1. Briefly describe the Feistel Cipher encryption and decryption operations. What is the influence of the cipher parameters on the encryption/decryption process.

Encryption:

Split the **plaintext** block into two parts: $M = L_0 \mid R_0$
Where | is the concatenation operator

For $i = 1 \; to \; n-1$: $L_i = R_{i-1}$; $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$;

Where f is the round function and K_i is the sub-key for the i_{th} step/round
The final step n is $L_n = R_{n-1}$; $R_n = L_{n-1}$
And the encrypted message (ciphertext) is $E = L_n \mid R_n$

Decryption is performed in the reverse order, namely,
split the cyphertext in two halves: $E = L_0 \mid R_0$

For $i = 1 \; to \; n-1$: $L_i = R_{i-1}$; $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$;
The final step n is $L_n = R_{n-1}$; $R_n = L_{n-1}$
And the decrypted message, plaintext is: $M = L_n \mid R_n$

Parameters:
Block size: larger block sizes mean greater security but reduce encryption/decryption speed
Key Size: larger key size means greater security but may decrease encryption/decryption speed
Number of rounds: multiple rounds offer increasing security, typically from 10 to 16 rounds
Subkey generation algorithm: greater complexity will lead to greater difficulty of cryptanalysis.
Round function: greater complexity means greater resistance to cryptanalysis.
Ease of analysis: if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities.

2. What is SHA? Where/what for is it used? Briefly describe steps of SHA-512

SHA is a secure hash function used to produce a message digest. For SHA-512, the message digest is 512 bits long

- **Append padding bits:** message is padded (with what?) so that its length is congruent to 896 modulo 1024
  L = (N-1)*1024+896; L mod 1024 = 896 L is represented as an unsigned 128-bit number
- **Append length:** a block of 128 bits is appended to the message and treated as an unsigned 128-bits integer and contains the length of original message. M = M|L
  After that the message has N 1024-bit blocks
- **Initialize hash buffer H:** A 512-bit buffer is used to hold intermediate and final results of the hash function. Note that 512 = 64*8, hence H is 64 bytes long
- **Process message in 1024-bit (128-word) blocks:** The heart of the algorithm is a module that consists of 80 rounds.
  Each round m produces $H_{nm} = G(H_{nm-1}, M_n, K_m)$
  Where K_m is the cryptographic key used in round m
- **Output:** After all N 1024-bit blocks have been processed, the output from the Nth stage is the 512-bit message digest.

3. What is PKIX? What is the principle objective behind it? Briefly describe its Management functions and two protocols

Public-Key Infrastructure

■ PKI Definition:

Hardware, software, people, policies, procedures to create, manage, store, distribute, revoke digital certificates in asymmetric cryptography.

■ Principal objective for developing a PKI is to enable secure, convenient and efficient acquisition of public keys.

PKIX Management Functions

1. Registration

This is the process whereby a user first makes itself known to a CA (directly, or through an RA), prior to that CA issuing a certificate or certificates for that user.

2. Initialization

Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure.

3. Certification

This is the process in which a CA issues a certificate for a user's public key and returns that certificate to the user's client system and/or posts that certificate in a repository.

4. Key pair recovery

Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both.

5. Key pair update

All key pairs need to be updated and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation.

6. Revocation request

An authorized person advises a CA of an abnormal situation requiring certificate revocation.

7. Cross certification

A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates

PKIX Management Protocols

1. Certificate management protocols (CMP) Designed to be a flexible protocol able to accommodate a variety of technical, operational, and business models

2. Certificate management messages over CMS (CMC) s built on earlier work and is intended to leverage existing implementations

4. What is TSL/SSL? Describe details of the SSL Record Protocol operations.

A new layer inserted between transport layer and application layer therefore capable of protecting communication from any application protocol above TCP.

