CMR ENGINEERING COLLEGE

KANDLAKOYA (V), MEDCHAL (M), R.R.DIST.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

SUBJECT - INFORMATION SECURITY III C.S.E 2015-16

STEP MATERIAL

PART-A SHORT ANSWER QUESTIONS & ANSWERS

Q) Define Information Security?

It can be defined as "measures adopted to prevent the unauthorized use, misuse, modification or denial of use of knowledge, facts, data or capabilities". Three aspects of IS are:

 Security Attack: Any action that comprises the security of information

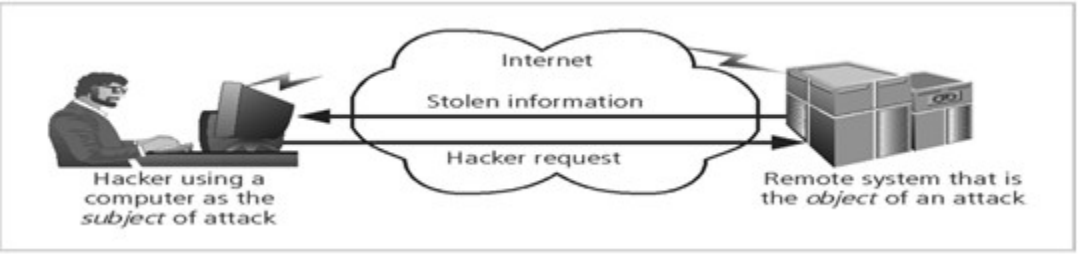
 Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security.

 Security Service: It is a processing or communication service that enhances the security of the data processing systems and information transfer.

Q) How components are secured in an information system?

Securing the Components

- The computer can be either or both the subject of an attack and/or the object of an attack
- When a computer is
  - the subject of an attack, it is used as an active tool to conduct the attack
  - the object of an attack, it is the entity being attacked.



Q) What is the difference between a threat agent and a threat?

A threat is a category of objects,persons,or other entities that pose a potential danger to an asset. Threats are always present.

A threat agent is a specific instance or component of a threat.

Example: All hackers in the world are a collective threat

Kevin Mitnick,who was convicted for hacking into phone systems was a threat agent.

Q)What is information security?

Information security in today's enterprise is a "well-informed sense of assurance that the **information risks and controls are in balance**." –Jim Anderson, Inovant (2002)

- The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information
- Tools, such as policy, awareness, training, education, and technology are necessary
- The C.I.A. triangle was the standard based on **confidentiality, integrity, and availability**
- The C.I.A. triangle has expanded into a list of critical characteristics of information

Q) What is the difference between vulnerability and exposure?

The exposure of an information system is a single instance when the system is open to damage.Weakness or faults in a system expose information or protection mechanism that expose information to attack or damage or known as vulnerabilities.

Q) What is attack?

An attack is an intentional or unintentional attempt to cause damage or otherwise compromise the information.If some one casually reads sensitive information not intended for his or her use ,this considered as a **passive attack.**If a hacker attempts to break into an information system,the attack is considered **active.**

Q) What is hacking?

Hacking can be defined positively and negatively.

(1) to write computer programs for enjoyment
(2) to gain access to a computer illegally

In early days the computer enthusiasts are called hacks or hackers because they could tear apart the computer instruction code or even a computer itself.

In recent years ,the term hacker is used in a negative sense, that is, the persons gaining illegal access to others' computer systems and programs and manipulating and damaging.

Q)What is security blue print?

The security blue print is the plan for the implementation of new security measures in the organization. Some times called a framework, the blue print presents an organized approach to the security planning process.

Q)What's the difference between encoding, encryption, and hashing?

Encoding is designed to protect the integrity of data as it crosses networks and systems, i.e. to keep its original message upon arriving, and it isn't primarily a security function. It is easily reversible because the system for encoding is almost necessarily and by definition in wide use. Encryption is designed purely for confidentiality and is reversible only if you have the appropriate key/keys. With hashing the operation is one-way (non-reversible), and the output is of a fixed length that is usually much smaller than the input.

Q)What's the difference between Diffie-Hellman and RSA?

Diffie-Hellman is a key-exchange protocol, and RSA is an encryption/signing protocol. If they get that far, make sure they can elaborate on the actual difference, which is that one requires you to have key material beforehand (RSA), while the other does not (DH).

Q)What is Sniffer?

- A **sniffer** is a program or device that can monitor data traveling over a network.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

Q)Write a short note on Man in the Middle Attacks ?

In cryptography, the **man-in-the-middle attack** (often abbreviated **MITM**), is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (ex: unencrypted Wi-Fi access point).

This is not easy in the Internet because of hop-by-hop routing, unless you control one of the backbone hosts or source routing is used. This can also be done combined with IP source routing option. IP source routing is used to specify the route in the delivery of a packet, which is independent of the normal delivery mechanisms.

Q)Define Elliptic Curve Cryptography(ECC)?

Elliptic curve cryptography (ECC) is an approach to public-key **cryptography** based on the algebraic structure of **elliptic curves** over finite fields. ECC requires smaller keys compared to non-ECC **cryptography** (based on plain Galois fields) to provide equivalent security.

Q) Write a short notes on Cryptography

A cipher is a secret method of writing, as by code. **Cryptography**, in a very broad sense, is the study of techniques related to aspects of information security. Hence cryptography is concerned with the writing (ciphering or encoding) and deciphering (decoding) of messages in secret code. Cryptographic systems are classified along three independent dimensions:

1. The type of operations used for performing plaintext to ciphertext :

All the encryption algorithms make use of two general principles; substitution and transposition through which plaintext elements are rearranged. Important thing is that no information should be lost.

2. The number of keys used :

If single key is used by both sender and receiver, it is called symmetric, single-key, secret-key or conventional encryption. If sender and receiver each use a different key, then it is called asymmetric, two-key or public-key encryption.

