Module
8

Network Security

Lesson 2

Secured Communication

Specific Instructional Objectives

On completion of this lesson, the student will be able to:

- State various services needed for secured communication
- Explain how Privacy, Authentication, Integrity and Nonrepudiation are achieved using cryptography
- State how user authentication is performed
- Explain how the PGP protocol works
- Explain how VPN works

8.2.1 Introduction

The basic objective is to communicate securely over an insecure medium. Any action that compromises the security of information can be considered as attack on security. Possible type of attacks mentioned below:

- **Interruption:** It is an attack on the availability of information by cutting wires, jamming wireless signals or dropping of packets by a switch.
- **Interception:** As a message is communicated through a network, eavesdroppers can listen in use it for his/her own benefit and try to tamper it.
- **Modification:** As a message is communicated through a network, eavesdroppers can intercept it and send a modified message in place of the original one.
- **Fabrication:** A message may be sent by a stranger by posing as a friend. This is also known as impersonation.

These attacks can be prevented with the help of several services implemented with the help of cryptography, as mentioned in the following section.

8.2.2 Security Services

Secured communication requires the following four basic services:

- **Privacy:** A person (say Sita) should be able to send a message to another person (say Ram) privately. It implies that to all others the message should be unintelligible.
- **Authentication:** After the message is received by Ram, he should be sure that the message has been sent by nobody else but by Sita.
- **Integrity:** Ram should be sure that the message has not been tampered on transit.
- **Nonrepudiation:** Ram should be able to prove at a later stage that the message was indeed received from Sita.

8.2.3 Privacy

Privacy can be achieved using symmetric key cryptography. In this case, the key is shared between the sender (Sita) and the receiver (Ram) as shown in Fig. 8.2.1. Privacy can also be achieved by using public-key cryptography as shown in Fig. 8.2.2. However, in this case the owner should be verified.

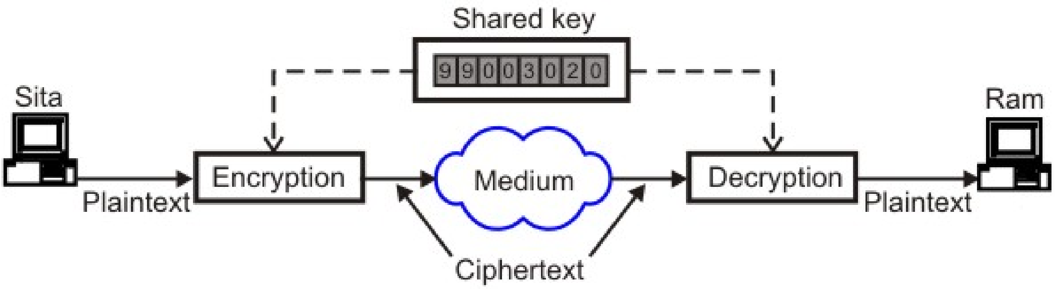


Figure 8.2.1 Privacy using private-key cryptography

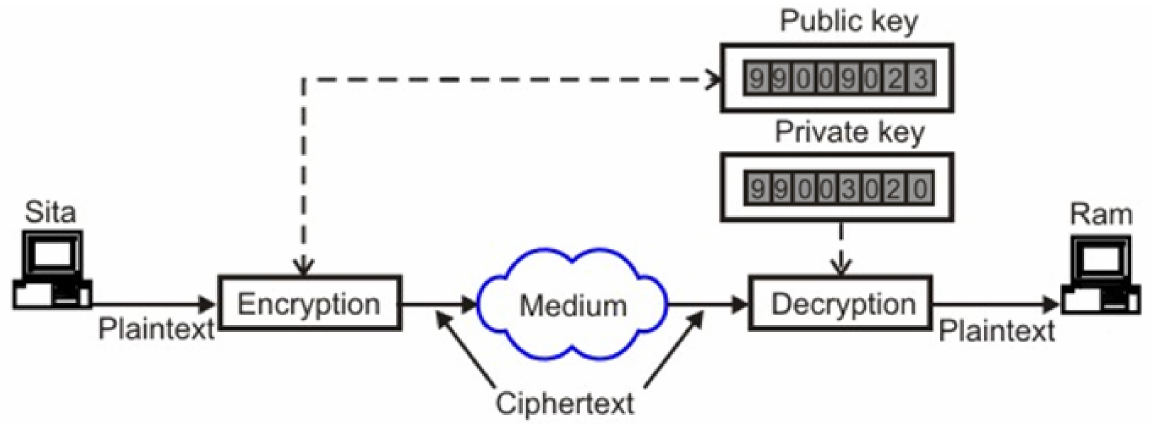


Figure 8.2.2 Privacy using public-key cryptography.

8.2.4 Authentication, Integrity and Nonrepudiation using Digital Signature

By message authentication we mean that the receiver should be sure about sender's identity. One approach to provide authentication is with the help of digital signature. The idea is similar to signing a document. Digital Signature provides the remaining three security services; Authentication, Integrity and Nonrepudiation.

Digital Signature

There are two alternatives for Digital Signature:

- Signing the entire document
- Signing the digest

In the first case the entire document is encrypted using private key of the sender and at the receiving end it is decrypted using the public key of the sender as shown in Fig. 8.2.3. For a large message this approach is very inefficient. In the second case a miniature version of the message, known as *digest*, is encrypted using the private key of the sender and then the signed digest along with the message is sent to the receiver as shown in Fig. 8.2.4. The receiver decrypts the signed digest using the public key of the sender and the digest created using the received message is compared with the decrypted digest as shown in Fig. 8.2.5. If the two are identical, it is assumed that the sender is authenticated. This is somewhat similar to error detection using parity bit.