- **The SSL Record Protocol** actually transfer the data
- Provides confidentiality and message integrity
- Defines a set of formats and procedures by which message are handed down from the application layer
- Takes data from application layer, encapsulates into appropriate headers and creates an object called record
- Encrypted records are forwarded to TCP layer

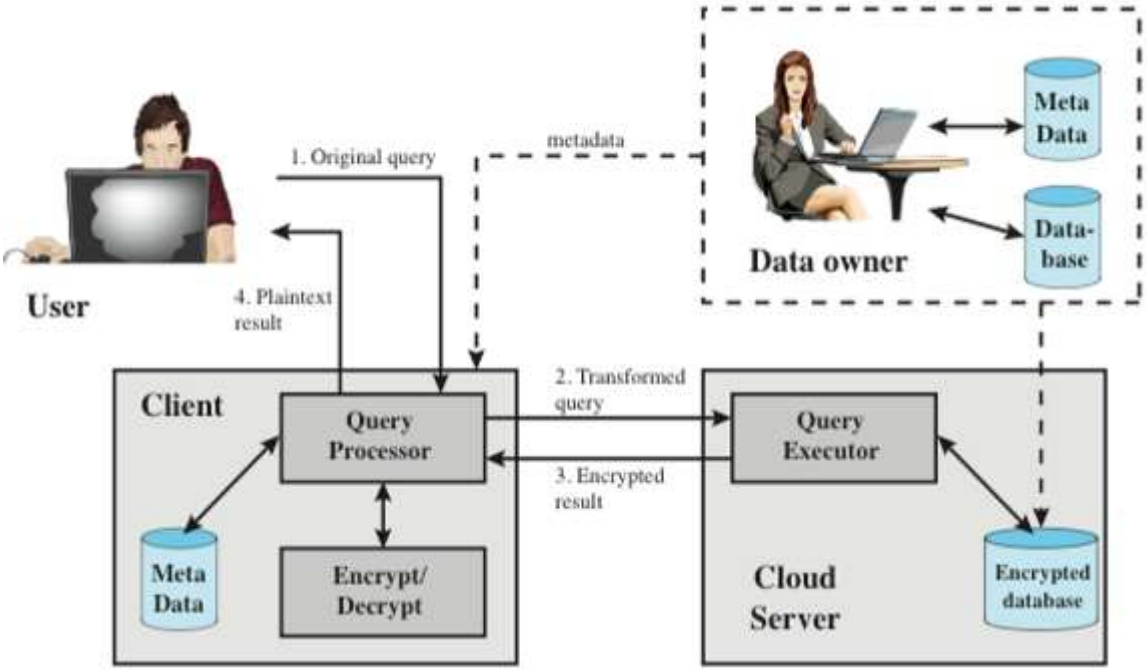
SSL Record Protocol operation involves:

- Fragmentation
  fragments the data in manageable block size (16KB or less)
- Compression
  Optional must be lossless SSLv3 (TLS) does not specify any compression algorithm
- Integrity protection
  compute MAC on the compressed data using SHA-1, MD5 uses a shared secret key negotiated in handshake protocol
- Encryption
  compressed message and MAC are encrypted using symmetric encryption algorithm
  Algorithm permitted: AES, IDEA, RC2, RC4, DES, 3DES, Fortezza
    - Append SSL record header

The final step of SSL Record Protocol processing is to prepare a header consisting of the following fields:

- Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment
- Major Version (8 bits): Indicates major version of SSL in use
- Minor Version (8 bits): Indicates minor version in use
- Compressed Length (16 bits): The length in bytes of the plaintext

