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. 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.

The general model shows that there are four basic tasks in designing a particular security
service:

1. Design an algorithm for performing the security-related transformation. The
algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security
algorithm and the secret information to achieve a particular security service.

A general model is illustrated by the above Figure 1.6, which reflects a concern for
protecting an information system from unwanted access. Most readers are familiar with the
concerns caused by the existence of hackers, who attempt to penetrate systems that can be
accessed over a network. The hacker can be someone who, with no malign intent, simply gets
satisfaction from breaking and entering a computer system. Or, the intruder can be a
disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer
assets for financial gain.