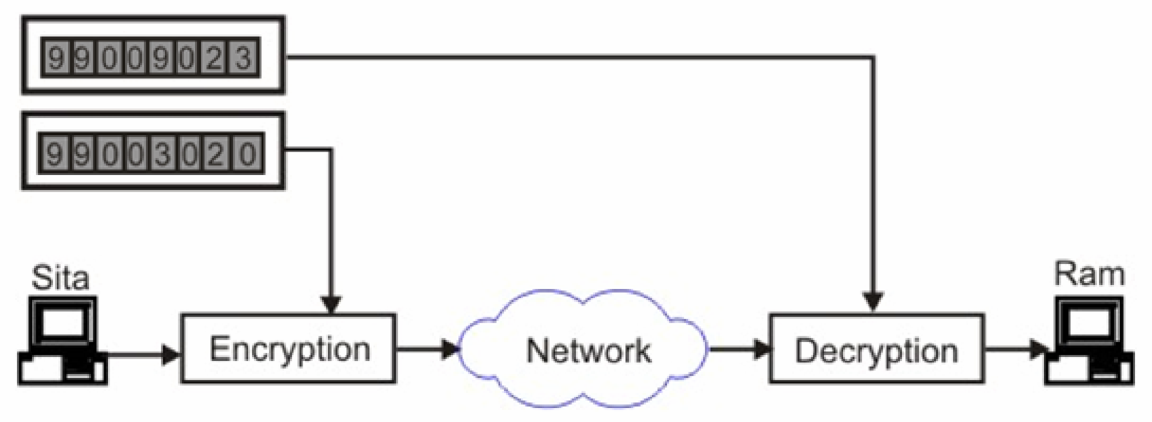


Figure 8.2.3 Authentication by signing the whole document.

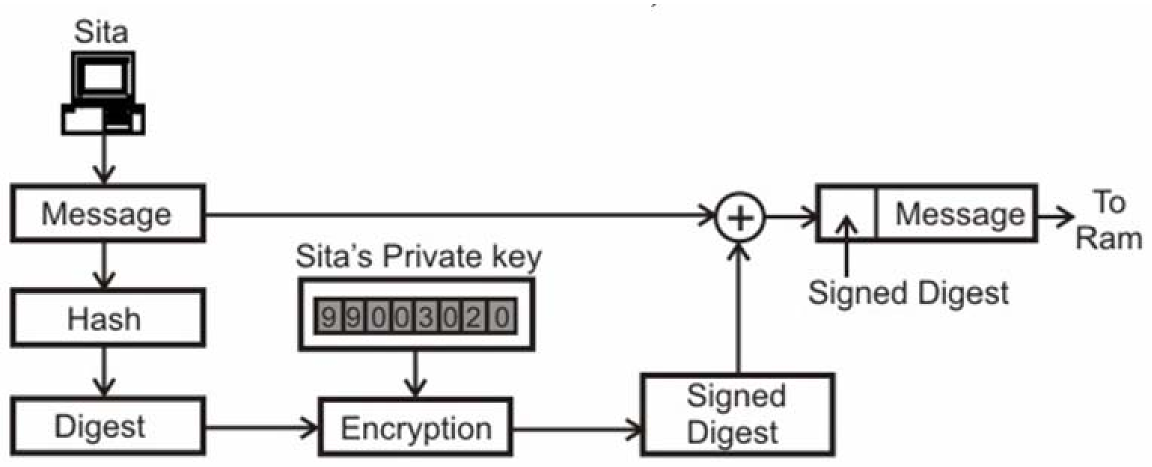


Figure 8.2.4 Sender site for authentication by signed digest

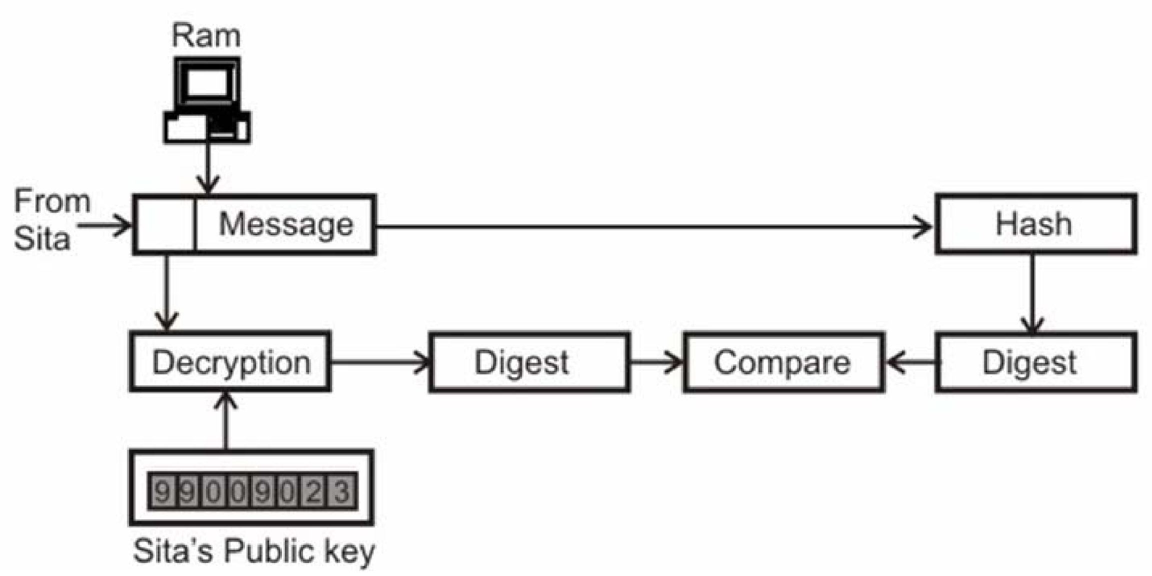


Figure 8.2.5 Receiver site for authentication by signed digest

Some key features of this approach are mentioned below:

