Block 1

1. Define Authentication

- ✓ Assurance of **valid users** and logical connections
- ✓ Ensure the sender is actually it **claims to be**

2. Define Access Control

- ✓ Prevention of **unauthorized used** of resources

3. Define Data Confidentiality

- ✓ Preserving authorized restrictions on **information access and disclosure**, including means for protecting **personal privacy and proprietary** information
- ✓ A loss of confidentiality is the **unauthorized disclosure** of information

4. Define Data Integrity

- ✓ Guarding against improper information **modification or destruction**
- ✓ A loss of integrity is the **unauthorized modification or destruction** of information

5. Define Non-repudiation

- ✓ Protection against **denial** from either party

6. Define Data Availability

- ✓ Ensuring **timely and reliable** access to and use of information
- ✓ A loss of availability is the **disruption of access** to or use of information or an information system

7. What is Substitution?

- ✓ Each element of the plaintext is **mapped into** another element
- ✓ **Replace** one letter for another

8. What is Transposition(Permutation)?

- ✓ Each element of plaintext is **rearranged**
- ✓ Change the **order** of the letters

9. What is Stream Cipher?

- ✓ Process **one input** element at a time

10. What is Block Cipher?

- ✓ Process **a block of elements** at a time

11. What’s the advantages and disadvantages of Stream Cipher?

- ✓ **Advantages**
  - ➢ Encryption can be very **fast**

  - ➢ **No** error propagation

- ✓ **Disadvantages**
  - ➢ **No** protection against **message manipulation**
  - ➢ It's **easy to know the key-stream** using the plaintext and ciphertext
    - ● message XOR ciphertext = key
  - ➢ Easy to get wrong

12. Why one-time pad is unbreakable?

- ✓ For each message, it uses a **new random key** that is **as long as the message**
- ✓ Encryption produces a random output that has **no statistical relationship** to the plaintext
- ✓ Given one ciphertext, the attacker can **try different random keys** and get **different intelligible plaintexts**
- ✓ There is **no way** the attacker will know **which one is the plaintext**

13. What are the weaknesses/practical problems of one-time pad?

- ✓ The practical difficulty is how to **transmit and protect** the random **key**
- ✓ Message manipulation
- ✓ The **key size** is as big as the message, so can have limitation
- ✓ Like other stream ciphers, **easy to get wrong**

14. What's Cryptanalysis Attacks?

- ✓ The attacker relies on the **nature of the algorithm** and perhaps some knowledge of the **general characteristics of the plaintext** or even some **sample plaintext-ciphertext pairs**
- ✓ The aim is to **deduce** a specific **plaintext** or the **key** being used
- ✓ The process of attempting to **discover the plaintext or key** from the ciphertext

15. When do we call an encryption algorithm is computationally safe?

- ✓ **Cost** of breaking the cipher is **much greater** than the **value** of the encrypted information
- ✓ **Time** to break the cipher is **much longer** than the **useful lifetime** of the encrypted information

16. What's Brute-force Attack?

- ✓ The attacker t**ries every possible key** on a piece of ciphertext until an **intelligible translation** into plaintext is obtained

17. What's the purpose of the S-Box in DES?

- ✓ The S-Box is used to **perform substitution** on the message contents
- ✓ The purpose is to **confuse** the information of the original message

18. How does S-Box work in DES?

- ✓ It consists of a **table (4*16)** where the entries of the table are the substitution values
- ✓ The **first and last** bits from a 6-bits block are used to represent a binary number refer to a **row** on the table
- ✓ The remaining **2 to 5 bits** form a binary number to refer to a **column** in the table
- ✓ The **overlap** between the selected row and column holds the new value which the S-Box is going to use in the substitution

19. What are the two main areas of concern related to the level of security provided by DES?

- ✓ Key **Size**
- ✓ The **nature** of the algorithm
  - ➢ The design of S-Boxes
  - ➢ The choice of specific permutations

20. What's Meet-in-the-middle Attack?

- ✓ Eve has intercepted the message m and $c = E_{K1}(E_{K2}(m))$
- ✓ She wants to find K1 and K2
- ✓ She computes $\boldsymbol{E_K(m)}$ for all **possible keys** and stores the result in al list

- ✓ She computes $D_K(c)$ for all **possible keys** and stores the result in al list
- ✓ She **compares** the two lists, and looks for a **match**
- ✓ If she found a match, then Eve knows K1 and K2

21. What's the purpose of the key expansion (key addition) algorithm used in AES?

- ✓ The AES key is 4 words (128 bits), which is used for round 0
- ✓ For round 1-10, the key expansion algorithm provides a new 4-word **round key** each of the 10 rounds

22. List the four stages of a typical round in AES and describe the functionality of each stage

- ✓ **Substitute Bytes**
  - ➢ Uses an **S-Box** to perform block substitution
  - ➢ Each of the state bytes is split into **two 4-bit** values, which represents the **column and row values** of the S-Box containing the new substitution value
- ✓ **Shift Rows**
  - ➢ A simple **permutation** where the state block is altered by rearranging the bytes located on **each of the four rows**
- ✓ **Mix Columns**

- A **substitution** that makes used of arithmetic over **GF(2^8)**
- Hence, each of the state elements is updated using the product of elements of one row and one column

✓ **Add Round Key**

- A simple **bitwise XOR** of the **current block** with a portion of the **expanded key**
- The expanded key is obtained through the expansion algorithm