5. With reference to the following figure discuss data protection in the Cloud

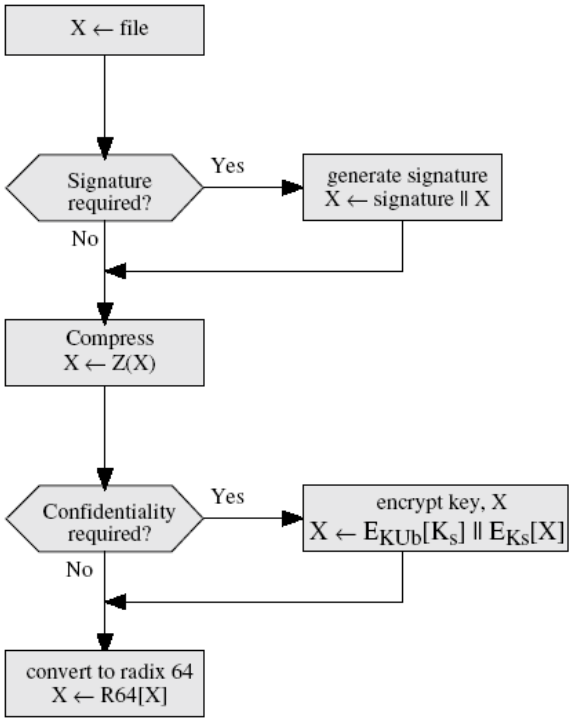


Data must be secured while at rest, in transit, and in use, and access to the data must be controlled
The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CP
For data at rest the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CP having no access to the encryption key
A straightforward solution to the security problem in this context is to encrypt the entire database and not provide the encryption/decryption keys to the service provider
The user has little ability to access individual data items based on searches or indexing on key parameters
The user would have to download entire tables from the database, decrypt the tables, and work with the results
To provide more flexibility it must be possible to work with the database in its encrypted form.

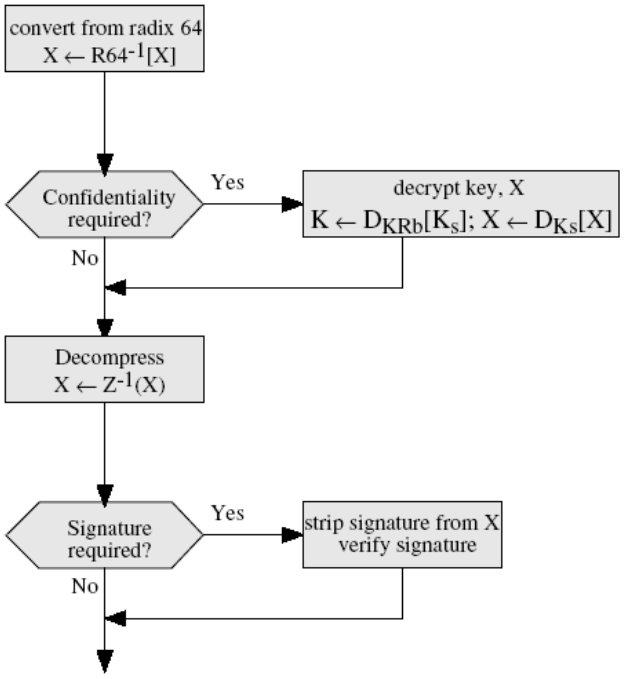
An example of such an approach, depicted in Figure 5.10, is reported in
[DAMI05] and [DAMI03]. A similar approach is described in [HACI02]. Four entities are involved:

- Data owner: An organization that produces data to be made available for controlled release, either within the organization or to external users.
- User: Human entity that presents requests (queries) to the system. The user could be an employee of the organization who is granted access to the database via the server, or a user external to the organization who, after authentication, is granted access.
- Client: Frontend that transforms user queries into queries on the encrypted data stored on the server.
- Server: An organization that receives the encrypted data from a data owner and makes them available for distribution to clients. The server could in fact be owned by the data owner but, more typically, is a facility owned and maintained by an external provider. For our discussion, the server is a cloud server.

6. What is PGP? Describe briefly PGP operations referring to the following flowchart.



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Pretty Good Privacy (PGP)

Provides a confidentiality and authentication service that can be used for electronic mail and file storage applications

Developed by Phil Zimmermann

- Selected the best available cryptographic algorithms as building blocks
- Integrated these algorithms into a general-purpose application that is independent of operating system and processor and that is based on a small set of easy-to-use commands
- Made the package and its documentation, including the source code, freely available via the Internet, bulletin boards, and commercial networks
- Entered into an agreement with a company to provide a fully compatible, low-cost commercial version of PGP

7. What is IPsec? With reference to the security association database and the security policy database explain how the inbound and the outbound IP packets are processed in the IPsec.

IPsec provides the capability to secure communications across a LAN, private/public WANs and Internet at the IP level.