3. The way in which plaintext is processed :

A block cipher process the input as blocks of elements and generated an output block for each input block. Stream cipher processes the input elements continuously, producing output one element at a time as it goes along.

Q) What are the Symmetric encryption scheme ingredients ?

1. ***Plain Text***: This is the original message or data which is fed into the algorithm as input.
2. ***Encryption Algorithm***: This encryption algorithm performs various substitutions and transformations on the plain text.
3. ***Secret Key***: The key is another input to the algorithm. The substitutions and transformations performed by algorithm depend on the key.

4. ***Cipher Text*****:** This is the scrambled (unreadable) message which is output of the encryption algorithm. This cipher text is dependent on plaintext and secret key. For a given plaintext, two different keys produce two different cipher texts.
5. ***Decryption Algorithm***: This is the reverse of encryption algorithm. It takes the cipher text and secret key as inputs and outputs the plain text.

Q) Define Message authentication Process?

It is a procedure to verify that received messages come from the alleged source and have not been altered. Message authentication may also verify sequencing and timeliness. It is intended

against the attacks like content modification, sequence modification, timing modification and repudiation. For repudiation, concept of digital signatures is used to counter it. There are three classes by which different types of functions that may be used to produce an authenticator. They are:

 Message encryption–the ciphertext serves as authenticator

 Message authentication code (MAC)–a public function of the message and a secret key producing a fixed-length value to serve as authenticator. This does not provide a digital signature because A and B share the same key.

 Hash function–a public function mapping an arbitrary length message into a fixed-length hash value to serve as authenticator. This does not provide a digital signature because there is no key.

Q) Define Hash Function?

A variation on the message authentication code is the one-way hash function. As with the message authentication code, the hash function accepts a variable-size message M as input and produces a fixed-size hash code H(M), sometimes called a message digest, as output. The hash code is a function of all bits of the message and provides an error-detection capability: A change to any bit or bits in the message results in a change to the hash code.

A fixed-length hash value h is generated by a function H that takes as input a message of arbitrary length**: h=H(M).**

 A sends M and H(M)

 B authenticates the message by computing H(M) and checking the match.

PART-B ESSAY QUESTIONS & ANSWERS

Q) Explain Different kinds of security attacks ?

Interruption Sender Receiver An asset of the system is destroyed or becomes unavailable or unusable. It is an attack on availability.

Examples:

- Destruction of some hardware
- Jamming wireless signals
- Disabling file management systems

Interception Sender Receiver

Hacker An unauthorized party gains access to an asset. Attack on confidentiality. **Examples**:

- Wire tapping to capture data in a network.
- Illicitly copying data or programs
- Eavesdropping

Modification:

When an unauthorized party gains access and tampers an asset. Attack is on Integrity.

Examples:

- Changing data file
- Altering a program and the contents of a message

Fabrication An unauthorized party inserts a counterfeit object into the system. Attack on Authenticity. Also called impersonation

Examples:

- Hackers gaining access to a personal email and sending message
- Insertion of records in data files
- Insertion of spurious messages in a network

Q) Explain in brief about Passive Attacks ?

A Passive attack attempts to learn or make use of information from the system, but does not affect system resources. **Two types:**

Release of message content :

It may be desirable to prevent the opponent from learning the contents (i.e sensitive or confidential info) of the transmission.

Traffic analysis :
A more subtle technique where the opponent could determine the location and identity of communicating hosts and could observe the frequency & length of encrypted messages being exchanged there by guessing the nature of communication taking place. Passive attacks are very difficult to detect because they do not involve any alternation of the data. As the communications take place in a very normal fashion, neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. So, the emphasis in dealing with passive attacks is on prevention rather than detection.

Q)Explain in brief about Active Attacks ?

Active attacks involve some modification of the data stream or creation of a false stream. An active attack attempts to alter system resources or affect their operation. ***Four types:***

 Masquerade: Here, an entity pretends to be some other entity. It usually includes one of the other forms of active attack.

 Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

 Modification of messages: It means that some portion of a legitimate message is altered, or that messages are delayed to produce an unauthorized effect.

Ex: “John’s acc no is 2346” is modified as “John’s acc no is 7892”

 Denial of service: This attack prevents or inhibits the normal use or management of communication facilities.

Ex: a: Disruption of entire network by disabling it b: Suppression of all messages to a particular destination by a third party. Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

Q) What are the various security services?
It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.

Confidentiality : Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems. It has been defined as “ensuring that information is accessible only to those authorized to have access”. The

other aspect of confidentiality is the protection of traffic flow from analysis. **Ex:** A credit card number has to be secured during online transaction.

Authentication : This service assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties. Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties. Two specific authentication services defines in X.800 are

 Peer entity authentication: Verifies the identities of the peer entities involved in communication. Provides use at time of connection establishment and during data transmission. Provides confidence against a masquerade or a replay attack

 Data origin authentication: Assumes the authenticity of source of data unit, but does not provide protection against duplication or modification of data units. Supports applications like electronic mail, where no prior interactions take place between communicating entities.

Integrity :

Integrity means that data cannot be modified without authorization. Like confidentiality, it can be applied to a stream of messages, a single message or selected fields within a message. Two types of integrity services are available. They are

 Connection-Oriented Integrity Service: This service deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. Destruction of data is also covered here. Hence, it attends to both message stream modification and denial of service.

 Connectionless-Oriented Integrity Service: It deals with individual messages regardless of larger context, providing protection against message modification only.

An integrity service can be applied with or without recovery. Because it is related to active attacks, major concern will be detection rather than prevention. If a violation is detected and the service reports it, either human intervention or automated recovery machines are required to recover.

Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. This capability is crucial to e-commerce. Without it an individual or entity can deny that he, she or it is responsible for a transaction, therefore not financially liable.

