text with every possible key until the plaintext makes sense. Using brute-force attack was a difficult task in the past; it is easier today using a computer. To prevent this type of attack, the number of possible keys must be very large.

2. **Statistical attack:**

   The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack. For example, we know that the letter E is the most frequently used letter in English text. The cryptanalyst finds the mostly-used character in the cipher text and assumes that the corresponding plaintext character is E. After finding a few pairs, the analyst can find the key and use it to decrypt the message. To prevent this type of attack, the cipher should hide the characteristics of the language.

3. **Patten attack:**

   Some ciphers may hide the characteristics of the language, but may create some patterns in the cyphertext. A cryptanalyst may use a pattern attack to break the cipher. Therefore, it is important to use ciphers that make the cyphertext look as random as possible.

Cryptanalysis:

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes. In addition to studying cryptography techniques, we also need to study cryptanalysis techniques. This is needed, not to break other people’s codes, but to learn how vulnerable our cryptosystem is. The study of cryptanalysis helps us create better secret codes. There are four common types of cryptanalysis attacks, as shown in Figure 2.1. We will study some of these attacks on particular ciphers in this and future chapters.

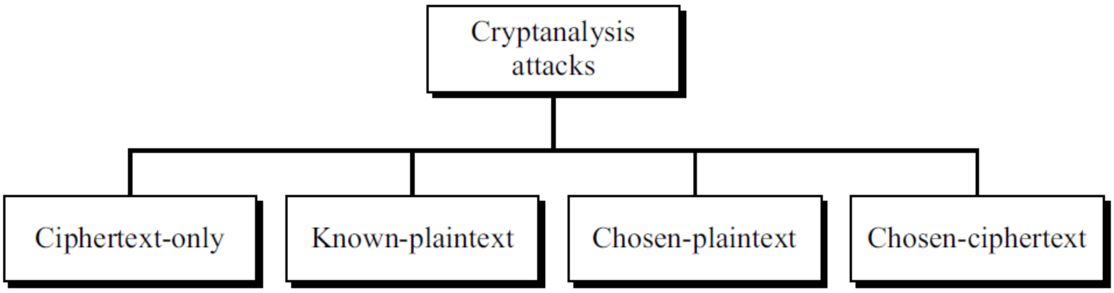

Figure 2.1: Cryptanalysis attacks

Cipher text-Only Attack:

In a cipher text-only attack, Eve has access to only some cipher text. She tries to find the corresponding key and the plaintext. The assumption is that Eve knows the algorithm and can intercept the cipher text. The cipher text-only attack is the most probable one because Eve needs only the cipher text for this attack. To thwart the decryption of a message by an adversary, a cipher must be very resisting to this type of attack. Figure 2.2 shows the process. Various methods can be used in cipher text only attack. We mention some common ones here.

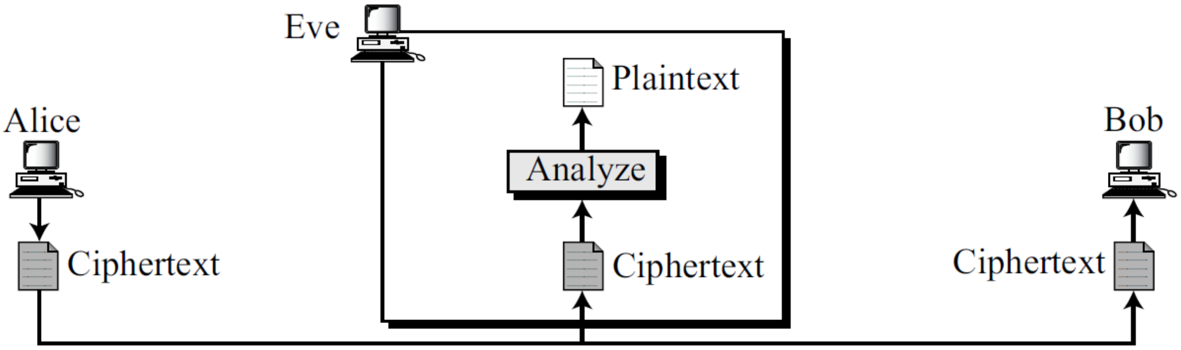

Figure 2.2 Cipher text-only attack

Known-Plaintext Attack:

In a known-plaintext attack, Eve has access to some plaintext/cipher text pairs in addition to the intercepted cipher text that she wants to break, as shown in Figure 2.3.