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establish extranet and intranet connectivity with partners
- Enhance electronic commerce security
- Play a vital role in routing architecture
    - A router or neighbour advertisement from an authorized router.
    - A redirect message from router to which initial packet was sent.
    - A routing is not forged

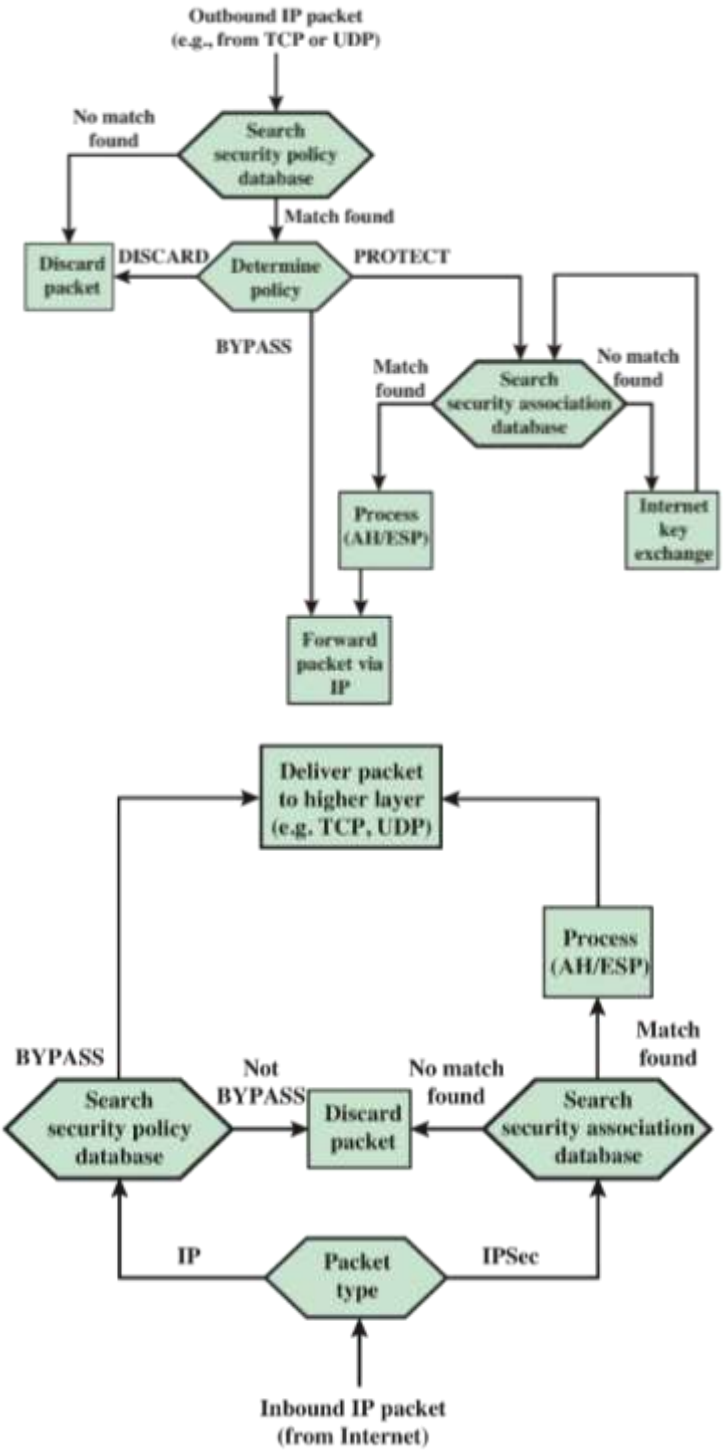
Security Association Database

- Defines the parameters associated with each SA
- Parameters in an SAD entry
    - Security Parameter Index
        - A 32-bit valued selected by the receiving end of an SA to identify the SA
    - Sequence Number Counter
        - A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
    - Anti-Replay Window
        - Used to determine whether an inbound AH or ESP packet is a replay
    - AH Information
        - Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.

