goals we want to achieve for successful e-commerce.

13.9.1. Attacks on Security

Security attacks can be classified in the following two categories depending on the nature of the attacker and figure 13.13 shows attacks and Encryption model.

1. Passive Attacks

The attacker can only eavesdrop or monitor the network traffic. Typically, this is the easiest form of attack and can be performed without difficulty in many networking environments, *e.g.*, broadcast type networks such as Ethernet and wireless networks.

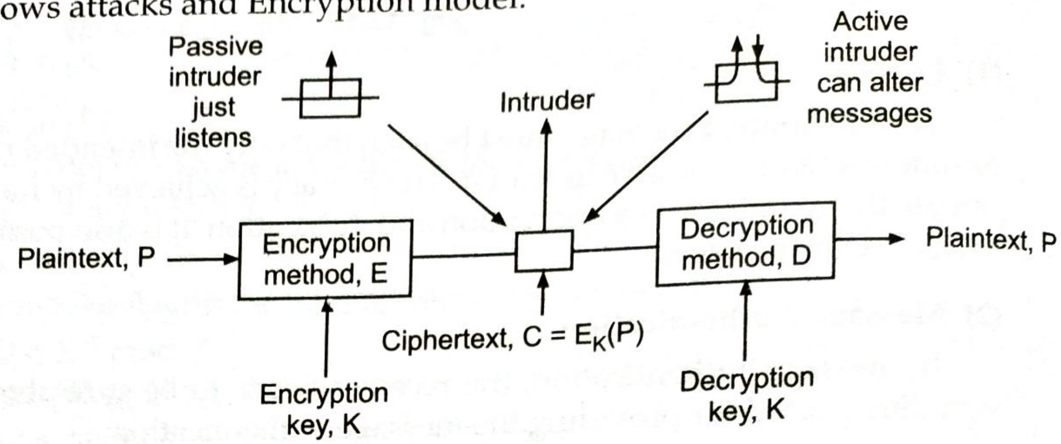

Fig. 13.13. Attacks and Encryption model

2. Active Attacks

The attacker is not only able to listen to the transmission but is also able to actively alter or obstruct it. Furthermore, depending on the attackers actions, the following subcategories can be used to cover the majority of attacks.

3. Eavesdropping

This attack is used to gain knowledge of the transmitted data. This is a passive attack which is easily performed in many networking environments as mentioned above. However, this attack can easily be prevented by using an encryption scheme to protect the transmitted data.

4. Traffic Analysis

The main goal of this attack is not to gain direct knowledge about the transmitted data, but to extra information from the characteristics of the transmission, e.g., amount of data transmitted, identity of the communicating nodes etc. This information may allow the attacker to deduce sensitive information, e.g., the roes of the communicating nodes, their position etc. Unlike the previously described attack, this one is more difficult to prevent.

5. Impersonation

Here, the attacker uses the identity of another node to gain unauthorized access to a resource or data. This attack is often used as a prerequisite to eavesdropping. By impersonating a legitimate node, the attacker can try to gain access to the encryption key used to protect the transmitted data. Once, this key is known by the attacker, she can successfully perform the eavesdropping attack.

6. Modification

This attack modifies data during the transmission between the communicating nodes, implying that the communicating nodes do not share the same view of the transmitted data. An example could be when the transmitted data represents a financial transaction where the attacker has modified the transactions value

7. Insertion

This attack involves an unauthorized party, who insets new data claiming that it originates from a legitimate party. This attack is related to that of impersonation.