- Digital signature does not provide privacy
- Hash function is used to create a message digest
- It creates a fixed-length digest from a variable-length message
- Most common Hash functions:
    - MD5 (Message Digest 5): 120-bit
    - SHA-1 (Secure Hash algorithm 1): 160-bit
- Important properties:
- One-to-One
- One-way

8.2.5 User Authentication using symmetric key cryptography

User authentication is different from message authentication. In case of message authentication, the identity of the sender is verified for each and every message. On the other hand, in user authentication, the user authentication is performed once for the duration of system access.

In the first approach, the sender (Sita) sends her identity and password in an encrypted message using the symmetric-key K_{SR} and then sends the message as shown in Fig. 8.2.6. However, an intruder (say Ravana) can cause damage without accessing it. He can also intercept both the authentication message and the data message, store them and then resends them, which is known as *replay attack.*

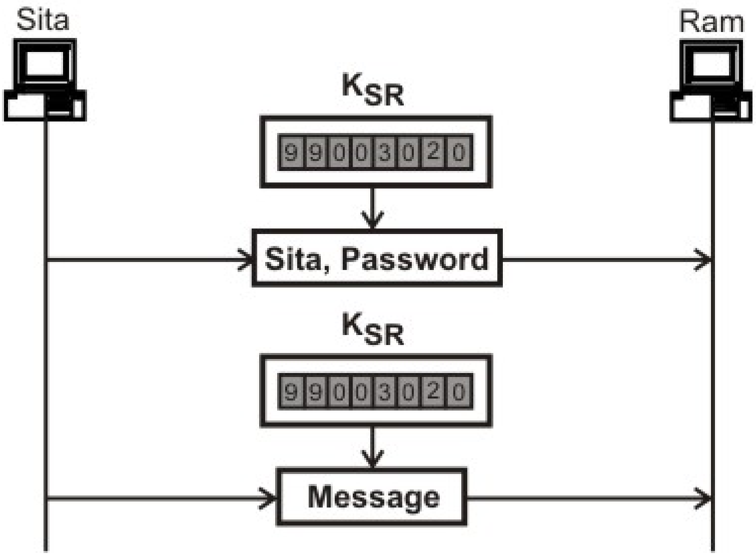


Figure 8.2.6 User authentication using symmetric key cryptography

Using nonce, a large random number used only once

To prevent the replay attack, the receiver (Ram) sends *nonce*, a large random number that is used only once to the sender (Sita) to challenge Sita. In response Sita sends an encrypted version of the random number using the symmetric key. The procedure is shown in Fig. 8.2.7.

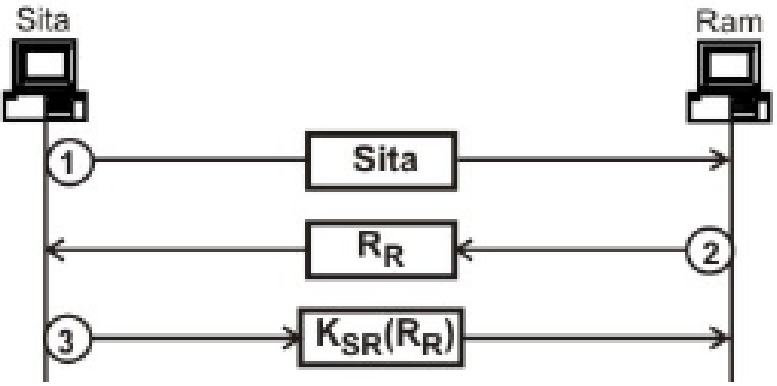


Figure 8.2.7 User authentication using a nonce

Bidirectional Authentication

In the bidirectional authentication approach, Ram sends *nonce* to challenge Sita and Sita in turn sends nonce to challenge Ram as shown in Fig. 8.2.8. This protocol uses extra messages for user authentication. Protocol with lesser number of messages is possible as shown in Fig. 8.2.9.