Security Policy Database

Each SPD entry is defined by set of IP and upper-layer protocol field value, called selectors, defined by following parameters

- Remote IP Address :
  Latter two are required to support dest system sharing same SA
- Local IP Address :
  Latter two are required to support src system sharing same SA
- Next Layer Protocol:
  Includes a field designating the protocol operating over IP
- Name:
  User identifier from the operationg system
- Local and Remote Ports:
  These may be individual TCP or UDP port values


Outbound IP packet
(e.g., from TCP or UDP)
No match found
Search security policy database
Match found
Discard packet
DISCARD
Determine policy
PROTECT
BYPASS
Match found
Search security association database
No match found
Process (AH/ESP)
Internet key exchange
Forward packet via IP
Deliver packet to higher layer (e.g. TCP, UDP)
Process (AH/ESP)
Match found
BYPASS
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPSec
Inbound IP packet
(from Internet)

8. What are the differences between viruses, worms and Trojans?

A Trojan Horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.
Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses.

A Virus is a program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised as games or images with clever marketing titles such as "Me, nude".
A virus must meet two criteria:
It must execute itself. It will often place its own code in the path of execution of another program.
It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Computer Worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers, such as through email or Internet Relay Chat (IRC).

9. Sketch the structure and describe the key elements of the model for intrusion detection message exchange

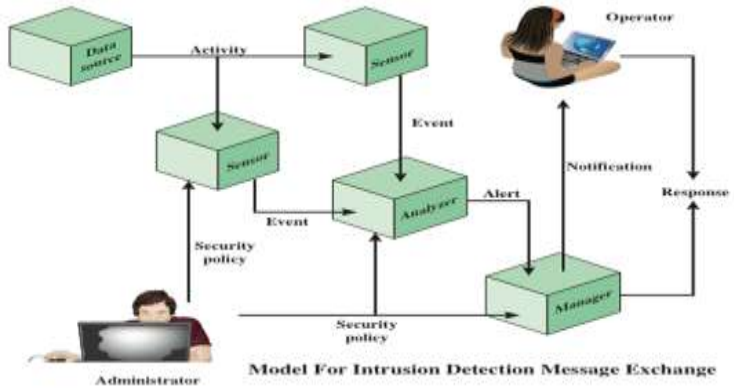


Figure 11.5 illustrates the key elements of the model on which the intrusion detection message exchange approach is based. This model does not correspond to any particular product or implementation, but its functional components are the key elements of any IDS. The functional components are as follows:

- Data source: The raw data that an IDS uses to detect unauthorized or undesired activity. Common data sources include network packets, operating system audit logs, application audit logs, and system-generated checksum data.
- Sensor: Collects data from the data source. The sensor forwards events to the analyzer.
- Analyzer: The ID component or process that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. In many existing IDSs, the sensor and the analyzer are part of the same component.
- Administrator: The human with overall responsibility for setting the security policy of the organization, and, thus, for decisions about deploying and configuring the IDS. This may or may not be the same person as the operator of the IDS. In some organizations, the administrator is associated with the network or systems administration groups. In other organizations, it's an independent position.
- Manager: The ID component or process from which the operator manages the various components of the ID system. Management functions typically include sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting.
- Operator: The human that is the primary user of the IDS manager. The operator often monitors the output of the IDS and initiates or recommends further action.

In this model, intrusion detection proceeds in the following manner. The sensor monitors data sources looking for suspicious activity , such as network sessions showing unexpected telnet activity, operating system log file entries showing a user attempting to access files to which he or she is not authorized to have access, and application log files showing persistent login failures. The sensor communicates suspicious activity to the analyzer as an event , which characterizes an activity within a given period of time. If the analyzer determines that the event is of interest, it sends an alert to the manager component that contains information about the unusual activity that was detected, as well

as the specifics of the occurrence. The manager component issues a notification to the human operator. A response can be initiated automatically by the manager component or by the human operator. Examples of responses include logging the activity; recording the raw data (from the data source) that characterized the event; terminating a network, user, or application session; or altering network or system access controls. The security policy is the predefined, formally documented statement that defines what activities are allowed to take place on an organization's network or on particular hosts to support the organization's requirements. This includes, but is not limited to, which hosts are to be denied external network access. The specification defines formats for event and alert messages, message types, and exchange protocols for communication of intrusion detection information.

10. Firewalls:

a. What is a firewall?

A firewall is a software program or a piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

b. List three design goals for a firewall.

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

c. List four techniques used by firewalls to control access and enforce a security policy.

- **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
- **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users.
- **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.