Access Control : This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individuals.

Availability : It is defined to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity. The availability can significantly be affected by a variety of attacks, some amenable to automated counter measures i.e authentication and encryption and others need some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

Q) List out the Specific Security Mechanisms:

Incorporated into the appropriate protocol layer in order to provide some of the OSI security services,

 Encipherment: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys.

 Digital Signature: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

 Access Control: A variety of techniques used for enforcing access permissions to the system resources.

 Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

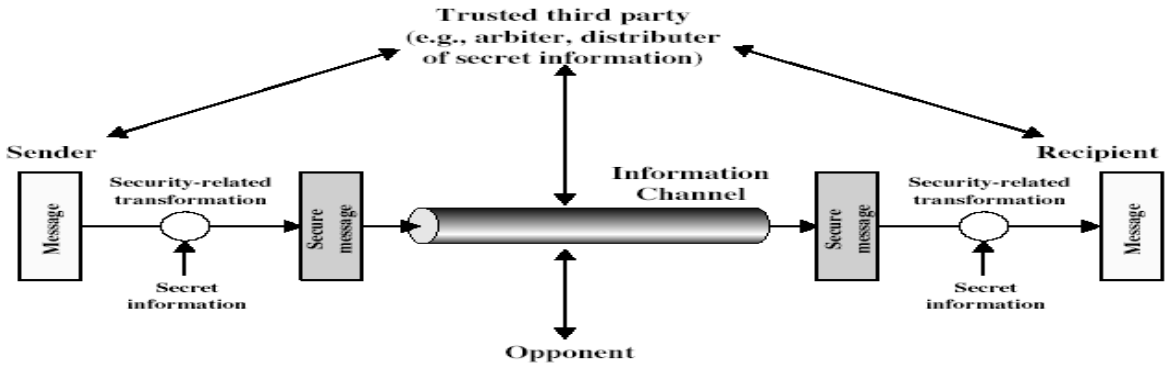
Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

 Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

 Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes once a breach of security is suspected.

 Notarization: The use of a trusted third party to assure certain properties of a data exchange

Q)Summarize about Inter Network Security Model?



Data is transmitted over network between two communicating parties, who must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination by use of communication protocols by the two parties. Whenever an opponent presents a threat to confidentiality authenticity of information,

security aspects come into play. Two components are present in almost all the security providing techniques.

 A security-related transformation on the information to be sent making it unreadable by the opponent, and the addition of a code based on the contents of the message, used to verify the identity of sender.

 Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

A trusted third party may be needed to achieve secure transmission. It is responsible for distributing the secret information to the two parties, while keeping it away from any opponent. It also may be needed to settle disputes between the two parties regarding authenticity of a message transmission. The general model shows that there are four basic tasks in designing a particular security service:

Q)**What is Security? What are the security layers ,a successful organization should have?**

"The quality or state of being secure--to be free from danger"

- Physical Security – to protect physical items,objects or areas of organization from unauthorized access and misuse
- Personal Security – involves protection of individuals or group of individuals who are authorized to access the organization and its operations
- Operations security – focuses on the protection of the details of particular operations or series of activities.
- Communications security – encompasses the protection of organization's communicatons media ,technology and content
- Network security – is the protection of networking components,connections,and contents
- Information security – is the protection of information and its critical elements,including the systems and hardware that use ,store,and transmit the information

Q)What are the critical characteristics of information?

- **Availability** – enables authorized users – persons or computer systems – to access information without interference or obstruction and receive it in the required format
- **Accuracy** – Accuracy of information refers to information which is free from mistakes or errors and has the value the end user expects(Eg inaccuracy of your bank account may result in mistakes such as bouncing of a check).

- **Authenticity** – refers to quality or state of being genuine or original,rather than reproduction or fabrication. Information is authentic when the contents are original as it was created,palced or stored or transmitted.(The information you receive as e-mail may not be authentic when its contents are modified what is known as **E-mail spoofing**).
- **Confidentiality** – Information has confidentiality when disclosure or exposure to unauthorized individuals or systems is prevented Confidentiality ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information.confidentiality is breached.
- **Integrity** – Information has integrity when it is whole,complete, and uncorrupted The integrity of information is threatened when it is exposed to corruption,damage,destruction,other disruption of its authentic state.(Many computer virues or worm are designed with the explicit purpose of corrupting data. Information integrity is the corner stone of information systems,because information is of no value or use if users cannot verify its integrity. Redundancy bits and check bits can compensate for internal and external threats to integrity of information.
- **Utility** – The utility of information is the quality or state of having value for some purpose or end. (For example,the US census data reveals information about the voters like their gender,age,race,and so on.
- **Possession** – the possession of information is the quality or state of having ownership or control of some object or item. Breach of possession does not result in breach of confidentiality.(Illegal possession of encrypted data never allows someone to read it without proper decryption methods).

Q)What are the components of an information system?

An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization

The **software component** of IS comprises applications, operating systems, and assorted command utilities. Software programs are the vessels that carry the life blood of information through an organization. Information security is often implemented as an after thought rather than developed as an integral component from the beginning. Software programs become an easy target of accidental or intentional attacks.

Hardware is the physical technology that houses and executes the software, stores and carries the data, provides interfaces for the entry and removal of information from the sytem.Physical security policies deals with the hardware as a physical asset and with the protection of these assets from harm or theft.

Data – Data stored,processed,and transmitted through a computer system must be protected. Data is the most valuable asset possessed by an organization and it is the main target of intentional attacks.

People – Though often overlooked in computer security considerations, people have always been a threat to information security and they are the weakest link in a security chain.. Policy, education and training,awareness,and technology should be properly employed to prevent people from accidently or intentionally damaging or losing information.