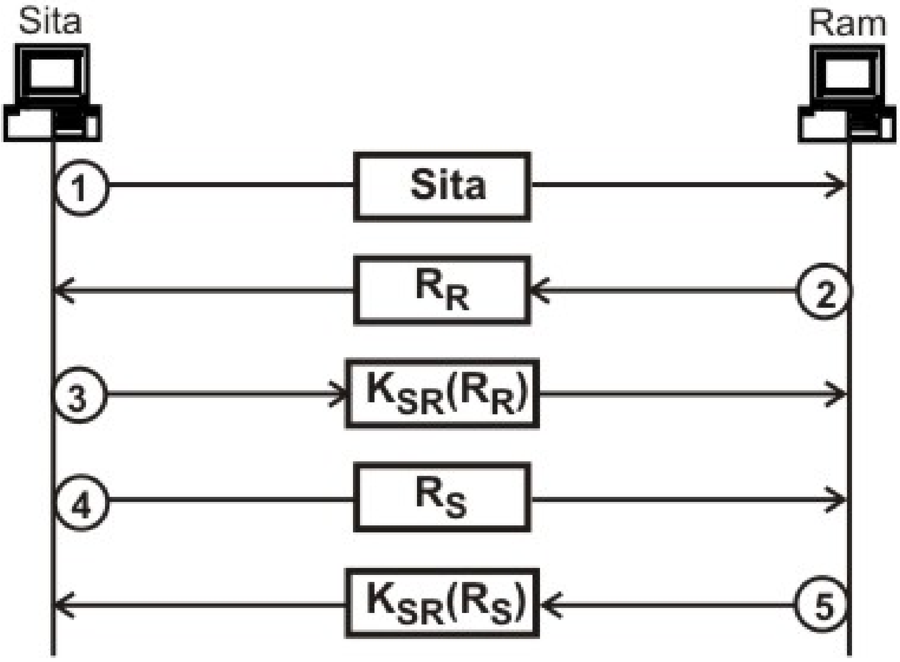


Figure 8.2.8 Bidirectional authentication using a nonce

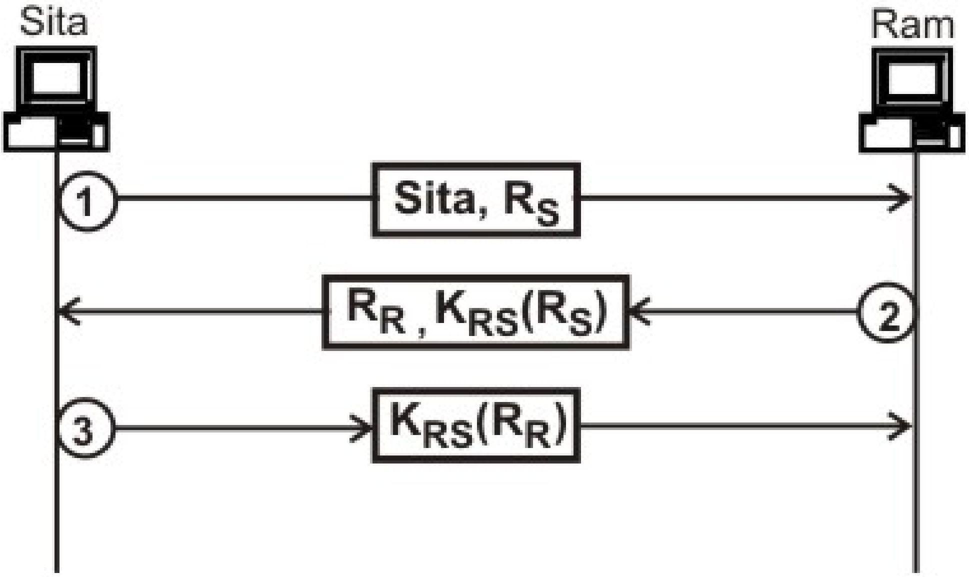
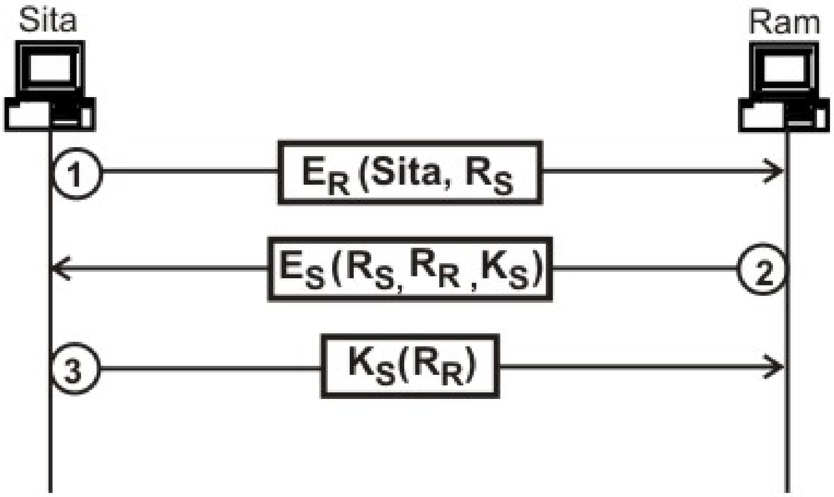


Figure 8.2.9 Bidirectional authentication using lesser number of messages

8.2.6 User Authentication using Public Key Cryptography

Public key cryptography can also be used to authenticate a user. The procedure is shown in Fig. 8.2.10.



E_R= Public key of Ram, E_S= Public key of Sita
R_S= nonce by Sita, R_R= nonce by Ram
K_S= Session key sent by Ram

Figure 8.2.10 User authentication using public key cryptography

8.2.7 Key Management

Although symmetric-key and public-key cryptography can be used for privacy and user authentication, question arises about the techniques used for the distribution of keys. Particularly, symmetric-key distribution involves the following three problems:

- For n people to communicate with each other requires n(n-1)/2 keys. The problem is aggravated as n becomes very large.
- Each person needs to remember (n-1) keys to communicate with the the remaining (n-1) persons.
- How the two parties will acquire the shared key in a secured manner?

In view of the above problems, the concept of *session key* has emerged. A session key is created for each session and destroyed when the session is over. The **Diffie-Hellman** protocol is one of the most popular approach for providing one-time session key for both the parties.

