CHAPTER 1
NETWORK SECURITY

1.1. Introduction

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message [1].

Network security problems can be divided roughly into four closely intertwined areas: confidentiality, authentication, non – repudiation, and integrity control. This is what usually comes to mind when people think about network security.

Network Security and Data Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well.

When transferring ciphertext over a network, it is helpful to have a secure network. This will allow for the ciphertext to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks.

The relationship of network security and data security to the Open System Interconnection (OSI) model is shown in figure 1.1. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. The user can possibly choose different methods of data security [1].

Network security is mostly contained within the physical layer. Layers above the physical layer are also used to accomplish the network security required.

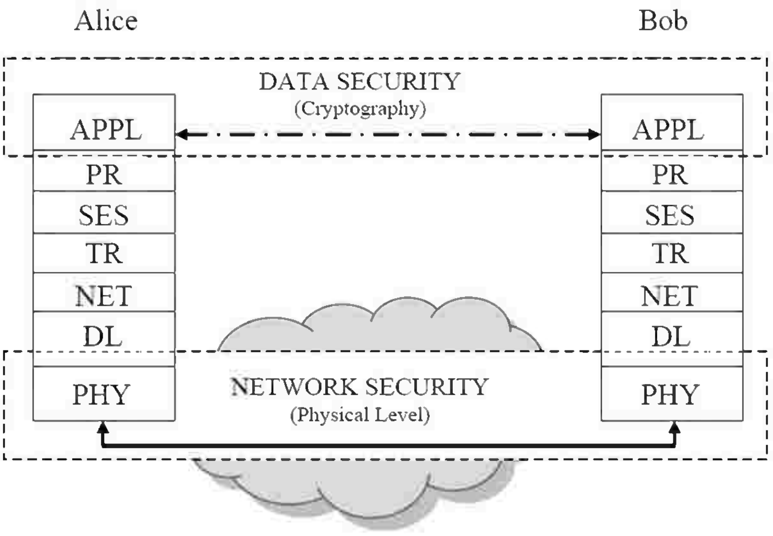


Figure 1.1. Relation between Data Security and Network Security based on OSI Model [1]

Internet Architecture and Vulnerable Security Aspects

Fear of security breaches on the internet is causing organizations to use protected private networks or intranets . Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol (IP). These security mechanisms allow for the logical protection of data units that are transferred across the network, the security architecture of IP, known as IP Security or IPSec, covers the current version of IP (IPv6) as well as the version (IPv4) [1,2].

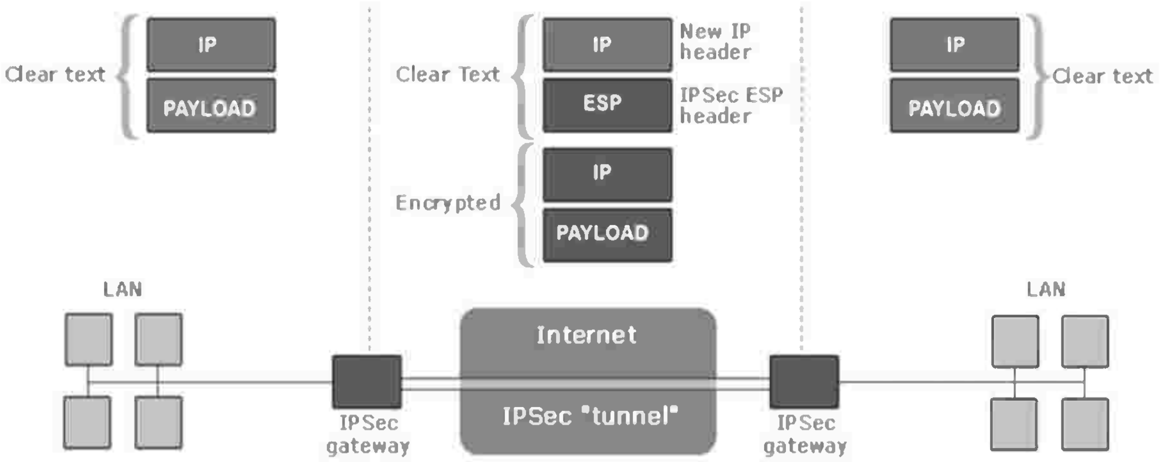


Figure 1.2. IPSec contains gateways and tunnel in order to secure communications

1.2. IP Security Overview

IPSec is an IETF standard that employs the cryptographic mechanisms on the network layer; authentication of every IP packet, verification of data integrity for each packet and confidentiality of packet payload. IPSec consists of open standards for securing private communications and scales from small to very large networks.

IPSec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet. IPSec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or Security Association. IPSec provides the rules while existing algorithms provide the encryption, authentication, key management [3].

Definition and Protocols

IPSec is a set of security protocols and algorithms used to secure data at the network layer. Companion security architecture specifies how IPSec secures data [3,4].