Procedures – Procedures are written instructions for accomplishing when an unauthorized user obtains an organization's procedures ,it poses threat to the integrity of the information. Educating employees about safeguarding the procedures is as important as securing the information system. Lax in security procedures caused the loss of over ten million dollars before the situation was corrected.

Networks - Information systems in LANs are connected to other networks such as the internet and new security challenges are rapidly emerge. Apart from locks and keys which are used as physical security measures ,network security also an important aspect to be considered.

Q)What is a block cipher?what are the various types of block cipher encryption algorithms?

- A block cipher is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. So for example, a 64-bit block cipher will take in 64 bits of plaintext and encrypt it into 64 bits of ciphertext. In cases where bits of plaintext is shorter than the block size, padding schemes are called into play. Majority of the symmetric ciphers used today are actually block ciphers. DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group.

Popular block ciphers:

- **DES** - DES, which stands for Data Encryption Standard, used to be the most popular block cipher in the world and was used in several industries. It's still popular today, but only because it's usually included in historical discussions of encryption algorithms. The DES algorithm became a standard in the US in 1977. However, it's already been proven to be vulnerable to brute force attacks and other cryptanalytic methods. DES is a 64-bit cipher that works with a 64-bit key. Actually, 8 of the 64 bits in the key are parity bits, so the key size is technically 56 bits long.

- **3DES** - As its name implies, 3DES is a cipher based on DES. It's practically DES that's run three times. Each DES operation can use a different key, with each key being 56 bits long. Like DES, 3DES has a block size of 64 bits. Although 3DES is many times stronger than DES, it is also much slower (about 3x slower). Because many organizations found 3DES to be too slow for many applications, it never became the ultimate successor of DES. That distinction is reserved for the next cipher in our list - AES.

- **AES** - A US Federal Government standard since 2002, AES or Advanced Encryption Standard is arguably the most widely used block cipher in the world. It has a block size of 128 bits and supports three possible key sizes - 128, 192, and 256 bits. The longer the key size, the stronger the encryption. However, longer keys also result in longer processes of encryption. For a discussion on encryption key lengths, read Choosing Key Lengths for Encrypted File Transfers.

- **Blowfish** - This is another popular block cipher (although not as widely used as AES). It has a block size of 64 bits and supports a variable-length key that can range from 32 to 448 bits. One thing that makes blowfish so appealing is that Blowfish is unpatented and royalty-free.

- **Twofish** - Yes, this cipher is related to Blowfish but it's not as popular (yet). It's a 128-bit block cipher that supports key sizes up to 256 bits long.

Q)What is a stream cipher?what are the various types of stream cipher encryption algorithms?

A stream cipher is an encryption algorithm that encrypts 1 bit or byte of plaintext at a time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.

The One-Time Pad, which is supposed to employ a purely random key, can potentially achieve "perfect secrecy". That is, it's supposed to be fully immune to brute force attacks. The problem with the one-time pad is that, in order to create such a cipher, its key should be as long or even longer than the plaintext. In other words, if you have 500 MegaByte video file that you would like to encrypt, you would need a key that's at least 4 Gigabits long.

Clearly, while Top Secret information or matters of national security may warrant the use of a one-time pad, such a cipher would just be too impractical for day-to-day public use. The key of a

stream cipher is no longer as long as the original message. Hence, it can no longer guarantee "perfect secrecy". However, it can still achieve a strong level of security.

Popular stream ciphers:

RC4 - RC4, which stands for Rivest Cipher 4, is the most widely used of all stream ciphers, particularly in software. It's also known as ARCFOUR or ARC4. RC4 has been used in various protocols like WEP and WPA (both security protocols for wireless networks) as well as in TLS. Unfortunately, recent studies have revealed vulnerabilities in RC4, prompting Mozilla and Microsoft to recommend that it be disabled where possible. In fact, RFC 7465 prohibits the use of RC4 in all versions of TLS.

An interesting distinction is made between two types of stream ciphers { synchronous stream ciphers and self-synchronizing stream ciphers}. A synchronous stream cipher is a cipher where the a key stream is generated separately from the plaintext and is then combined with the plaintext later to form the cipher text.

Q)Illustrate Feistel Cipher Structure with a neat sketch?

In cryptography, a **Feistel cipher** is a symmetric structure used in the construction of block **ciphers**, named after the German IBM cryptographer Horst **Feistel**; it is also commonly known as a **Feistel** network. A large set of block **ciphers** use the scheme, including the Data Encryption Standard (DES).

The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore the size of the code or circuitry required to implement such a cipher is nearly halved.

A Feistel network is an iterated cipher with an internal function called a round function. Many modern and also some old symmetric block ciphers are based on Feistel networks (e.g. GOST 28147-89 block cipher), and the structure and properties of Feistel ciphers have been extensively explored by cryptographers. Specifically, Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with K_i used as the seed, then 3 rounds are sufficient to make the block cipher a pseudorandom permutation, while 4 rounds are sufficient to make it a "strong" pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation). Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby–Rackoff block ciphers. Further theoretical work has generalized the construction somewhat, and given more precise bounds for security.

Construction details

et Fbe the round function and let $K_0, K_1, \ldots, K_n$be the sub-keys for the rounds $0, 1, \ldots, n$respectively.

Then the basic operation is as follows:

Split the plaintext block into two equal pieces, (L_0, R_0)

For each round $i = 0, 1, \ldots, n$, compute

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i).$$

Then the ciphertext is (R_{n+1}, L_{n+1}).