The plaintext/cipher text pairs have been collected earlier. For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public. Eve has kept both the cipher text and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key. Eve uses the relationship between the previous pair to analyze the current cipher text. The same methods used in a cipher text-only attack can be applied here. This attack is easier to implement because Eve has more information to use for analysis. However, it is less likely to happen because Alice may have changed her key or may have not disclosed the contents of any previous messages.

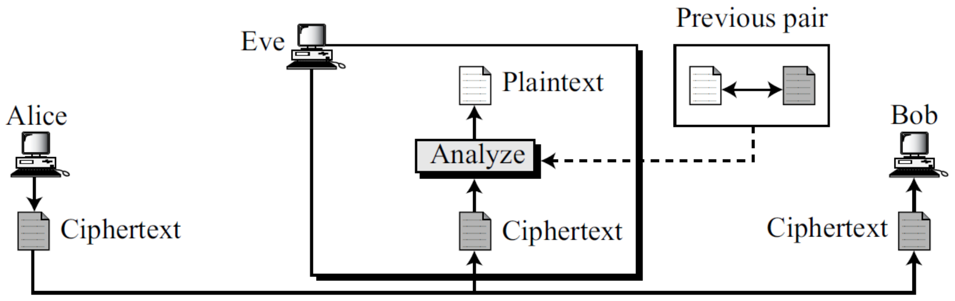

Figure 2.3 Known-plaintext attack

Chosen-Plaintext Attack:

The chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/cipher text pairs have been chosen by the attacker herself. Figure 2.4 shows the process.

This can happen, for example, if Eve has access to Alice's computer. She can choose some plaintext and intercept the created cipher text. Of course, she does not have the key because the key is normally embedded in the software used by the sender. This type of attack is much easier to implement, but it is much less likely to happen.