Following is a long and growing list of current Request For Comment (RFC) that concern IPSec:

- RFC 1829: The ESP DES-CBC Transform
- RFC 1851: The ESP Triple DES Transform
- RFC 2085: HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2207: RSVP Extensions for IPSec Data Flows
- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408: Internet Security Association and Key Management Protocol(ISAKMP)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPSec
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2539: Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
- RFC 2631: Diffie-Hellman Key Agreement Method
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 2875: Diffie-Hellman Proof-of-Possession Algorithms
- RFC 3070: Layer Two Tunneling Protocol (L2TP) over Frame Relay
- RFC 3104: RSIP Support for End-to-End IPSec
- RFC 3145: L2TP Disconnect Cause Information
- RFC 3193: Securing L2TP Using IPSec
- RFC 3301: Layer Two Tunneling Protocol (L2TP):ATM access network extensions

Applications of IPSec

IPSec provides the capability to secure communications across Local Area Network (LAN), across private and public Wide Area Networks (WAN), and across the Internet [4]. Examples of its use include the following:

- **Secure branch office connectivity over the Internet**: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- **Secure remote access over the Internet**: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
- **Establishing extranet and intranet connectivity with partners**: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- **Enhancing electronic commerce security**: Even though some web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

the principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level. Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

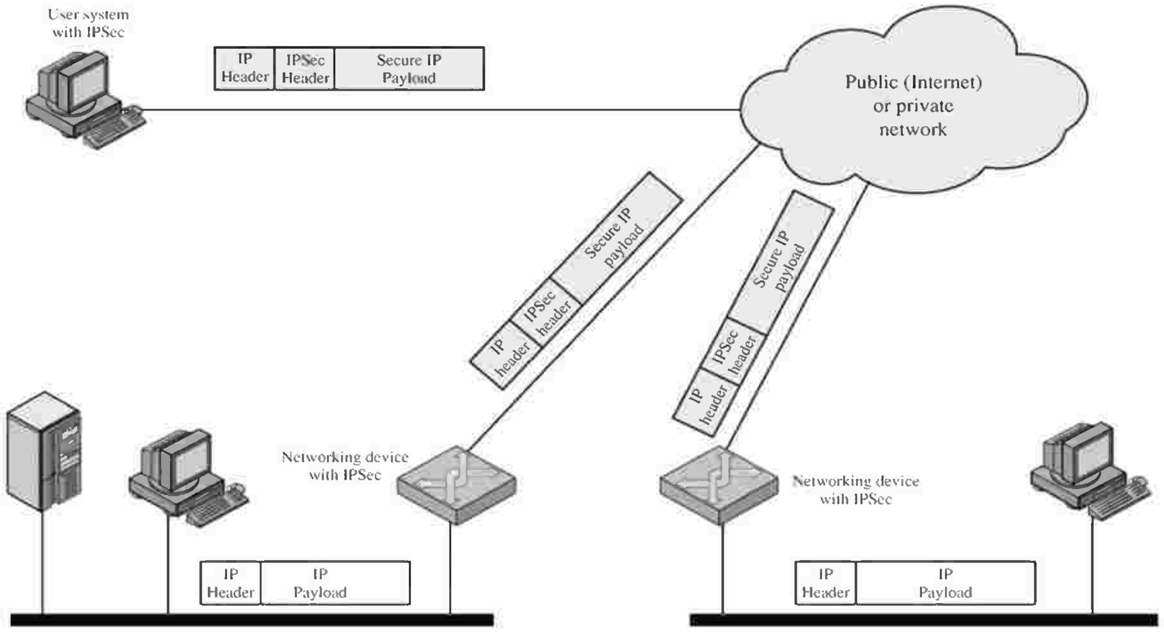


Figure 1.3. IP Security Scenario [3]

IPSec Security Features

1- **Data confidentiality:** The IPSec sender can encrypt packets before transmitting them across a network, thereby preventing anyone from eavesdropping on the communication. If intercepted, the communications cannot be read.

2- **Data integrity:** The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that there has been no alteration to the data during transmission.

3- **Data origin authentication**: The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.

4- **Anti-replay:** Anti-replay protection verifies that each packet is unique, not duplicated. IPSec packets are protected by comparing the sequence number of the received packets and a sliding window on the destination host, or security gateway. A packet whose sequence number is before the sliding window is considered late or a duplicate. Late and duplicate packets are dropped.

1.3. IPSec Protocols

IPSec consists of three primary protocols to help implement the overall IPSec architecture:

- Internet Key Exchange (IKE)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Together, these three protocols offer the various IPSec features. Every IPSec over Virtual Private Network (VPN) uses some combination of these protocols to provide the desired features for the VPN [3,5].

1.3.1. IKE

A secure IPSec connection between two devices can initially be established by configuring encryption keys in both devices. However, the failure to periodically change these keys makes the network susceptible to brute-force password attacks. The need to manually change the IPSec keys every hour or every day can prove troublesome. If dozens or hundreds of IPSec connections are in use, manual key maintenance can be a nightmare.

1.3.1.1. IKE Protocols

The IKE protocol is a means of dynamically exchanging IPSec parameters and keys. IKE makes IPSec scalable by automating the key exchange/update process needed to repel password attacks against the IPSec sessions. IKE helps to automatically establish Security Associations (SAs) between two IPSec endpoints. SA is an agreement between two peers engaging in a crypto exchange. This agreement includes the type and strength of the encryption algorithm used to protect the data also includes the method and strength of the data authentication and the method of creating new keys for that data protection [3,4].

IKE actually uses other protocols to perform peer authentication (will be discussed later) and key generation:

- **ISAKMP**: defines procedures on how to establish, negotiate, modify, and delete SAs. All parameter negotiation is handled through ISAKMP, such as header authentication and payload encapsulation ISAKMP performs peer authentication, but it does not involve key exchange [2,4].
- **Oakley:** The Oakley Key Determination Protocol uses the Diffie-Hellman algorithm to manage key exchanges across IPSec SAs. Diffie-Hellman is a cryptographic protocol that permits two end points to exchange a shared secret over an insecure channel [2,4].
- **SKEME:** The key exchange protocol that supports key exchange based on public keys of the parties and the strong security of the Diffie-Hellman mechanism. It provides key management for the IP layer security protocols and key management solution for other security applications over Internet [3].