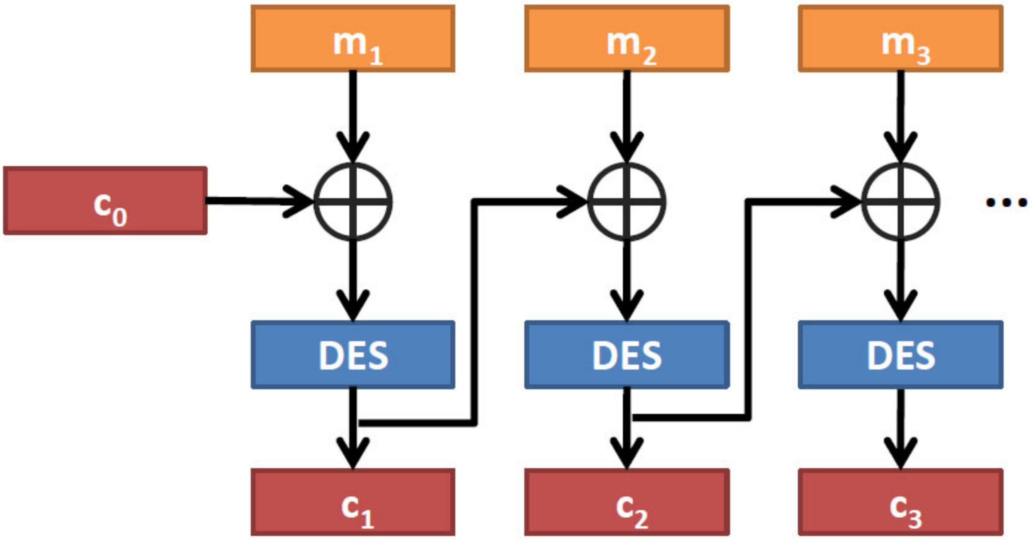
23. What's the problem of ECB mode?

✓ A block cipher process one block of data at a time, using the **same key**

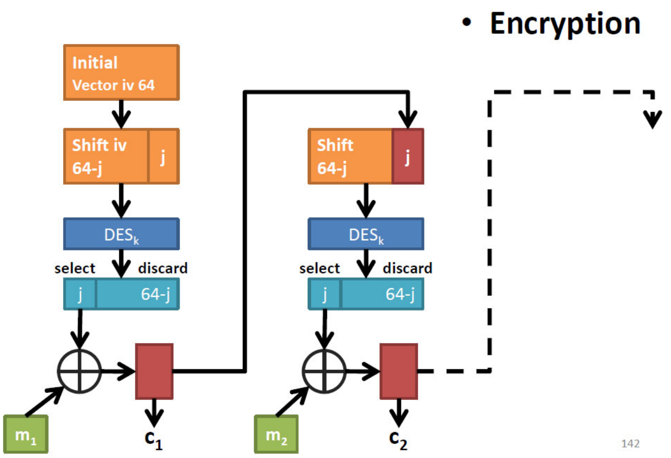
✓ Same plaintext will result in **same** ciphertext

✓ Problem: Easy to compromise

24. Explain how does CBC mode work



25. Explain how does **CFB** mode work



✓ Start with an **initial vector** (iv)

✓ **Shift j** bits

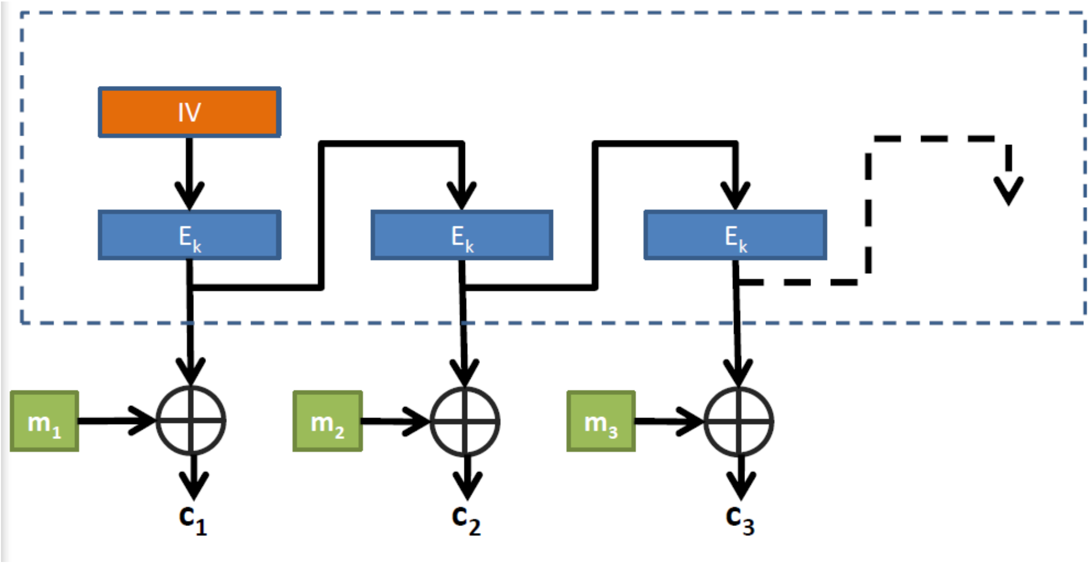
✓ **Encrypt** using DES

✓ **Select first j** bits

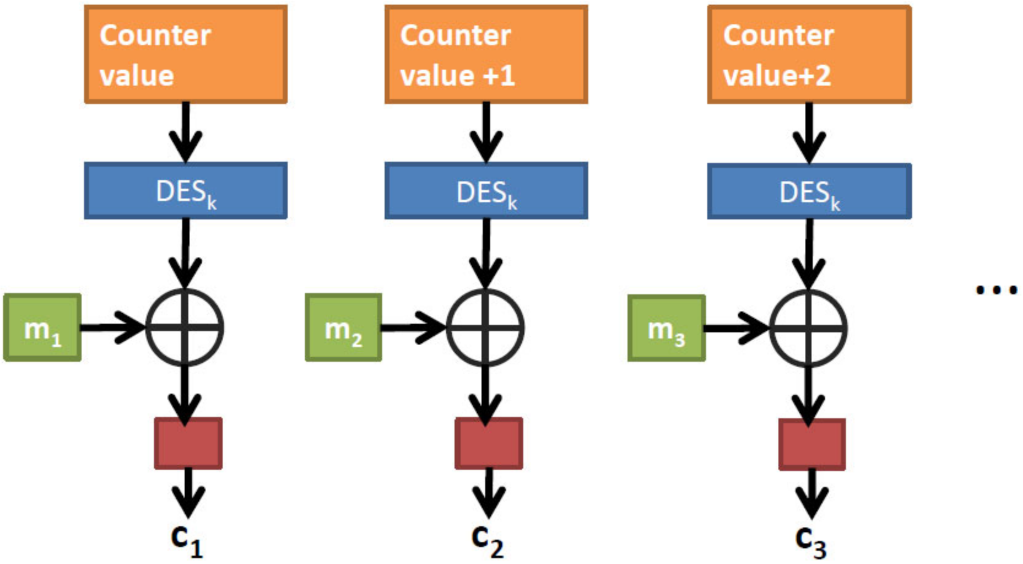
✓ **XOR** with the j bits of the **message**