Diffie-Hellman Protocol

Key features of the Diffie-Hellman protocol are mentioned below and the procedure is given in Fig. 8.2.11.

- Used to establish a shared secret key

- Prerequisite: N is a large prime number such that (N-1)/2 is also a prime number. G is also a prime number. Both N and G are known to Ram and Sita..
- Sita chooses a large random number x and calculates R1 = G^xmod N and sends it to Ram
- Ram chooses another large random number y and calculates R2 = G^ymod N and sends it to Sita
- Ram calculates K = $(R1)^y$ mod N
- Sita calculates K = $(R2)^x$ mod N

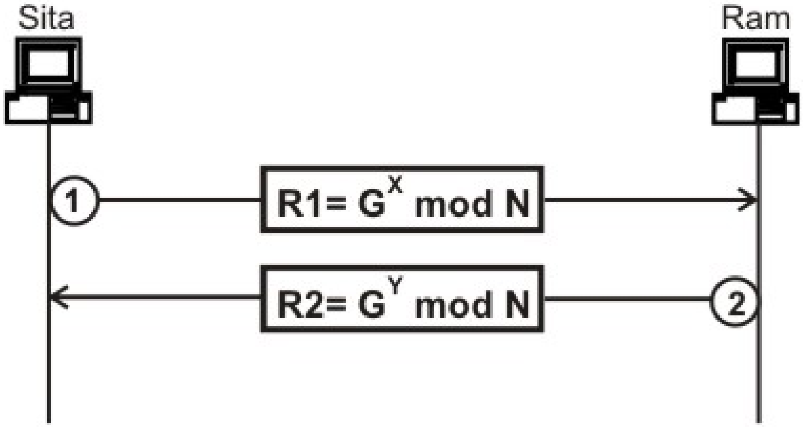


Figure 8.2.11 Diffie-Hellman Protocol

Key Management using KDC

It may be noted that both R1 and R2 are sent as plaintext, which may be intercepted by an intruder. This is a serious flaw of the Diffie-Hellman Protocol. Another approach is to use a trusted third party to assign a symmetric key to both the parties. This is the basic idea behind the use of *key distribution center (KDC).*

Key Management using Kerberos

Another popular authentication protocol known as *Kerberos.* It uses an authentication server (AS), which performs the role of KDC and a ticket-granting server (TGS), which provides the session key (K_{AB}) between the sender and receiver parties. Apart from these servers, there is the real data server say Ram that provides services to the user Sita. The operation of Kerberos is depicted with the help of Fig. 8.2.12. The client process (Sita) can get a service from a process running in the real server Ram after six steps as shown in the figure. The steps are as follows:

Step 1. Sita uses her registered identity to send her message in plaintext.
Step 2. The AS server sends a message encrypted with Sita's symmetric key K_S. The message contains a session key $K_{se,}$ which is used by Sita to contact the TGS and a ticket for TGS that is encrypted with the TGS symmetric key K_{TG}.

Step3. Sita sends three items to the TGS; the ticket received from the AS, the name of the real server, and a timestamp encrypted by K_{se}. The timestamp prevents replay by Ram.
Step 4. The TGS sends two tickets to Sita. The ticket for Sita encrypted with Kse and the ticket for Ram encrypted with Ram's key. Each of the tickets contains the session key K_{SR} between Sita and Ram.
Step 5. Sita sends Ram's ticket encrypted by K_{SR}.
Step 6. Ram sends a message to Sita by adding 1 to the timestamp confirming the receipt of the message using K_{SR} as the key for encryption.

Following this Sita can request and get services from Ram using K_{SR} as the shared key.