1.3.1.2. IKE Phases

The IKE protocol/process is broken into two phases, which create a secure communications channel between two IPSec endpoints. Although there are two primary and mandatory IKE phases, there is an optional third phase [3]. The three phases are described here:

- **IKE phase 1** is one of the mandatory IKE phases. A bidirectional SA is established between IPSec peers in phase 1. This means that data sent between the end devices uses the same key material. Phase 1 may also perform peer authentication to validate the identity of the IPSec endpoints. There are two IKE modes available for IKE phase 1 to establish the bidirectional SA main mode and aggressive mode. IKE modes are described in the next section; Phase 1 consists of parameter negotiation, such as hash methods and transform sets. The two IPSec peers must agree on these parameters or the IPSec connection cannot be established [3,4].
- **IKE phase 1.5** is an optional IKE phase. Phase 1.5 provides an additional layer of authentication, called Xauth, or Extended Authentication. IPSec authentication provided in Phase 1 authenticates the devices or endpoints used to establish the IPSec connection. However, there is no means of validating the users behind the devices. A preconfigured IPSec device can be used by both friends and foes. Xauth forces the user to authenticate before use of the IPSec connection is granted [3].
- **IKE phase 2** is the second mandatory IKE phase. Phase 2 implements unidirectional SAs between the IPSec endpoints using the parameters agreed upon in Phase 1. The use of unidirectional SAs means that separate keying material is needed for each direction. Phase 2 uses IKE quick mode to establish each of the unidirectional SAs [3,4].

1.3.1.3. IKE Modes

IKE consists of three different modes main, aggressive and quick mode. IKE phase 1 has a choice of two modes main or aggressive, while IKE phase 2 always uses the same mode quick. For one IPSec session between two devices, either main or aggressive mode is used for IKE phase 1, and quick mode is always used for IKE phase 2. The IKE modes are described in the sections that follow. The third optional IKE mode is phase 1.5, which is optionally used for extended authentication [3].

- **IKE Main Mode**

  In the main mode, an IKE session begins with the initiator sending a proposal or proposals to the responder. These proposals define which encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced so the main mode squeezes the IKE SA negotiation into six messages exchanged between the IPSec peers and they are broken into three pairs:

  – IPSec parameters and security policy: The initiator sends one or more proposals, and the responder selects the appropriate one.

  – Diffie-Hellman public key exchange: Public keys are sent between the two IPSec endpoints.

  – ISAKMP session authentication: Each end is authenticated by the other.

- **IKE Aggressive Mode**

  Aggressive mode is an abbreviated version of main mode but the six messages of the IKE SA negotiation in the main mode are condensed into three messages:

  – The initiator sends all data, including IPSec parameters, security policies, and Diffie-Hellman public keys.

  – The responder authenticates the packet and sends the parameter proposal, key material, and identification back.

  – The initiator authenticates the pack

  in aggressive mode negotiation is quicker, and the initiator and responder ID pass in plaintext.

- **IKE Quick Mode**

  Quick mode is used during IKE phase 2. The negotiation of quick mode is protected by the IKE SA negotiated in Phase 1. Such an option is not available during main or aggressive modes, because their function is to establish the first SA. Quick mode negotiates the SAs used for data encryption across the IPSec connection. It also manages the key exchange for those SAs [2,3].

1.3.1.4. Extended Authentication

Xauth is based on the IKE protocol. Xauth allows AAA methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange [3].

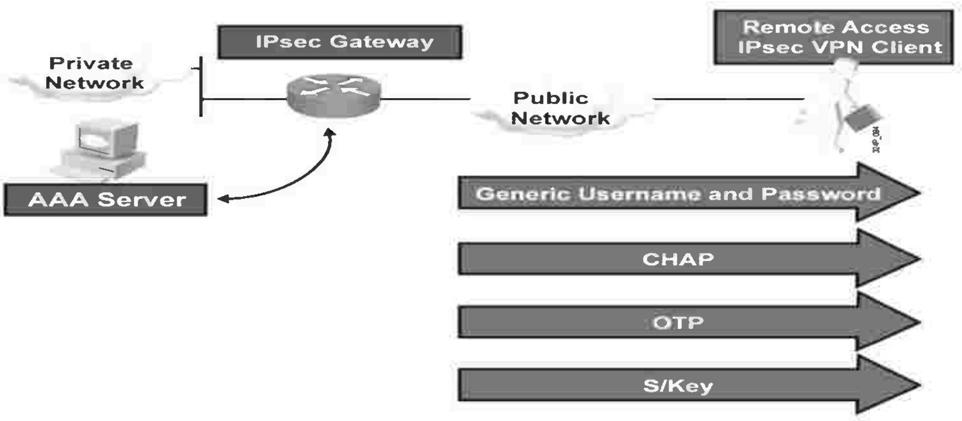


Figure 1.4. Extended Authentication [3]

Xauth does not replace IKE. IKE allows for device authentication while Xauth allows for user authentication, which occurs after IKE device authentication. A user authentication option can be a generic username and password, Challenge Hand Shake Authentication Protocol (CHAP), One Time Password (OTP), or S/Key.

1.3.1.5. IKE Features

IKE automatically negotiates IPSec SAs and enables IPSec secure communications without costly manual preconfiguration [5].

IKE includes these features:

- Eliminates the need to manually specify all of the IPSec security parameters at both peers
- Allows specification for a lifetime for the IPSec SA
- Allows encryption keys to change during IPSec sessions
- Allows IPSec to provide anti-replay services
- Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation
- Allows dynamic authentication of peers

1.3.2. AH

The AH provides support for data integrity and authentication of IP packets. The data integrity feature ensures that undetected modification to a packet's content in transit is not possible. The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly, it also prevents the address spoofing attacks. The AH also guards against the replay attack. Where a replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence [3,4].