✓ Use the encrypted message **as new iv**

26. Explain how does **OFB** mode work



27. Explain how does CTR mode work



Block 2

1. What's the difference between symmetric encryption and asymmetric encryption?

- ✓ Symmetric encryption: Sender and receiver use the **same** key
- ✓ Asymmetric encryption: Sender and receiver each use a **different** key

2. What's the difference between the public key and private key?

- ✓ **Private Key**
  - ➢ A user's private key is **kept private** and **known only to the user**
  - ➢ The private key can be used to **decrypt** ciphertext messages encrypted by public key
  - ➢ The private key can also be used to **create a signature** that can be verified by anyone with the public key
- ✓ **Public Key**
  - ➢ The user's public key is made **available to others** to use
  - ➢ The public key can be used to **encrypt information** that can only be decrypted by the possessor of the private key

3. List the principle(basic) elements of a public-key encryption and briefly explain each of them

- ✓ **Plaintext**
  - ➢ Un-encrypted text/data that is fed into the algorithm as **input**

- ✓ **Encryption algorithm**
  - ➢ Performs various transformations on the plaintext
- ✓ **Public and private keys**
  - ➢ A pair of keys on the client and the server sides
  - ➢ If one is used for encryption, the other is used for decryption
- ✓ **Ciphertext**
  - ➢ Encrypted version of the plaintext and the key
- ✓ **Decryption algorithm**
  - ➢ Accepts the ciphertext and the matching key and produces the original plaintext

4. What are three broad categories of applications of public-key cryptosystems?

- ✓ **Encryption / Decryption**
  - ➢ The sender encrypts a message with the recipient's public key
- ✓ **Digital Signature**
  - ➢ The sender "signs" a message with its private key
  - ➢ Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message
- ✓ **Key Exchange**
  - ➢ Two sides cooperate to exchange a session key

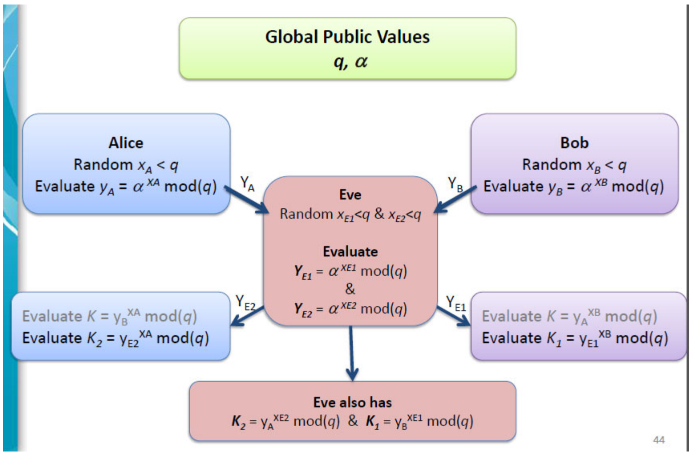
5. What is one-way function?

- ✓ A one-way mathematical function is very **easy to do**, but very **difficult to reverse**

6. Explain how does Diffie-Hellman algorithm exchange keys?

- ✓ Diffie-Hellman is based on **Discrete Algorithms**
- ✓ Both users know common values (**prime number and its primitive root**)
- ✓ Each user generates a **random secret value** (<p)
- ✓ Users then raise the **primitive root** to the **random value** to compute a public-value
- ✓ They **exchange** the public values and raise them to the **secret value** to achieve **identical key** value at both ends

7. Explain Man-in-the-middle Attack



Global Public Values
q, α

Alice
Random $x_A < q$
Evaluate $y_A = \alpha^{XA} \bmod(q)$

Bob
Random $x_B < q$
Evaluate $y_B = \alpha^{XB} \bmod(q)$

Eve
Random $x_{E1}<q$ & $x_{E2}<q$

Evaluate
$Y_{E1} = \alpha^{XE1} \bmod(q)$
&
$Y_{E2} = \alpha^{XE2} \bmod(q)$

Evaluate $K = y_B^{XA} \bmod(q)$
Evaluate $K_2 = y_{E2}^{XA} \bmod(q)$

Evaluate $K = y_A^{XB} \bmod(q)$
Evaluate $K_1 = y_{E1}^{XB} \bmod(q)$

Eve also has
$K_2 = y_A^{XE2} \bmod(q)$ & $K_1 = y_B^{XE1} \bmod(q)$

- ✓ Eve prepares for the attack by generating two random private keys X_{E1} and X_{E2}, and then computing the corresponding public keys Y_{E1} and

Y_{E2}

- ✓ Alice transmits Y_A to Bob
- ✓ Eve intercepts Y_A and transmits Y_{E1} to Bob
- ✓ Eve also calculates $K_2 = {Y_A}^{X_{E2}} \, mod \, q$
- ✓ Bob receives Y_{E1} and calculates $K_1 = {Y_{E1}}^{X_B} \, mod \, q$
- ✓ Bob transmits Y_B to Alice
- ✓ Eve intercepts Y_B and transmits Y_{E2} to Alice
- ✓ Eve also calculates $K_1 = {Y_B}^{X_{E1}} \, mod \, q$
- ✓ Alice receives Y_{E2} and calculates $K_2 = {Y_{E2}}^{X_A} \, mod \, q$