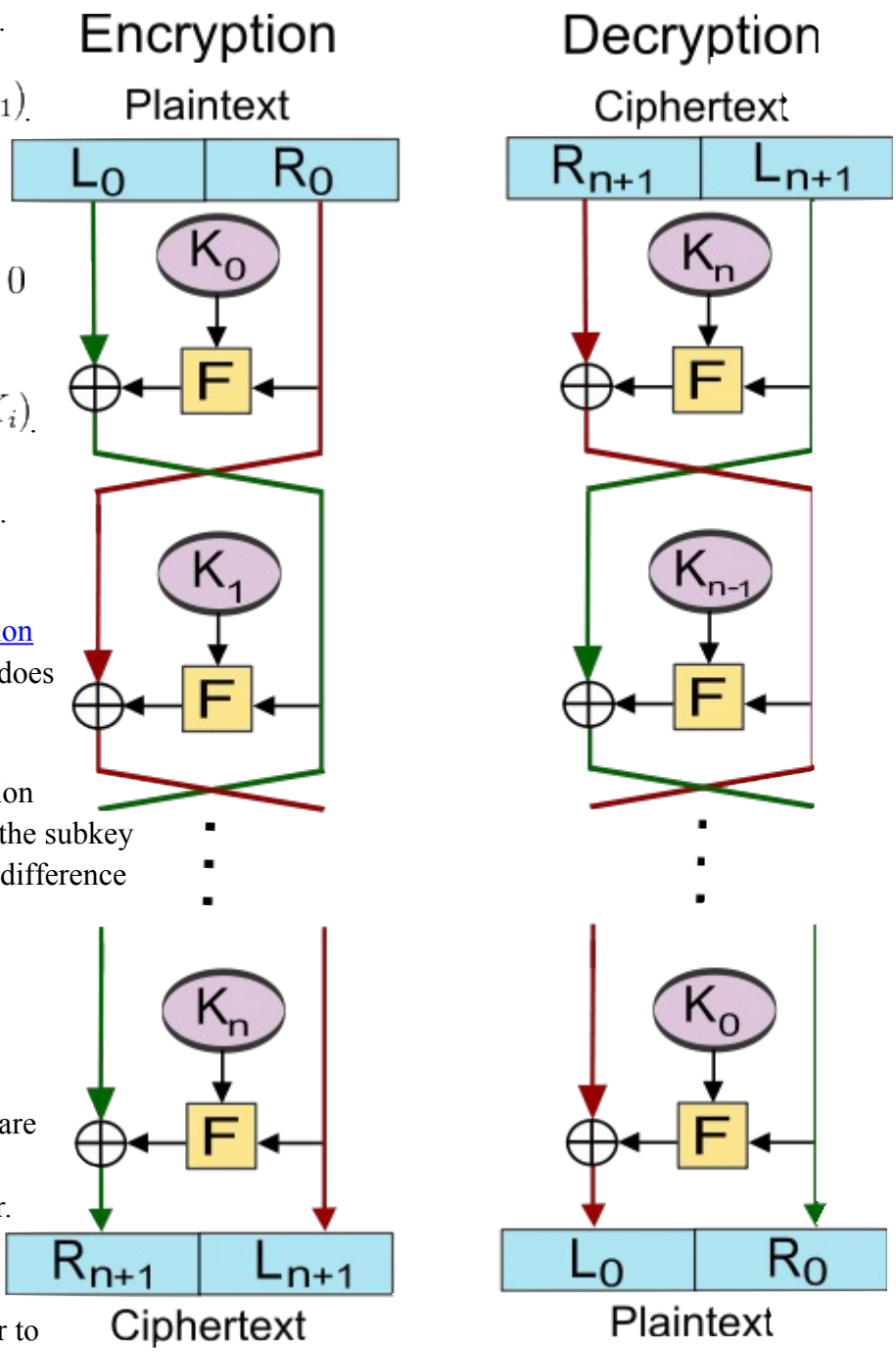
Decryption of a ciphertext (R_{n+1}, L_{n+1}) is accomplished by computing for $i = n, n-1, \ldots, 0$

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i).$$

Then (L_0, R_0) is the plaintext again.

One advantage of the Feistel model compared to a substitution-permutation network is that the round function F does not have to be invertible.

The diagram illustrates both encryption and decryption. Note the reversal of the subkey order for decryption; this is the only difference between encryption and decryption.