AH authentication can achieved by applying a keyed one-way hash function to the packet, creating a hash or message digest. The hash is combined with the text and transmitted. Changes in any part of the packet that occur during transit are detected by the receiver when it performs the same one-way hash function on the received packet and compares the value of the message digest that the sender has supplied. The fact that the one-way hash also involves the use of asymmetric key between the two systems means that authenticity is guaranteed.

Table 1.1. Hash Algorithm

Hash Algorithms	Input	Output	Used by IPSec
Message Digest 5 (MD5)	Variable	128 bits	128 bits
Secure Hash Algorithm (SHA-1)	Variable	160 bits	First 96 bits

Note, the AH function is applied to the entire datagram, except for any mutable IP header fields that change in transit, such as TTL fields that are modified by the routers along the transmission path.

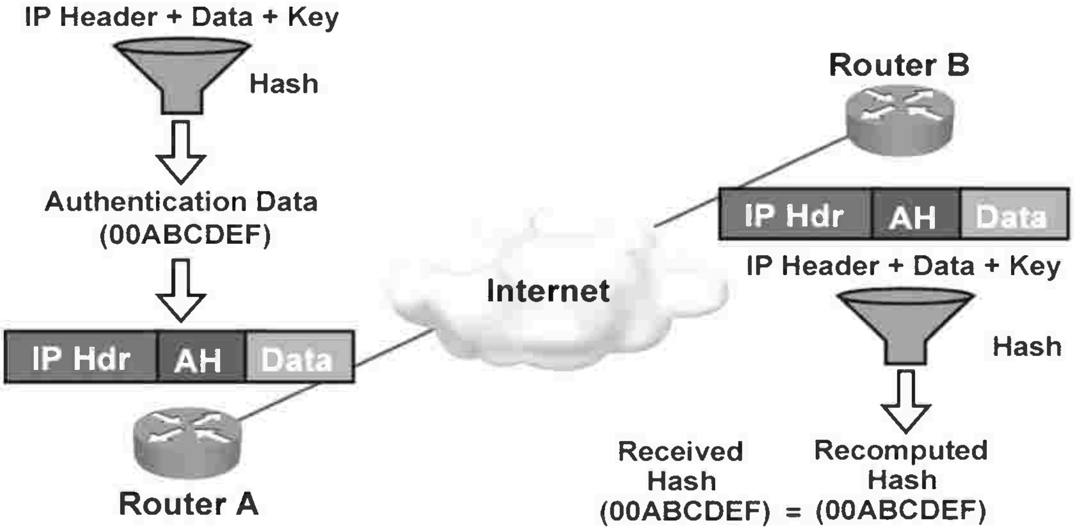


Figure 1.5. AH supports MD5 and SHA-1 algorithms [3].

AH works as follows:

Step 1 The IP header and data payload is hashed.

Step 2 The hash is used to build an AH header, which is appended to the original packet.

Step 3 The new packet is transmitted to the IPSec peer router.

Step 4 The peer router hashes the IP header and data payload.

Step 5 The peer router extracts the transmitted hash from the AH header.

Step 6 The peer router compares the two hashes. The hashes must exactly match. Even if one bit is changed in the transmitted packet, the hash output on the received packet will change and the AH header will not match.

1.3.3. ESP

The ESP provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service. So, between two security gateways, the original payload is well protected because the entire original IP datagram is encrypted. An ESP header and trailer are added to the encrypted payload. With ESP authentication, the encrypted IP datagram and the ESP header or trailer are included in the hashing process. Lastly, a new IP header is appended to the front of the authenticated payload. The new IP address is used to route the packet through the Internet [3,4].

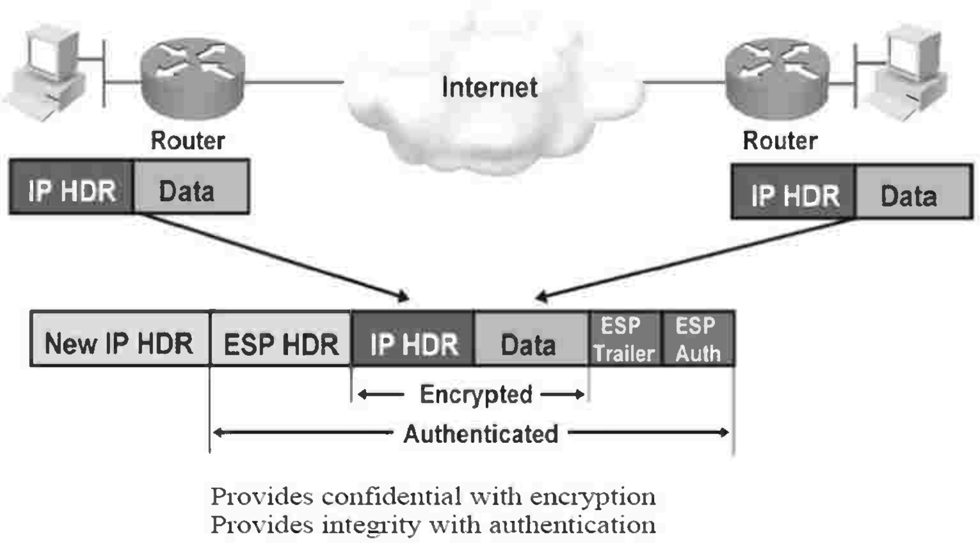


Figure 1.6. ESP Protocol

When both ESP authentication and encryption are selected, encryption is performed first before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can authenticate inbound packets.