8. What is Trapdoor One-Way Function?

- ✓ Trapdoor one-way function is a **one-way** function, together with a **secret y**, such that, given f(x) and y, it’s **easy to compute x**

9. What is the RSA?

- ✓ RSA is a public-key encryption algorithm
- ✓ Block cipher in which the plaintext and ciphertext are integers between 0 and n-1
- ✓ n=p*q, where p and q are prime numbers
- ✓ Encryption: $\boldsymbol{c = m^e \, mod \, n}$
- ✓ Decryption: $\boldsymbol{m = c^d \, mod \, n}$
- ✓ Public key (e,n)

- ✓ Private key (d,n)

10. Explain how does RSA algorithm exchange keys?

- ✓ Each user holds a **Public-Private key** pair
- ✓ One user could generate a random **session key**
- ✓ The user uses the receiver’s public key to **encrypt** the session key
- ✓ The receiver uses his/her own private key **decrypt** the session key

11. How to combine two encryption methods to encrypt a large volume of data and why is it more effective?

- ✓ **Method**
  - ➢ Alice creates a fresh **session key**
  - ➢ Alice **encrypts** the session key by using Bob’s public key
  - ➢ Bob **decrypts** the message by using his private key and get the session key
  - ➢ Then they start to **use session key** to communicate
- ✓ **Reason**
  - ➢ Conventional encryption is **much faster** than Public-key encryption
  - ➢ Conventional encryption has the issue of the **key distribution**

12. What is a one-way hash function?

- ✓ A hash is a **one way** cryptographic function and the sender and receiver

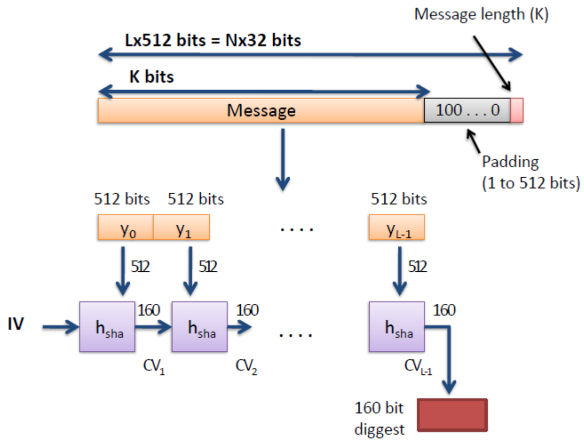
don't need to share a **secret** key

- ✓ A hash function takes a message of a variable length and produces a fixed length output as **message digest**

13. What is the security property of hash function?

- ✓ **Preimage Resistance**
  - ➢ **Given** an output value **c**, it should be a difficult operation to **find** any **input** value m such that **h(m)=c**
- ✓ **Second Preimage Resistance**
  - ➢ **Given** an **input m** and its **output value h(m)**, it should be a difficult operation to **find any other input** value n such that **h(m)=h(n)**
- ✓ Collision Resistance
  - ➢ For a hash function h, it's hard to **find two different inputs** m and n such that **h(m)=h(n)**

14. Explain how does SHA1 works



CV: Compression Value.

- ✓ Messages are appended with padding bits to reach a length dividable by 512 bits
- ✓ Then, each 512 bits block is processed using h_{sha} process
  - ➢ Each block is processed with the previous stage
  - ➢ Each block outputs 160 bits, same length as the initial stage takes a pre-defined IV

15. Explain what is the birthday attack (hash attack)

- ✓ Alice is ready to sign a message by encrypting, using her **private-key**, the m-bit **hash code** of the message
- ✓ Eve generates $2^{m/2}$ **variations of the message**, all of each convey the **same meaning**
- ✓ Eve also generates an **equal number of messages** all of which are **variations of the fraudulent message** that Eve **wants to substitute** for the original one
- ✓ Eve **searches in the two sets** of messages a pair that produce the **same hash code**, whose successful probability is greater than 0.5
- ✓ Eve **presents the valid variation** of the original message to Alice for **signature**
- ✓ After Alice **signs the hash**, the hash is **attached to the fraudulent version** of the message

16. What is MAC?

- ✓ Message Authentication Code is a method used to **check the integrity** of a message
- ✓ It requires a key or **secret value**
- ✓ A MAC takes a **variable-length message** and a **secret key** as input and produces a **fixed length authentication code**

17. What's the difference between MAC and one-way function?

- ✓ MAC needs sender and receiver to share a secret key, but no key is required for hash functions
- ✓ One-way hash function only provides integrity, but MAC provides integrity and authentication

18. What changes are required to replace a HMAC with an underlying hash function?

- ✓ To replace a given hash function in an HMAC implementation, all that is required is to **remove** the existing hash function module and **drop in** the new module

Block 3

1. What is a public-key certificate?

- ✓ It's used to **authenticate public-keys** of users
- ✓ A public-key certificate contains a **public key**, an **identifier of the key owner** and other information, is **signed and create**d by a **certificate authority**, and is given to the participant
- ✓ A participant **conveys its key** information to another by **transmitting its certificate**
- ✓ Other participants can **verify** that the certificate was created by the **authority**

2. Define the X.509 standard

- ✓ X.509 defines a **framework** for the **provision** of authentication services by the X.500 directory to its users
- ✓ The directory may serve as a **repository** of public-key certificates
- ✓ The public key of a user and is **signed** with the **private key** of a trusted **certification authority**
- ✓ In addition, X.509 defines **alternative authentication protocols** based on the use of public-key certificates

3. Why a certificate should be revoked by before its expiry data?

- ✓ **User's Private-key** has been compromised

✓ **Certification Authority** has been compromised

✓ User is **no longer certificated** by this Authority

4. How is an X.509 certificate revoked?

✓ **Each CA** must **maintain a certificate revocation list (CRL)** consisting of **all revoked certificates** issued by that CA

✓ The list is **signed by the issuer** and includes the **issuer’s name**, the **date** the list was created, the date the **next CRL is scheduled** to be issued, and an **entry** for each **revoked certificate**