Unbalanced Feistel cipher

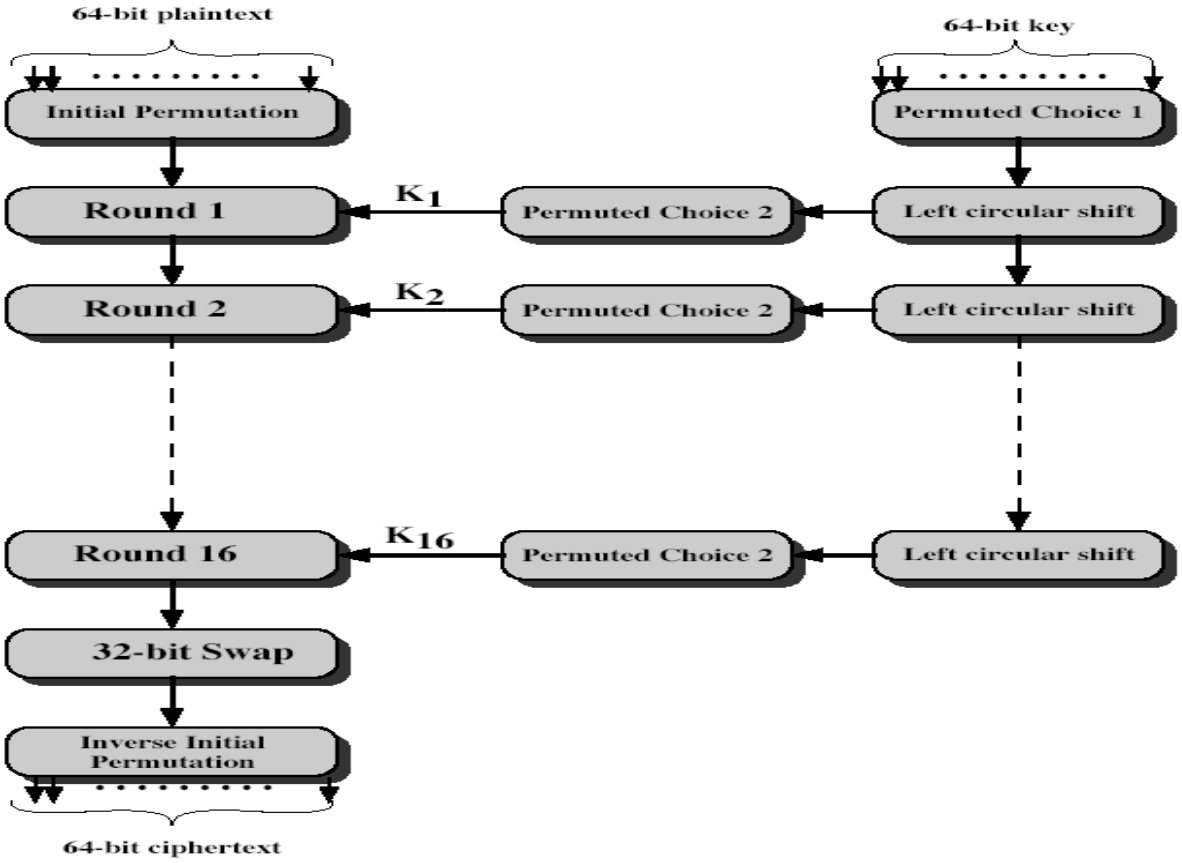
Unbalanced Feistel ciphers use a modified structure where L_0 and R_0 are not of equal lengths.[4] The Skipjack cipher is an example of such a cipher. The Texas Instruments Digital Signature Transponder uses a proprietary unbalanced Feistel cipher to perform challenge-response authentication.

The Thorp shuffle is an extreme case of an unbalanced Feistel cipher in which one side is a single bit. This has better provable security than a balanced Feistel cipher but requires more rounds.

Explain Data Encryption Standard (DES) with block structure and random key generations

IBM developed Lucifer cipher by team led by Feistel used 64-bit data blocks with 128-bit key then redeveloped as a commercial cipher with input from NSA and others in 1973 NBS issued request for proposals for a national cipher standard IBM submitted their revised Lucifer which was eventually accepted as the DES

DES Encryption



The basic process in enciphering a 64-bit data block using the DES, shown on the left side, consists of:

- an initial permutation (IP)

- 16 rounds of a complex key dependent round function involving substitution and permutation functions

- a final permutation, being the inverse of IP

The right side shows the handling of the 56-bit key and consists of:

- an initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves

- 16 stages to generate the subkeys using a left circular shift and a permutation

IP

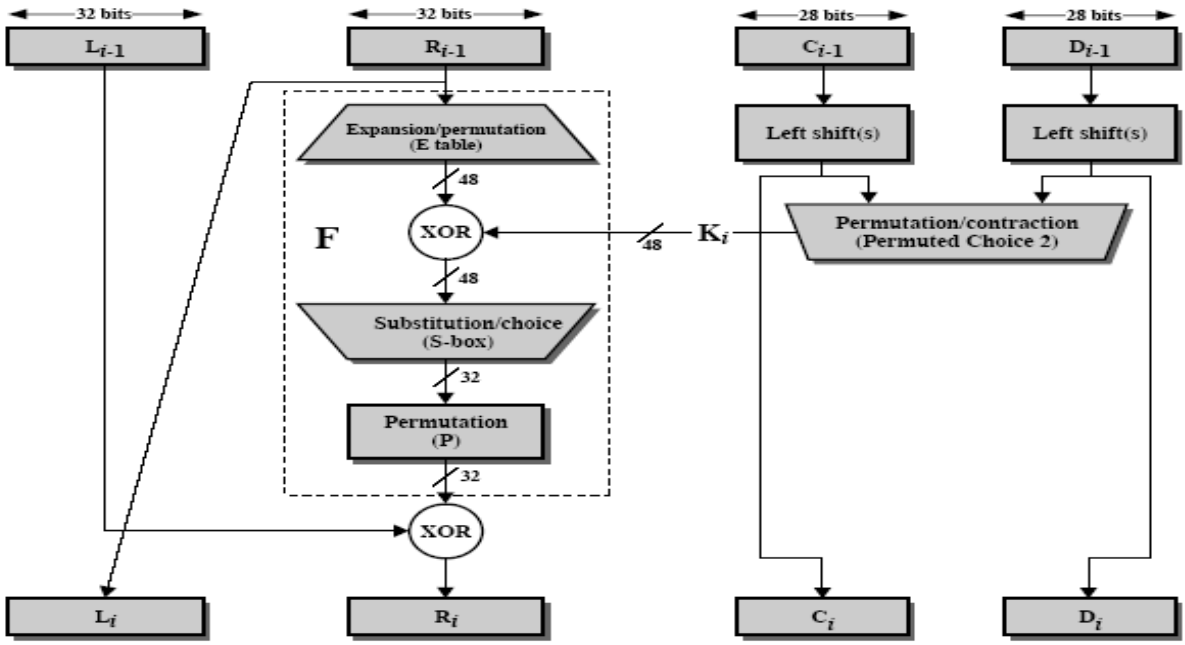
There is an *initial permutation* **IP** of the 64 bits of the message data **M**. This rearranges the bits according to the following table, where the entries in the table show the new arrangement of the bits from their initial order. The 58th bit of **M** becomes the first bit of **IP**. The 50th bit of **M** becomes the second bit of **IP**. The 7th bit of **M** is the last bit of **IP**.