1.3.3.1. ESP Encryption Algorithms

The purpose of encryption is to make data unreadable for everyone except those specified. A mathematical function is applied to the plaintext and converts it to an encrypted ciphertext [3]. These two types of mathematical functions are used:

Symmetric Algorithm

A form of cryptosystem in which encryption and decryption are performed using the same secret key (the sender and receiver share the same key) [4]. Also known as conventional encryption. The main advantages of symmetric key encryption; high speed (high throughput) and using a short key size (> 128 bits). And its disadvantages are represented in keeping the shared key secret at both parts which known as key distribution problem, not support digital signature, and the key management problem where in a large network there are many key pairs to be managed (for n nodes the required number of keys are

$$\left(\frac{n\times(n-1)}{2}\right)$$

Examples: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES).

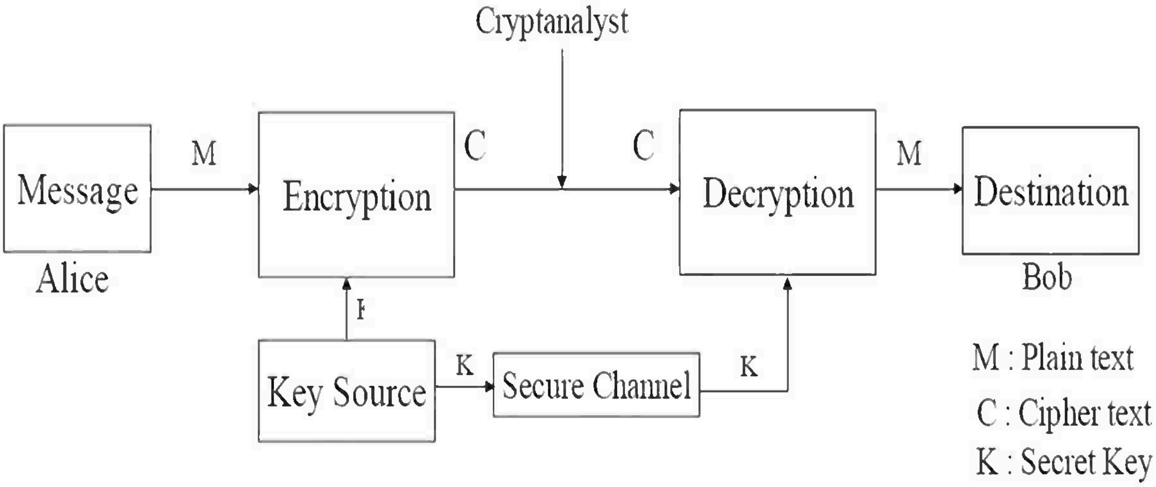


Figure 1.7. Symmetric Algorithm

Asymmetric Algorithm

A form of cryptosystem in which encryption and decryption are performed using two different keys (pair of keys); one is referred to as the public key and known to all, and the other one is referred to as the private key. And the pair of keys are related by a mathematical relation but, it is computationally infeasible to determine the private key only from knowledge of the public key. It is known as public key cryptography [4].

The main advantages of public key cryptography are; easy key distribution as only the private key must be kept secret, easy key management on a network, where in a large network the required number of keys is smaller than symmetric-key scenario (for n nodes need n pairs of keys). Otherwise its disadvantages are; small throughput, larger Key size (160-1024 bits), and Public key schemes have their security based on some hard mathematical problems.

Example: Rivest, Shamir, and Adleman (RSA).

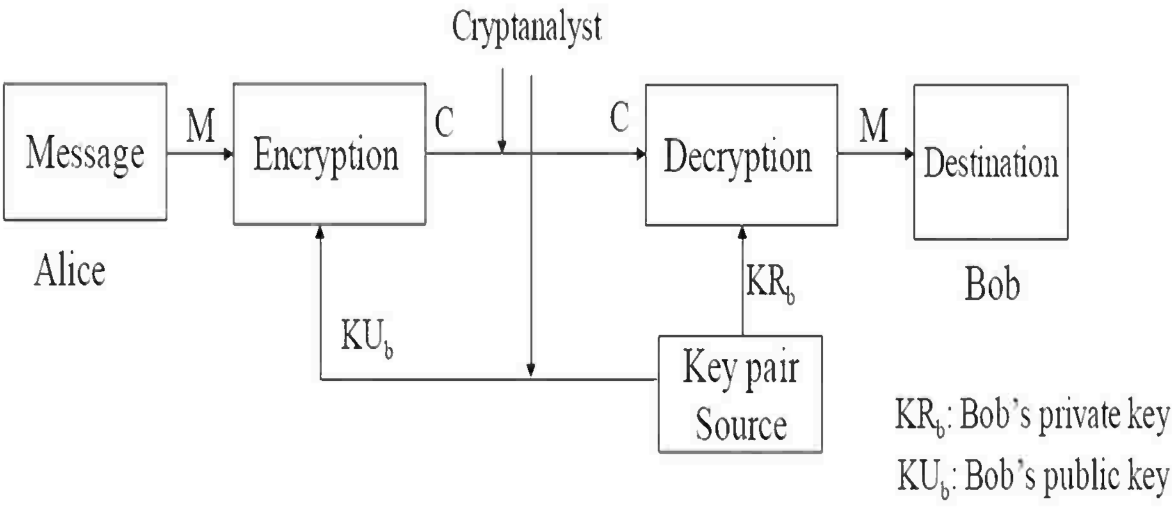


Figure 1.8. Asymmetric Algorithm.

1.3.3.2. ESP Authentication

ESP is used alone or in combination with AH. ESP with AH also provides integrity and authentication of the datagrams. First, the payload is encrypted. Next, the encrypted payload is sent through a hash algorithm: MD5 or SHA-1. The hash provides origin authentication and data integrity for the data payload [3,4].

Message Authentication and Integrity Check

Data is transported over the public Internet. Potentially, this data could be intercepted and modified. To guard against this, each message has a hash attached to the message. A hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with. However, if there is no match, the message was altered.