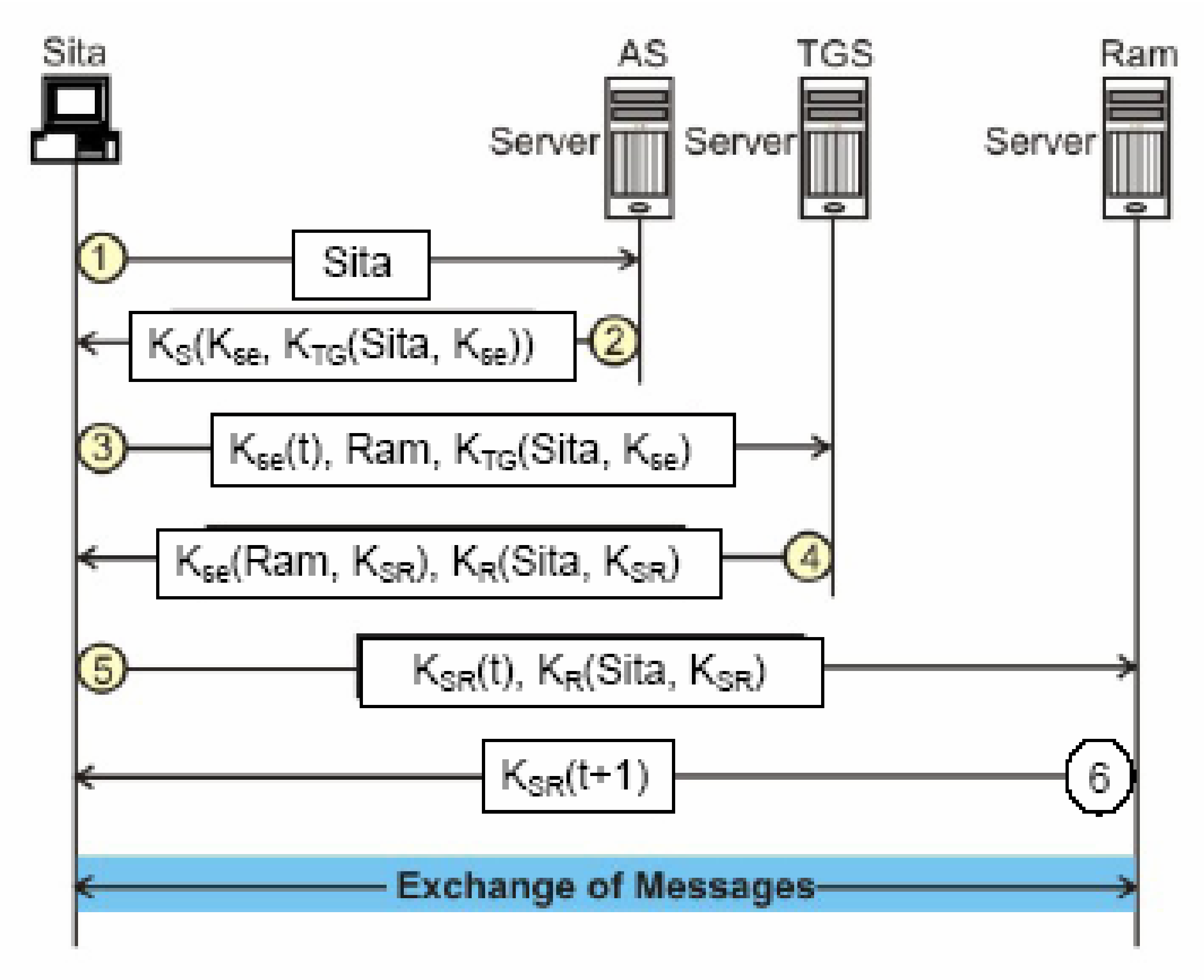

Sita
AS
TGS
Ram
Server
Server
Server
1
Sita
$K_S(K_{SE}, K_{TG}(Sita, K_{SE}))$
2
3
$K_{SE}(t)$, Ram, $K_{TG}(Sita, K_{SE})$
4
$K_{SE}(Ram, K_{SR})$, $K_R(Sita, K_{SR})$
5
$K_{SR}(t)$, $K_R(Sita, K_{SR})$
$K_{SR}(t+1)$
6
Exchange of Messages

Figure 8.2.12 The Kerberos Protocol

8.2.8 Application Layer Security

Based on the encryption techniques we have discussed so far, security measures can be applied to different layers such as network, transport or application layers. However, implementation of security features in the application layer is far simpler and feasible compared to implementing at the other two lower layers. In this subsection, a protocol known as *Pretty Good Privacy (PGP)*, invented by Phil Zinmermann, that is used in the application layer to provide all the four aspects of security for sending an email is briefly discussed. PGP uses a combination of private-key and public key for privacy. For integrity, authentication and nonrepudiation, it uses a combination of hashing to create digital signature and public-key encryption as shown in Fig. 8.2.13.