IP

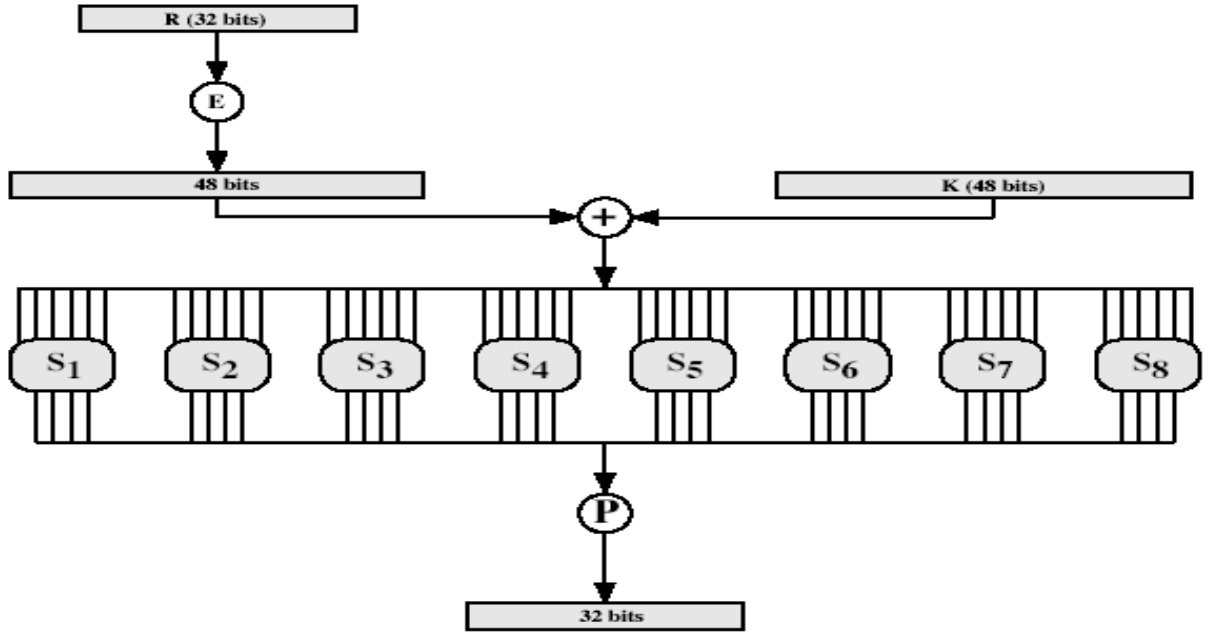
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

DES Round Structure

- uses two 32-bit L & R halves
- as for any Feistel cipher can describe as:
- $L_i = R_{i-1}$
- $R_i = L_{i-1}$ xor F(R_{i-1}, K_i)
- takes 32-bit R half and 48-bit subkey and:
    - expands R to 48-bits using perm E
    - adds to subkey
    - passes through 8 S-boxes to get 32-bit result
    - finally permutes this using 32-bit perm P



Calculation of F(R,K)

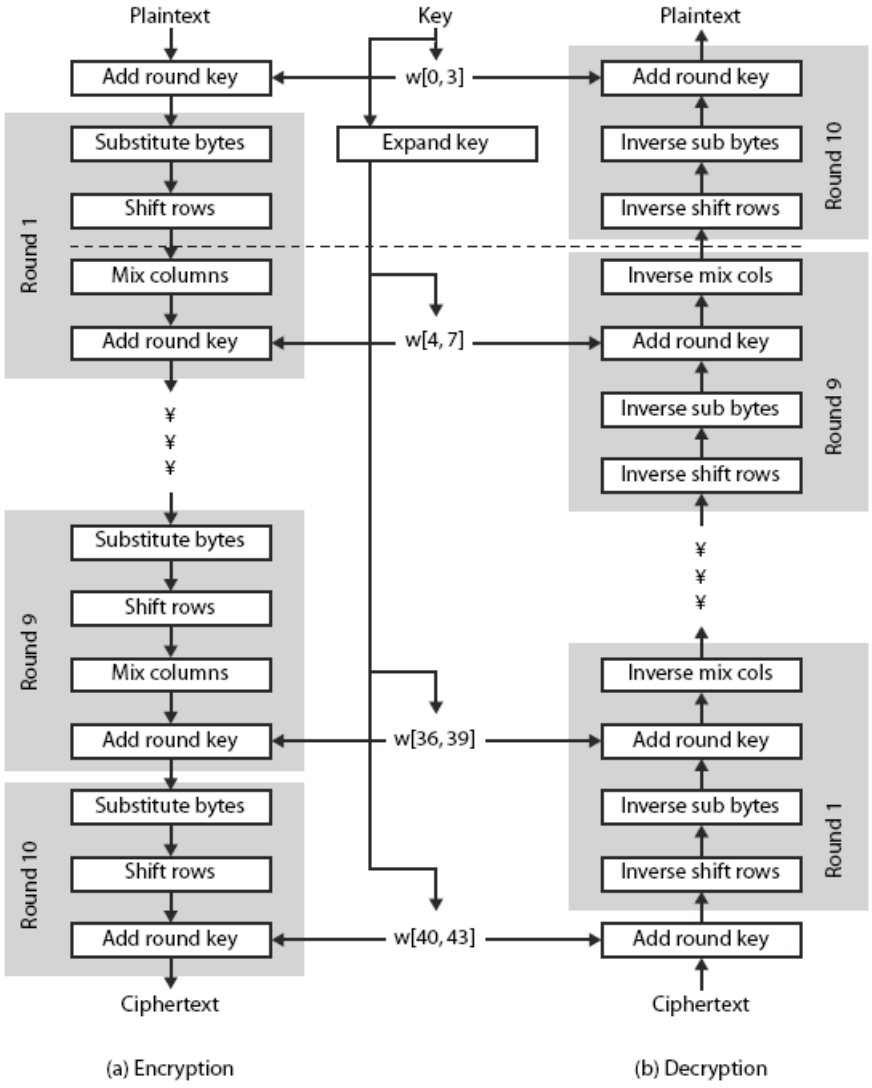


Q)Explain Advanced Encryption Standard (AES) with block structure and random key generations