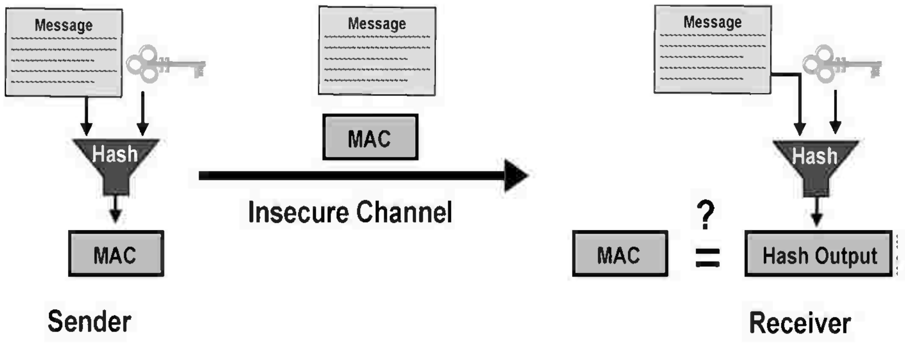


Figure 1.9. Message Authentication and Integrity Check

HMAC is used for message authentication and integrity check. HMAC can be used with any iterative cryptographic hash function, for example, MD5 or SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. HMAC also uses a secret key for calculation and verification of the message authentication values. MD5 and SHA-1 are examples of such hash functions.

Hash Functions

There are two hash functions for IPSec: MD5 and SHA-1. Both hash functions take some variable length input message and create a fixed-length hash.

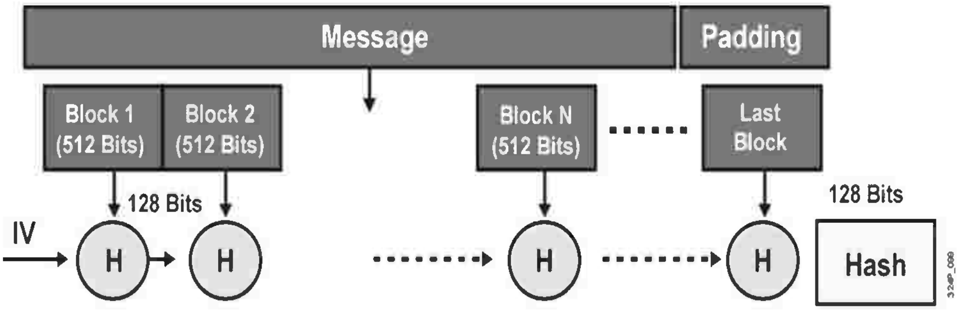


Figure 1.10. Hash Function

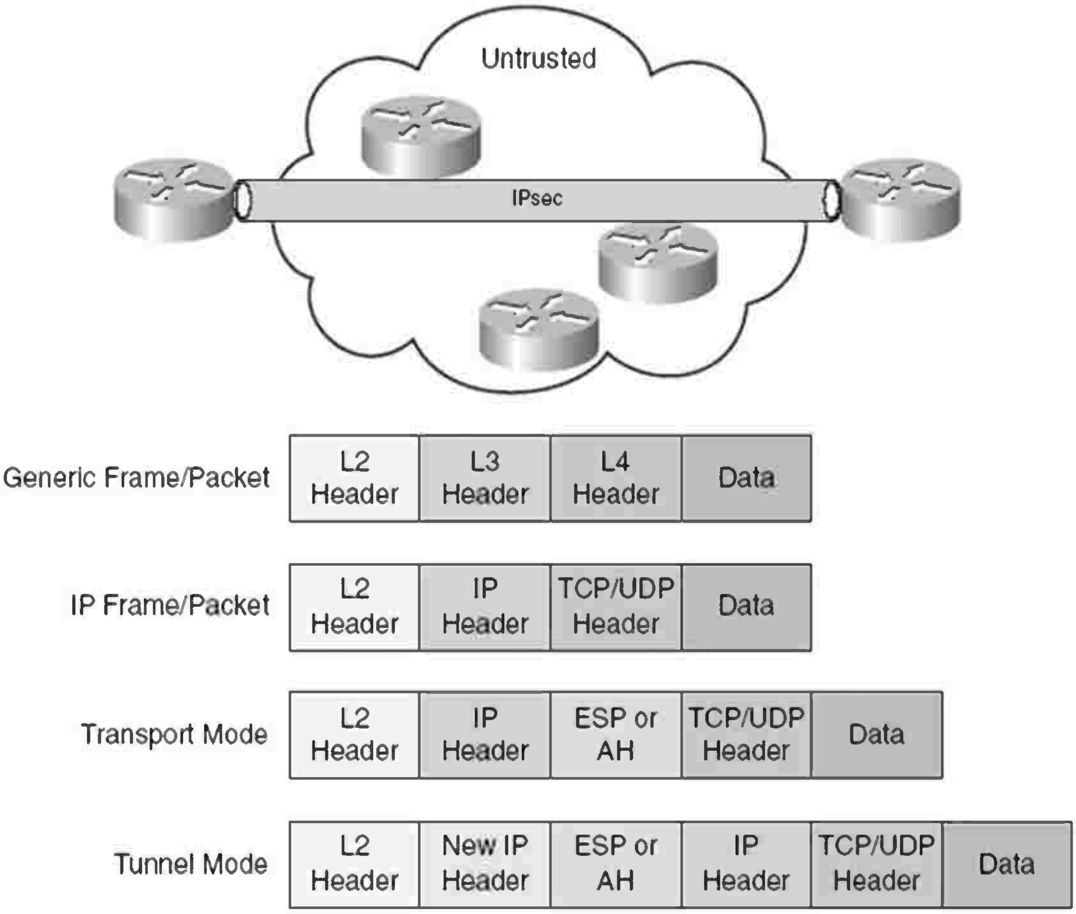
MD5 creates a 128-bit hash, while SHA-1 creates a 160-bit hash. In the case of SHA-1, only 96 bits of this hash are used for IPSec. The initialization vector is used as an initial value to start creating a hash.