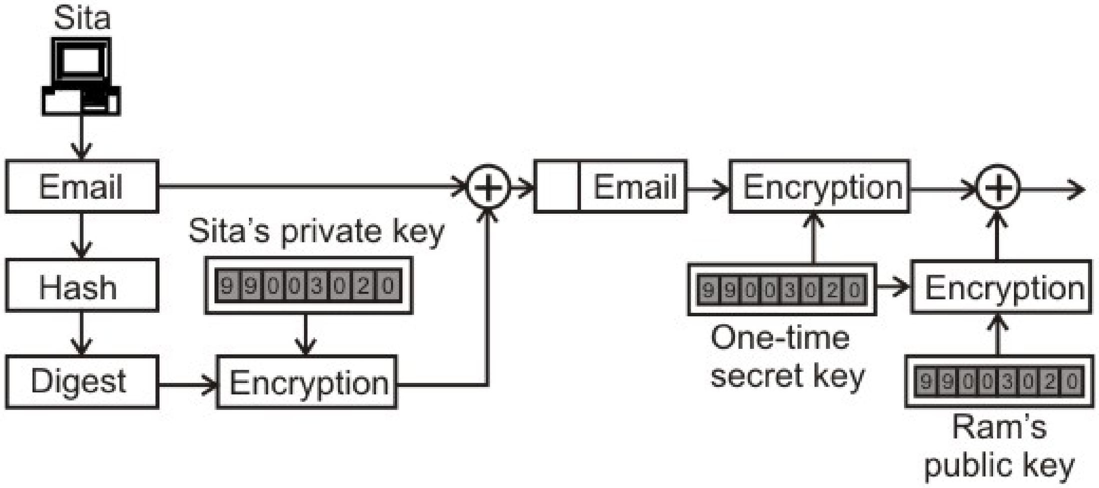


Figure 8.2.13 (a) Sender site of the PGP

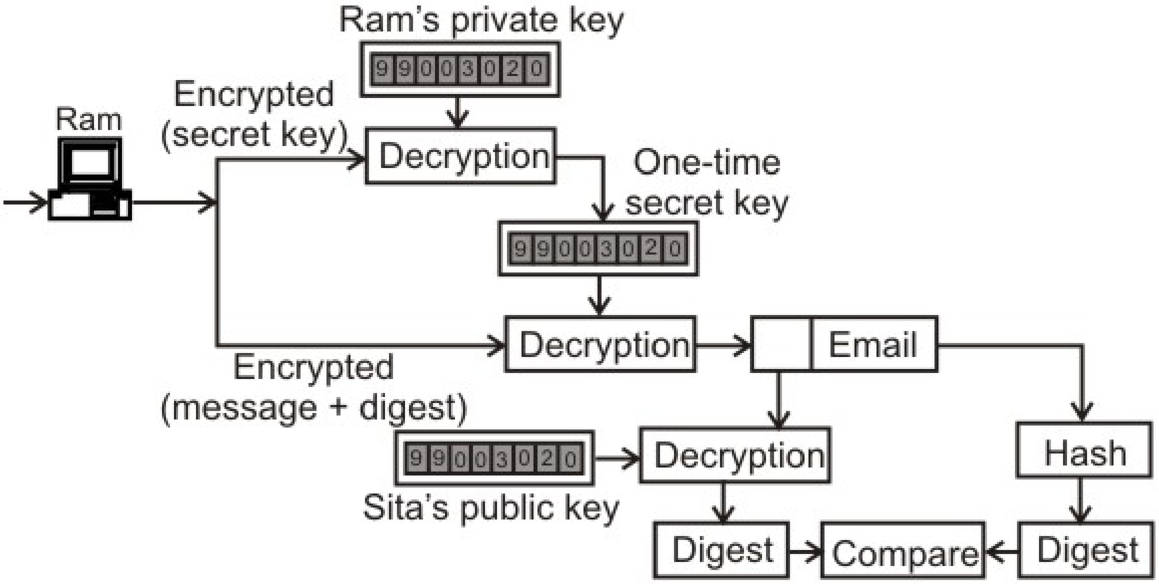


Figure 8.2.13 (b) Receiver site of the PGP

8.2.9 Virtual Private Network (VPN)

With the availability of huge infrastructure of public networks, the *Virtual Private Network (VPN)* technology is gaining popularity among enterprises having offices distributed throughout the country. Before we discuss about the VPN technology, let us first discuss about two related terms: *intranet* and *extranet*.

Intranet is a private network (typically a LAN) that uses the internet model for exchange of information. A private network has the following features:

- It has limited applicability because access is limited to the users inside the network
- Isolated network ensures privacy
- Can use private IP addresses within the private network

Extranet is same as the intranet with the exception that some resources can be allowed to access by some specific groups under the control of network administrator.

Privacy can be achieved by using one of the three models: Private networks, Hybrid Networks and Virtual Private Networks.

Private networks: A small organization with a single site can have a single LAN whereas an organization with several sites geographically distributed can have several LANs connected by leased lines and routers as shown in Fig. 8.2.14. In this scenario, people inside the organization can communicate with each other securely through a private internet, which is totally isolated from the global internet.

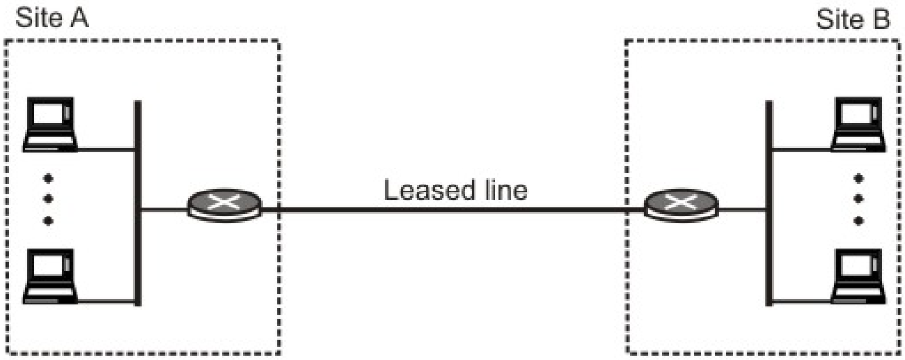


Figure 8.2.14 Private network with two LAN sites

Hybrid Networks: Many organizations want privacy for inter-organization level data exchange, at same time they want to communicate with others through the global internet. One solution to achieve this is to implement a hybrid network as shown in Fig. 8.2.15. In this case, both private and hybrid networks have high cost of implementation, particularly private WANs are expensive to implement.

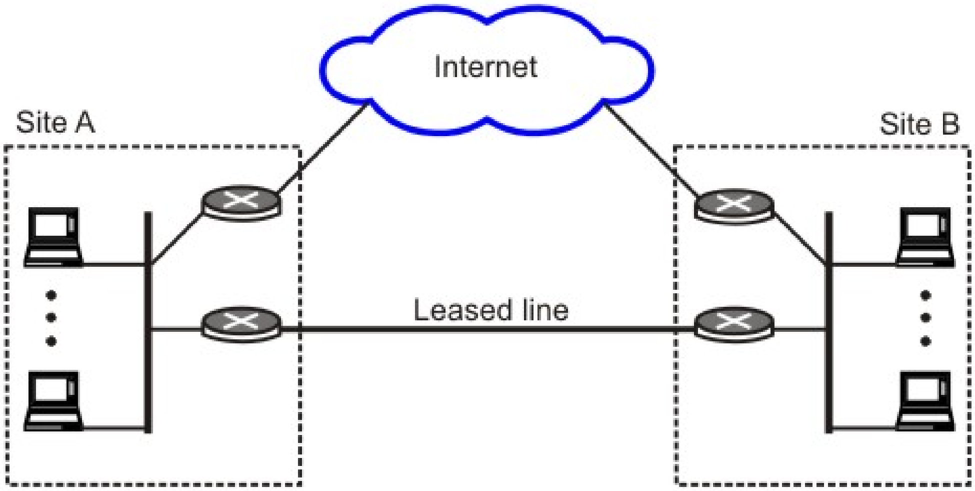


Figure 8.2.15 Hybrid network with two LAN sites

Virtual Private Networks (VPN): VPN technology allows both private communication and public communications through the global internet as shown in Fig. 8.2.16. VPN uses IPSec in the tunnel mode to provide authentication, integrity and privacy. In the IPSec tunnel mode the datagram to be sent is encapsulated in another datagram as payload. It requires two sets of addressing as shown in Fig. 8.2.17.