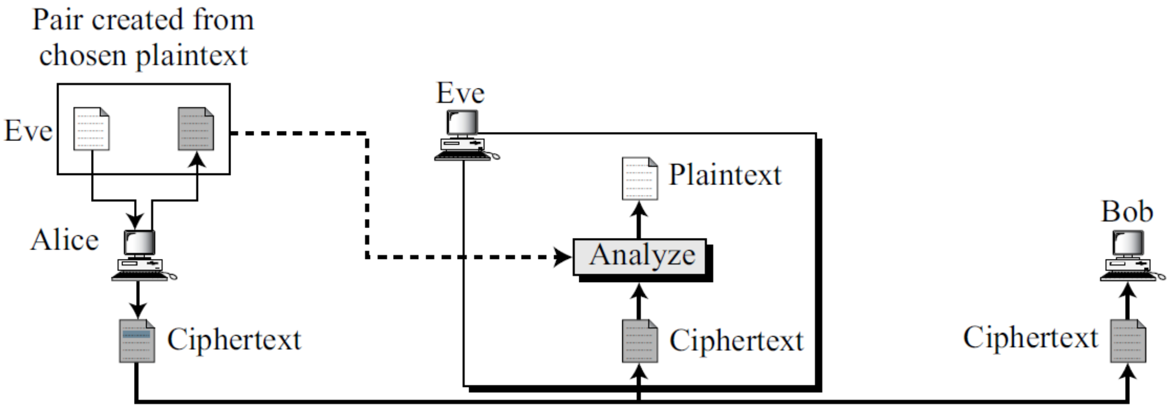

Fig.2.4 Chosen-plaintext attack

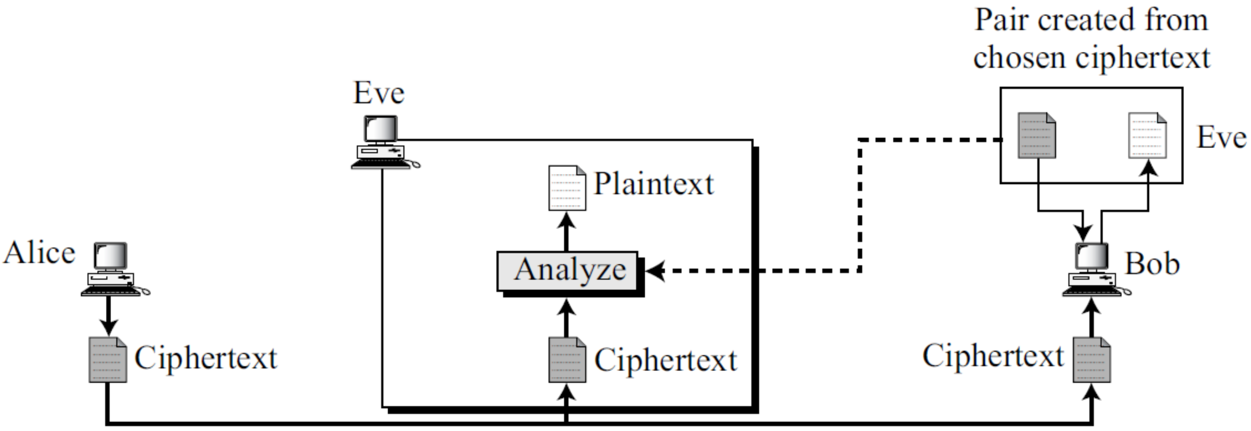

Figure 2.5 Chosen-cipher text attack

Chosen-Cipher text Attack:

The chosen-cipher text attack is similar to the chosen-plaintext attack, except that Eve chooses some cipher text and decrypts it to form a cipher text/plaintext pair. This can happen if Eve has access to Bob's computer. Figure 2.5 shows the process.

Security Mechanisms:

ITU-T (X.800) also recommends some security mechanisms to provide the security services defined in the previous section. Figure 2.6 gives the taxonomy of these mechanisms.

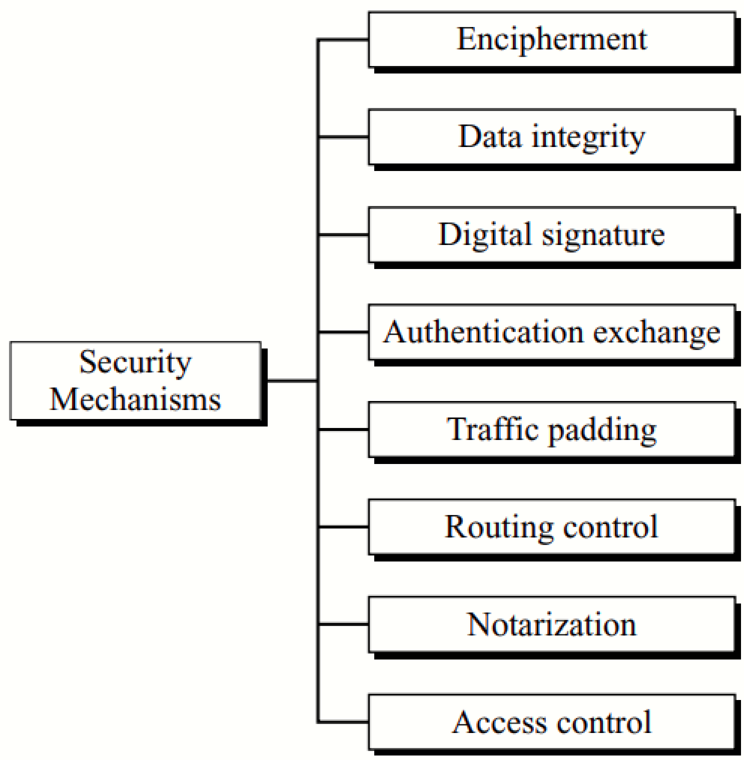

Fig.2.6. Security mechanisms

Encipherment:

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques cryptography and steganography are used for enciphering. We will discuss these shortly.

Data Integrity:

The data integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself. The receiver receives the data and the check value. He creates a new check value from the received data and compares the newly created check value with the one received. If the two check values are the same, the integrity of data has been preserved.

Digital Signature:

A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Authentication:

Exchange In authentication exchange, two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

Traffic Padding:

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

Routing Control:

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Notarization:

Notarization means selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

Access Control:

Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Security Service	**Security Mechanism**
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Non repudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Table 1.2 Relation between security services and security mechanisms

Relation between Services and Mechanisms:

Table 1.2 shows the relationship between the security services and the security mechanisms. The table shows that three mechanisms (encipherment, digital signature, and authentication exchange) can be used to provide authentication. The table also shows that encipherment mechanism may be involved in three services (data confidentiality, data integrity, and authentication)