✓ Each entry consists of the **serial number** of a certificate and **revocation date** for that certificate

✓ The **user** could **check the CRL list** each time a certificate is received to determine the certificate is not revoked

5. What is Kerberos?

✓ Kerberos is a **centralized authentication** and **access control** service designed for use in a **distributed environment**

✓ It makes use of a **trusted third-party** authentication service that enables clients and servers to establish **authenticated communication**

✓ Also, it provides **access control**

6. Why Kerberos doesn’t ask client for a password to authenticate?

- ✓ The main security weakness is that the **password is transmitted**
- ✓ So anybody **eavesdrop**ping can get hold of it

7. How does Kerberos authenticate the server and the clients?

- ✓ The client **requests** from the server a “**service granting ticket**”
- ✓ The client sends the request for using the **server**, and the **user’s ID**
- ✓ The server, which knows the user’s password, creates a **session key** using the **user’s password**
- ✓ Using this session key, the server **sends the ticket** granting a service
- ✓ The client **asks the user for** his/her **password**, **generates the session key** and recovers the ticket
- ✓ The **password is never transmitted** between server-client

8. What are the requirements for Kerberos and what mechanisms are used within Kerberos systems to achieve these requirements?

- ✓ **Secure**
  - ➢ Provided by the secure steps, mostly achieved by using **conventional encryption**
- ✓ **Reliable**
  - ➢ **Distributed** architecture
  - ➢ Use **mirrored system backups**

- ✓ **Transparent**
  - ➢ **Limitation** of user **interaction** to the authentication with the client (password, or other methods)
- ✓ **Scalable**
  - ➢ Principle of **Kerberos realms**

9. How does inter-realm in Kerberos use?

- ✓ For inter-realm authentication, the Kerberos server in each realm shares **a secret key** with the server in the other realm
- ✓ The two Kerberos server are **registered with each other**
- ✓ Client requests **Ticket of Local TGS** from Kerberos Server A
- ✓ Kerberos Server A sends **Ticket of Local TGS** to Client
- ✓ Client requests T**icket of Remote TGS** from Kerberos Server A
- ✓ Kerberos Server A sends **Ticket of Remote TGS** to Client
- ✓ Client requests **Ticket of Remote Server** from Kerberos Server B
- ✓ Client requests **Remote Server**

10. What is IPSec? And why it is important?

- ✓ IPSec stands for **IP Security** as it **protects IP packets**
- ✓ It's vital for providing **additional security** at the **IP layer**, and protect **security-ignorant** applications
- ✓ It provides **confidentiality, authentication,** or both for IP packets

11. What is the components of IPSec?

- ✓ IPSec Proper
  - ➢ Authentication
  - ➢ Encryption
- ✓ IPSec Key Management

12. What are the two modes of operations in IPSec? How can they achieve protection against traffic analysis?

- ✓ **Tunnel Mode:** Protects **entire** packet
- ✓ **Transport Mode:** Protects **payload**
- ✓ EPS **provides protection** against traffic analysis
  - ➢ In tunnel mode, ESP provides protection against traffic analysis where the host on the internet networks use the Internet transport of data but **do not interact with other Internet-based hosts**
  - ➢ In transport mode, ESP **only protects the payload**, hence the **IP header will not be hidden**, which provides **limited** protection against traffic analysis

13. What's the difference between transport mode and tunnel mode?

- ✓ **Transport mode**
  - ➢ Provides protection primarily for **upper-layer** protocols
  - ➢ Transport mode protection extends to the **payload** of an IP packet

- ✓ **Tunnel mode**
    - ➢ Provides protection to the **entire** IP packet

14. List the services provided by IPSec

- ✓ **Access** control
- ✓ Connectionless **integrity**
- ✓ Data origin **authentication**
- ✓ **Rejection** of **replayed** packets
- ✓ **Confidentiality**
- ✓ **Limited traffic flow** confidentiality

15. In IPSec, what is the Domain of Interpretation?

- ✓ Contains values to relate the different specifications of the protocol
- ✓ Identifiers for encryption and authentication algorithms
- ✓ And operational parameters, key lifetimes, key exchange etc.

16. What is a SA?

- ✓ SA is a **one-way relationship** between sender and receiver that describes a security service
- ✓ For two-way exchange of data, **two SAs** are needed, from sender-to-receiver and receiver-to-sender

17. What are the parameters used to define a SA?

- ✓ Security Parameter Index (SPI)
- ✓ IP Destination Address
- ✓ Security Protocol Identifier

18. What are the parameters used to characterize the nature of a particular SA?

- ✓ Sequence Number Counter
- ✓ Sequence Counter Overflow
- ✓ Anti-Replay Window
- ✓ AH Information
- ✓ ESP Information
- ✓ Lifetime of this Security Assocation
- ✓ IPSec Protocol Mode
- ✓ Path MTU

19. What is a replay attack?

- ✓ It's when an attacker **re-uses** a **valid sequence** of data in order to access a particular service

20. What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

- ✓ ISAKMP by itself **doesn't dictate** key exchange algorithm
- ✓ ISAKMP consists of **a set of message types** that enable the use of a **variety of key exchange algorithms**
- ✓ Oakley is the **specific key exchange algorithm** mandated for use with the initial version of ISAKMP

21. What is a firewall?

- ✓ A firewall protects a **local** system/network from **network-based** security threats, at the same time **allows access** to the outside world

22. List 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** and **TCP port number**
  - ➢ May provide **proxy software** that receives and interprets each service request before passing it on
  - ➢ 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
  - ➢ It may also be applied to incoming traffic from **external users**
    - ● Requires some form of secure authentication technology
- ✓ **Behavior Control**
  - ➢ Controls how **particular services** are used
  - ➢ For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local Web server

23. What is a Packet Filtering Router?

- ✓ Filters the **IP packets**, forwarding or discarding them depending on a **list of rules**