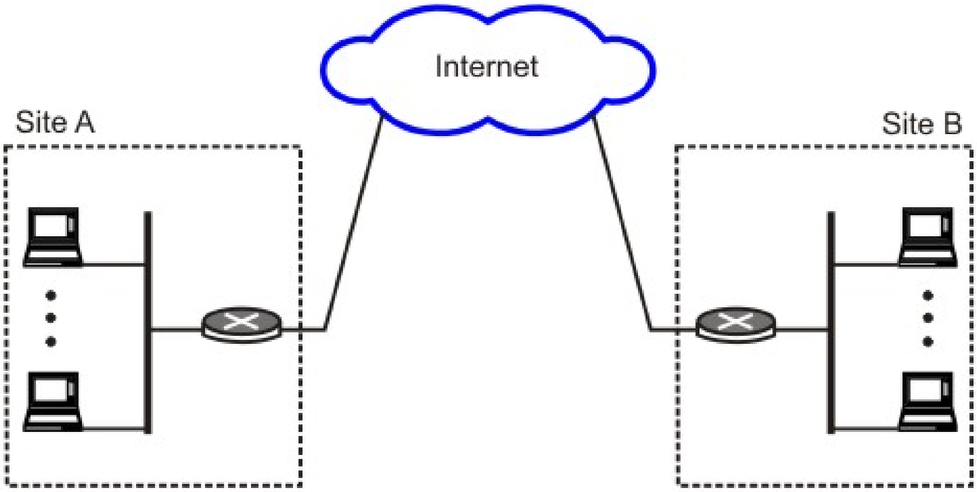
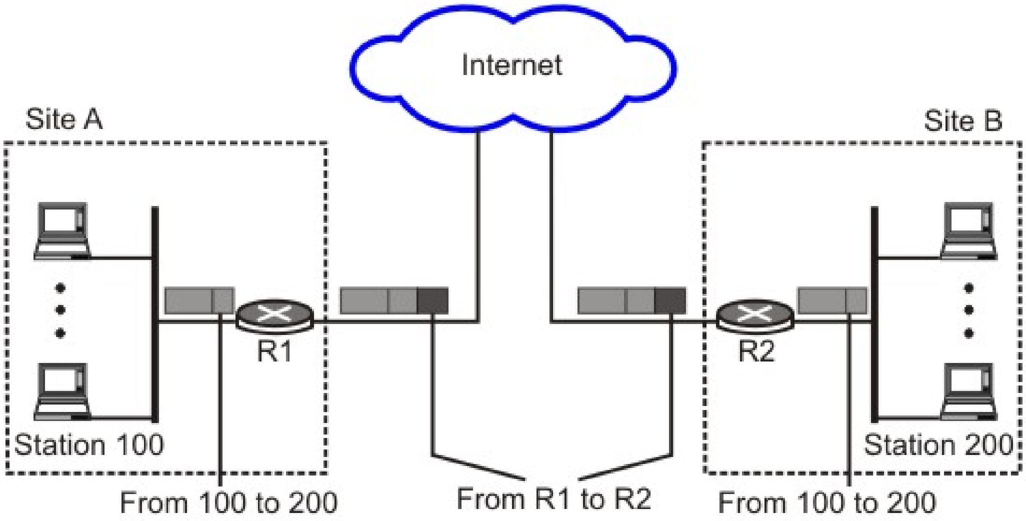


Figure 8.2.16 VPN linking two LANs



New IP Header	IPSec Header	IP Header	Rest of the packet

.

Figure 8.2.17 VPN linking two LANs

Review Questions

1.What are the four services required for secured communication?

Ans: The four services required for secured communication are: privacy, integrity, authentication and nonrepudiation.

2. What is nonce?

Ans: The nonce is a large random number that is used only once for the purpose of user authentication.

3. Explain the operation of the Diffie-Hellman protocol with an example.

Ans: Although the algorithm works on l;arge numbers, it is illustrated with smaller numbers in this example.
Let N = 23 and G = 7.
Sita chooses x = 5 and calculates R1 = 7^5Mod23 = 17
Sita sends 17 to Ram.
Ram chooses y = 3 and calculates R2 = 7^3Mod23 = 21
Ram sends 21 to Sita
Ram calculates K = 17^3Mod 23 = 14
Sita Calculates K = 21^5Mod23 = 14

4. Explain the function of Kerberos.

Ans: Kerberos is a popular technique for key distribution. The kerberos is an authentication protocol and at the same time acts as a Key Distribution Center. It requires an authentication server and a ticket-granting server in addition to the real data server.

5. What is VPN?

Ans: VPN allows private communication through public internet. It is essentially a logical (virtual) network within a conventional network. It makes use of cryptography (IPSec in tunnel mode) to perform private communication through insecure and public internet.