1.4. IPSec Modes

IPSec defines two modes that determine the extent of protection offered to the original IP packet. Remember that the IPSec header follows an IP header, because it is referenced by an IP protocol number. As such, encryption and integrity services can be offered only beyond the IP header [3,4]. The two IPSec modes are *tunnel mod*e and *transport mode.*

When IPSec headers are simply inserted in an IP packet after the IP header, it is called *transport mode*. In transport mode, the original IP header is exposed and unprotected. Data at the transport layer and higher layers benefits from the implemented IPSec features. Another way to think of this is that transport mode protects the transport layer and up. As such, when the IPSec packet travels across an untrusted network, all of the data within the packet is safe based on the IPSec services selected. Devices in the untrusted network can see only the actual IP addresses of the IPSec participants.

IPSec offers a second mode called *tunnel mode*. In tunnel mode, the actual IP addresses of the original IP header, along with all the data within the packet, are protected. Tunnel mode creates a new external IP header that contains the IP addresses of the tunnel endpoints such as routers or VPN Concentrators. The exposed IP addresses are the tunnel endpoints, not the device IP addresses that sit behind the tunnel end points. Figure 1.11 shows the two IPSec modes compared to a “normal” IP packet.



Generic Frame/Packet	L2 Header	L3 Header	L4 Header	Data		
IP Frame/Packet	L2 Header	IP Header	TCP/UDP Header	Data		
Transport Mode	L2 Header	IP Header	ESP or AH	TCP/UDP Header	Data	
Tunnel Mode	L2 Header	New IP Header	ESP or AH	IP Header	TCP/UDP Header	Data

Figure 1.11. IPSec Modes

1.5. IPSec Headers

Both AH and ESP are implemented by adding headers to the original IP packet. The IPSec VPN uses AH or ESP, or both, but the use of AH along with ESP has no appreciable benefit. Note that ESP implements all of the IPSec features, while AH offers all features except data confidentiality. Both AH and ESP are recognized by their particular IP protocol numbers, which makes each a transport layer protocol. AH and ESP are recognized by their respective IP protocol numbers (51 and 50).

The placement of these headers means that the IPSec features that they provide confidentiality and integrity can only be for portions of the IP packet that follow the AH or ESP header. The ESP and AH headers are applied to an existing IP packet. Both transport and tunnel modes are shown for comparison [3].