24. What are the disadvantages of Packet Filtering Router?

- ✓ **Difficulty setting up rules** and **no authentication**
- ✓ **IP address** of hosts on the protected side of the filter can be **readily determined by observing the packet traffic** on the unprotected side

of the filter

- ✓ Filters **cannot check all of the fragments** of higher level protocols as the TCP header information is only available in the first fragment
- ✓ Filters are not sophisticated enough to check the validity of the application-level protocols **imbedded** in the TCP packets

25. What is a Circuit-level Gateway?

- ✓ **Translates the address** of internal hosts in order to **hide** them from outside world
- ✓ It **doesn't permit an end-to-end TCP** connection, but rather **relays** them

26. What is a Bastion Host?

- ✓ Bastion Host is a **critical strong point** in the network's security
- ✓ It serves as a platform for **application-level or circuit-level gateway**
- ✓ Its hardware executes a **secure version** of its **operating system**
- ✓ Before the user is allowed to access the bastion host can require **authentication** of the user
- ✓ **Only essential** services are installed to **minimize vulnerability**

27. What is the difference between De-Militarized Zone and Screened Subnets?

- ✓ A **DMZ** is **in front of** a firewall
- ✓ A **screen subnet** is **behind** a firewall

28. What’s the rule of Trusted System?

- ✓ **No Read Up**
  - ➢ A subject can only **read** an object of **less or equal** security level
- ✓ **No Write Down**
  - ➢ A subject can only **write** into an object of **greater or equal** security

29. Which components are used in Trusted System to ensure the rule?

- ✓ Reference Monitor

Block 4

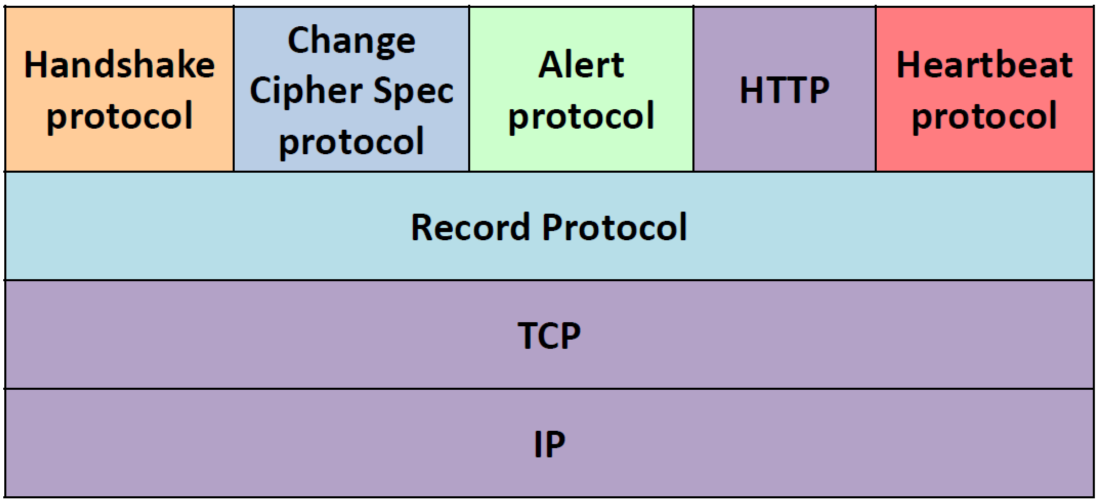
1. What is **SSL connection**?

- ✓ A connection in SSL is a **transport** that provides a suitable type of service
- ✓ The connections are **peer-to-peer relationships** and are **transient**
- ✓ Every connection is associated with **one session**

2. What is **SSL session**?

- ✓ A session in SSL is an **association** between a client and a server
- ✓ They define the security which can be **shared** between **multiple connections** to **avoid expansive renegotiation** of security parameters

3. What **protocols** are included in SSL architecture?



4. What is the **purpose** of **Handshake** protocol in SSL?

- ✓ Agree on the **cipher suite** to be used to establish the secure channel

- ✓ Allows the server and client to **authenticate** each other
- ✓ Establish the **keys** needed to secure the channel

5. How does Ephemeral Diffie-Hellman algorithm generates a session key?

- ✓ The server generates a **fresh** set of parameters, and sends the public value alongside a **digital signature** on the chosen parameter
- ✓ Client needs to **check** the server's public-key **certificate** is valid, then should **verify the digital signature** on the Diffie-Hellman parameters
- ✓ The client generates a **fresh temporary Diffie-Hellman key pair** and sends the **public value** to the server, after which both client and server **compute the shared secret** K_P

6. How does Handshake protocol in SSL works?

- ✓ **Step 1: Client Request**
  - ➢ A **session ID**: a unique identifier for the session
  - ➢ A **pseudorandom number (nonce)** r_c: For the provision of freshness (Replay Attack)
  - ➢ A list of **cipher suites** the client **supports** (including key exchange method)
- ✓ **Step 2: Server Response**
  - ➢ The **session ID**

  - ➢ Server's nonce r_s
  - ➢ The **particular cipher suite** the server has **decided to use**
  - ➢ A copy of the **server's public-key certificate**
  - ➢ If the **Ephemeral Diffie-Hellman** is chosen, then the server also generates a **fresh** set of parameters, and sends the public value alongside a **digital signature** on the chosen parameter

- ✓ **After receiving server response message, client need to**
  - ➢ **Check** the server's public-key **certificate** is valid
  - ➢ If the **Ephemeral Diffie-Hellman** is being used, then the client should **verify the digital signature** on the Diffie-Hellman parameters

- ✓ **Step 3: Pre-master Secret Transfer**
  - ➢ The client and server now need to **agree** on a shared secret K_P (the pre-master secret)
  - ➢ **RSA:** The client generates K_P, **encrypted** using the **server's public key** and sends to the server
  - ➢ **Ephemeral Diffie-Hellman:** The client generates a **fresh temporary Diffie-Hellman key pair** and sends the **public value** to the server, after which both client and server **compute the shared secret** K_P

- ✓ **The client and server can now derive the keys required to secure the TLS session**

- ➢ Compute the master secret $\boldsymbol{K_M}$, using a key derivation function, taking K_P, r_C, r_S as part of inputs
- ➢ Derive **MAC and encryption keys** from K_M. From this point on, all exchanged messages are **cryptographically protected**

✓ **Step 4: Client Finished**

- ➢ The client computes a **MAC** on the hash of all the message **sent thus far**
- ➢ This MAC is then **encrypted** and sent to the server

✓ **Step 5: Server Finished**

- ➢ The server **checks the MAC** received from the client
- ➢ The server computes a **MAC** on the hash of all the message **sent thus far**
- ➢ This MAC is then **encrypted** and sent to the server

7. What security services does TLS Record protocol provide, and how?

✓ **Security Services**

- ➢ Confidentiality
- ➢ Message Integrity

✓ **Process**

- ➢ Fragmentation
- ➢ Compress
- ➢ Add MAC

  - ➢ Encrypt
  - ➢ Append TLS Record Header

8. What's the basic requirements of email security?

- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity

9. What security services can PGP provides?

- ✓ Authentication
- ✓ Confidentiality
- ✓ Compression
- ✓ E-mail Compatibility
- ✓ Segmentation

10. Why do we need to compress the message after signing digital signature?

- ✓ If the message was first compressed and then signed, then for future **verification**
  - ➢ A **compressed version** of the document has to be stored or
  - ➢ **Re-compress** the message when verification is required
- ✓ A compression algorithm is **not deterministic**

- The **same message** when compressed can produce **different compressed forms**
  - ● Depend on **running speed** and **compression ratio**
- If sender and receiver **use different settings** for the compression algorithm, they obtain different forms, which makes authentication difficult

11. How many encryption keys are used/generated in PGP?

✓ Pass-phrase Key

✓ Session Key

✓ Public Key

✓ Private Key

12. How PGP manages the encryption keys?

✓ **Private-Key Ring**

- Stores the **private/public** key pairs owned at the node for **this user**

✓ **Public-Key Ring**

- Stores the **public key** of **other users** known at this node

13. Explain how PGP identifies the public key

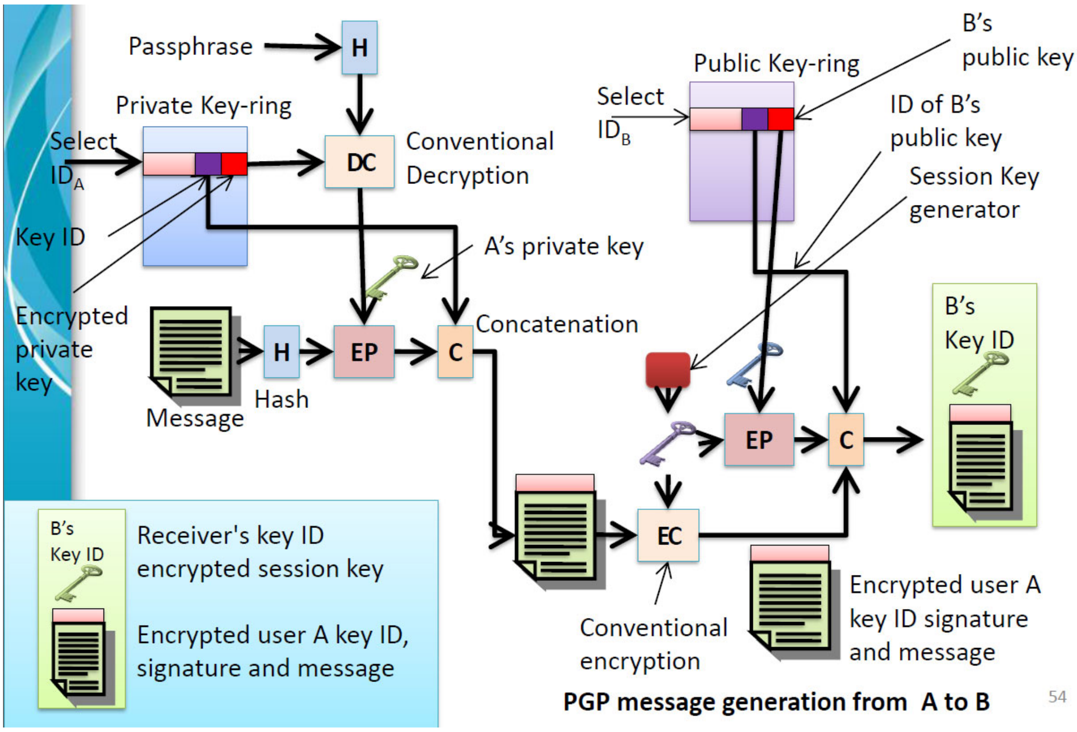
✓ PGP assigns an **ID** to each public key by using the **last 64 significant bits** of the key

- ✓ The ID can be used to identify which public key was used

14. What’s the purpose of pass-phrase key in PGP?

- ✓ Encrypt or Decrypt the private key of users stored in private-key ring

15. Describe how does authentication and confidentiality achieve in PGP



PGP message generation from A to B

16. What is the Trust in PGP?

- ✓ PGP doesn’t include any specification for establishing CAs and adopts a different trust model —— The Web of Trust
- ✓ **Key Legitimacy**
  - ➢ Indicates the extent to which PGP will trust that this is a valid

public key for this user

- ➢ The **higher** the level of trust, the **stronger** is the binding of this user ID to this key
- ➢ This field is computed by PGP

✓ **Owner Trust**

- ➢ Indicates the degree to which this public key is trusted to **sign other** public-key certificates
- ➢ This level of trust is assigned by the user