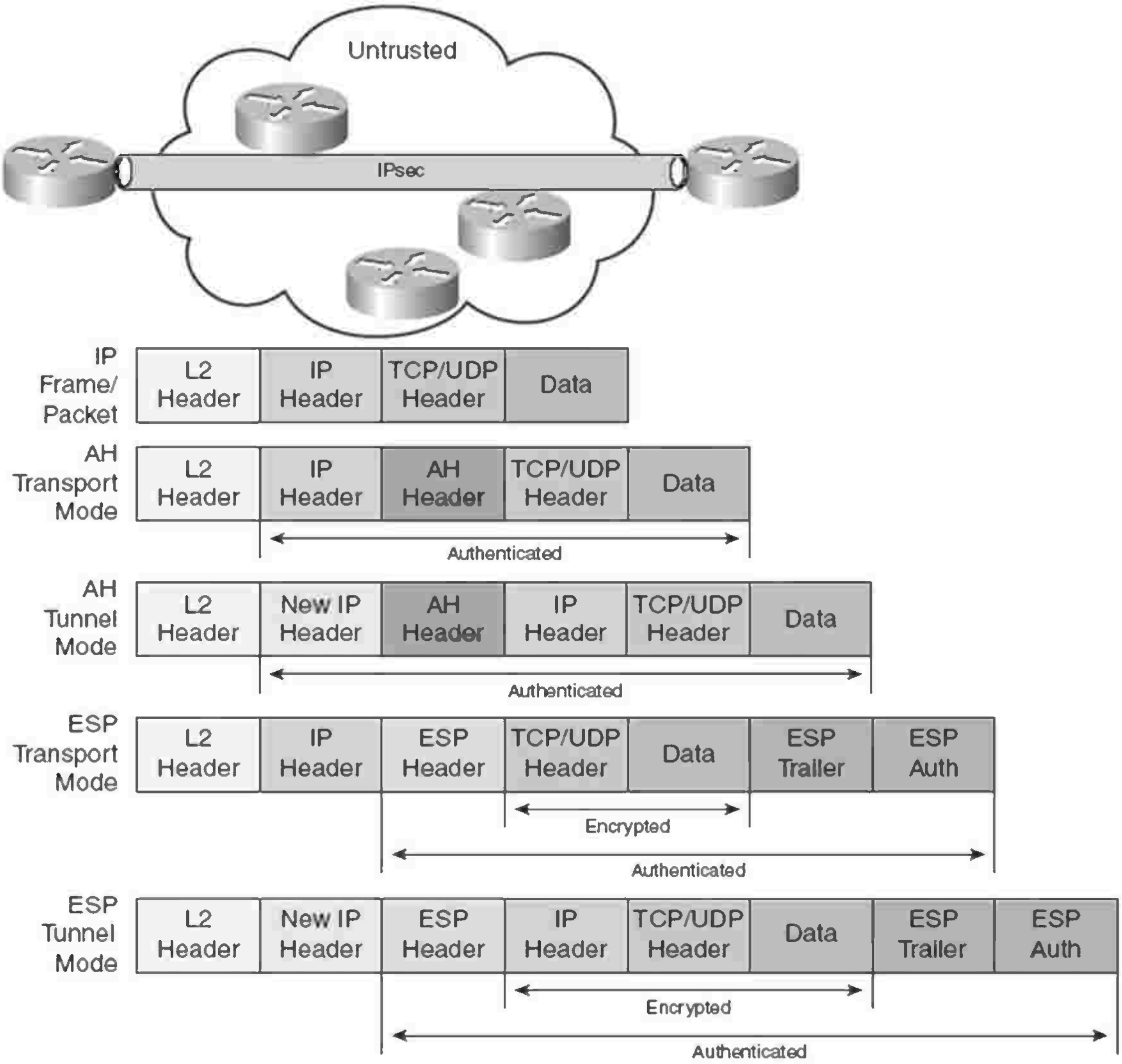


Figure 1.12. AH and ESP Headers

As shown in the figure 1.12, AH authenticates the entire packet after the Layer 2 header. If ESP authentication is used, the outer IP header is not authenticated. Also note that if ESP performs both encryption and authentication, encryption occurs first, and then the encrypted contents along with the ESP headers are authenticated.

1.6. Peer Authentication

As described, IPSec has the capability to protect data in transit. It can encrypt the data to prevent those in the middle from seeing it (data confidentiality), and it can ensure that the data has not been modified while in flight (data integrity). However, these functions lose their appeal if one VPN endpoint is not sure of whom the other endpoint truly is. IPSec can secure the data transfer, but before such services are employed, the endpoints of the IPSec VPN must be validated [3].

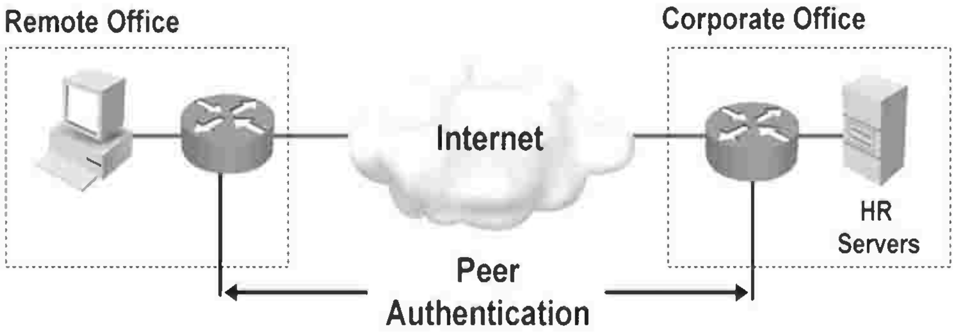


Figure 1.13. Peer Authentication

The concept of peer authentication certifies that the remote IPSec endpoint is truly who it says it is [3,4]. There are five different methods to authenticate an IPSec peer:

- **Username and password:** A username and password must be predefined and preconfigured in the IPSec endpoints. As such, they are typically used for long periods of time. They are generally not considered very safe, because if someone guesses or learns the username/password combination, that person can establish an IPSec connection with you.

- **One Time Password (OTP):** is typically implemented as Personal Identification Number (PIN) or a Transaction Authentication Number (TAN), such numbers are good for only one IPSec instantiation. If someone were to learn of an old OTP, it would be useless to establish a new IPSec connection.

- **Biometrics:** Biometric technologies analyze physical human characteristics, such as fingerprints, hand measurements, eye retinas and irises, voice patterns, and facial patterns. Such characteristics are difficult, if not impossible, to duplicate. Any combination of these can be used to authenticate a person, and thus provide assurance of who is at the other end of the IPSec connection.

- **Preshared keys:** Preshared keys are similar to the username/password concept. In this case, a single key (value) is preconfigured in each IPSec peer. Like the username/password, it is important that such manually configured information remain safeguarded. If someone were able to determine the preshared key, they would have the ability to establish an IPSec connection with you.

- **Digital certificates:** Digital certificates are a very popular way to authenticate people and devices. Typically, a digital certificate is issued to a device from a trusted third-party CA. This certificate is only good for the machine it was issued to.

when that device needs to authenticate, it presents its certificate, which is then validated against the third-party CA. If another device attempts to use the certificate, the authentication will fail [3,5].

1.7. Thesis Outline

Chapter 2 introduces the mathematical background to Elementary Number Theory discussing some theories are used in the cryptography systems, prime numbers, Euler's theory, Euler's function and Fermat's little theory. Also discuses summary to Elliptic curves including Group law, Finite fields and Elliptic Curve Domain parameters.

Chapter 3 introduces comparison between the common Public key cryptography algorithms (RSA – ElGamal Cryptography – Elliptic Curve Cryptography) and discusses the modified scheme, Signcryption Scheme, which proposed in 1997 by Zheng to fulfill the signature process and encryption process in one step instead of the traditional way signature – then – encryption with saving in communication over head and computational costs, discusses Signcryption for multi-recipients and its advantages in cost saving .

Chapter 4 introduces proposed scheme "*Modified Elliptic Curve Signcryption*" based on ECDLP and in addition to achieve the functionality of the Signcryption schemes; unforgeability, confidentiality, integrity and non – repudiation it achieves forward security and encrypted message authentication and public verifiability. And discusses the computational costs compared with other modified signcryption schemes and communication overhead which reach 50% .

Chapter 5 employs the proposed scheme in the multi – recipients and compare it with introduced scheme by Zheng (Signcryption for Multiple Recipients) according to cost saving. Also introduces how to apply the proposed scheme on the IPSec mechanism to protect the data over computer networks.

Chapter 6 discuses conclusions and future work of the proposed scheme .