✓ **Signature Trust**

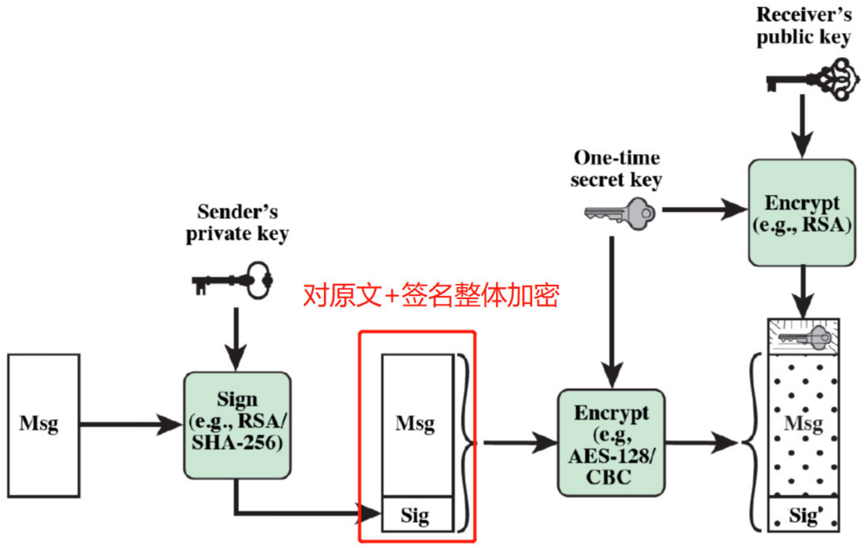
- ➢ Indicates the degree to which this PGP user trusts the **signer** to certify public keys
- ➢ The legitimacy field is derived from the collection of signature trust fields in the entry

17. What's difference between MIME and S/MIME?

✓ MIME is an **extended framework** that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) and RFC5322 or some other mail transfer protocol and emails

✓ S/MIME is a **security enhancement** to the MIME Internet e-mail format standard, based on technology from **RSA Data Security**

18. How does S/MIME achieve confidentiality and authentication?



19. Explain the certificate processing of S/MIME

- ✓ Uses **public-key certificates** that confirm to **X.509 v3**
- ✓ Key management is **hybrid** between **X.509** and **PGP's web of trust**
- ✓ Each client has a **list of trusted CA's certificates** and own **public/private key pairs** and **certificates**
- ✓ Certificates must be **signed by trusted CA's**

20. How to detect intrusion?

- ✓ **Audit Records**
  - ➢ **Native Audit Records**
    - ● Almost all multiuser **operating systems** including **accounting software** that collect information on user activity
    - ● **Advantages: No additional** collection software is needed
    - ● **Disadvantages:** Records **may not contain** the **needed info**

- **Detection-Specific Records**
    - **A collection facility** that generates **audit records** containing **only** the information **required** by the intrusion detection system
    - **Advantages: Vendor independent**, reported to **variety** of systems
    - **Disadvantages: Extra overhead** in having two accounting packages

✓ **Statistical Anomaly Detection**

- Uses **statistical tests** to **observe** and determine high level of confidence
    - Tests are applied on the collected data relating to the **behavior of legitimate user** over a period of time
- **Threshold Detection**
    - Defines the **thresholds** for the **frequency of events** occurrences, **independent** of the **user**
- **Profile Based Detection**
    - A **profile** of the behavior of **user**s is built and then used to **detect changes** in the behavior of the account activity

✓ **Rule-Based Detection**

- Defines **a set of rules** that can be used to decide that a given behavior is that of an intruder
- **Anomaly Detection**

        - Detection of deviation from **previous** usage patterns is **derived** from certain developed rules
    - **Penetration Identification**
        - An **expert system** approach that searches for suspicious behavior

- ✓ **Distribution Intrusion Detection**
    - To deal with **different** audit record **formats**
    - On the network, **one or more nodes** in the network will serve as collection and analysis points for the data and the system
    - Either centralized or decentralized architecture can be used
- ✓ **Honeypots (Decoy systems to lure attackers)**
    - Divert an attacker from accessing critical systems
    - **Collect** information about the **attacker's activity**
    - **Encourage the attacker** to **stay on** the system long enough for administrator to respond

21. List different types of malicious software and briefly explain each one

- ✓ **Virus**
    - Malware that, when executed, tries to **replicate itself into** other executable code; when it succeeds the code is said to be **infected**
    - When the infected code is executed, the **virus also executes**

- ✓ **Worm**
  - ➢ A computer program that can **run independently** and can **propagate** a complete working version of itself onto other hosts on a network
- ✓ **Trojan Horse**
  - ➢ A computer program that **appears to have a useful function**, but also has **a hidden and potentially malicious function** that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program
- ✓ **Backdoor (Trapdoor)**
  - ➢ Any mechanism that **bypasse**s a normal security check
  - ➢ It may allow **unauthorized access** to functionality
- ✓ **Downloaders**
  - ➢ Program that **installs other items** on a machine that is under attack
  - ➢ Usually, a downloader is sent in an e-mail
- ✓ **Auto-rooter**
  - ➢ Malicious tools used to r**emotely break** into new computers
- ✓ **Spammer Programs**
  - ➢ Used to **send large volumes** of unwanted e-mail
- ✓ **Flooders**
  - ➢ Used to attack **networked** computer systems with a **large volume**

of traffic to carry out a **DoS** attack

- ✓ **Zombie (Bot)**
  - ➢ Program activated on an **infected machine** that is activated to **launch attacks on other machines**
- ✓ **Spyware**
  - ➢ Software that **collects information** from a computer and **transmits** it to another system
- ✓ **Adware**
  - ➢ **Advertising** that is **integrated** into software
  - ➢ It can result in **pop-up ads** and **redirection** of a browser to a commercial site

22. What is Denial of Service attack?

- ✓ DoS is an attempt to prevent legitimate users of a service from using that service
- ✓ When this attack comes from a single host or network node, then it's simply referred to as a DoS attack

23. What is Distributed Denial of Service attack?

- ✓ DDoS attack attempts to **consume** the target's resources so that it **cannot provide services**
- ✓ In a DDoS attack, an attacker is able to **recruit a number of hosts**

throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the targe