AES

- data block of 4 columns of 4 bytes is state
- key is expanded to array of words
- has 9/11/13 rounds in which state undergoes:
    - byte substitution (1 S-box used on every byte)
    - shift rows (permute bytes between groups/columns)
    - mix columns (subs using matrix multiply of groups)
    - add round key (XOR state with key material)
    - view as alternating XOR key & scramble data bytes
- initial XOR key material & incomplete last round
- with fast XOR & table lookup implementation

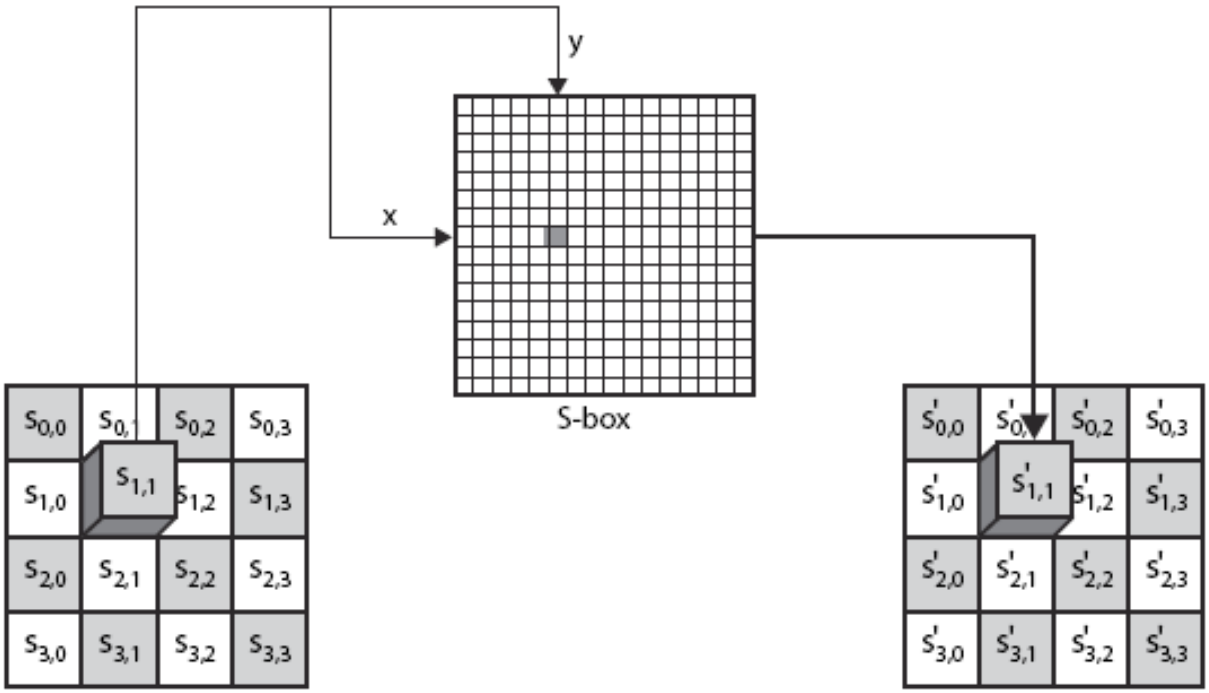
AES Structure:



1. an iterative rather than Feistel cipher
2. key expanded into array of 32-bit words
    a. four words form round key in each round
3. 4 different stages are used as shown
4. has a simple structure
5. only AddRoundKey uses key
6. AddRoundKey a form of Vernam cipher

7. each stage is easily reversible
8. decryption uses keys in reverse order
9. decryption does recover plaintext
10. final round has only 3 stages

Substitute Bytes



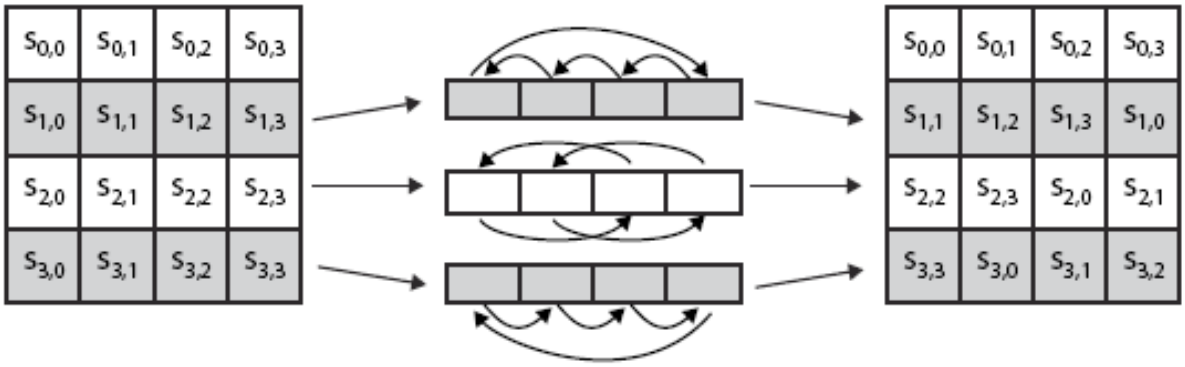
EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

SHIFT ROWS:

- **a circular byte shift in each each**
  - **1st row is unchanged**
  - **2nd row does 1 byte circular shift to left**
  - **3rd row does 2 byte circular shift to left**
  - **4th row does 3 byte circular shift to left**
- **decrypt inverts using shifts to right**
- **since state is processed by columns, this step permutes bytes between the columns**



87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

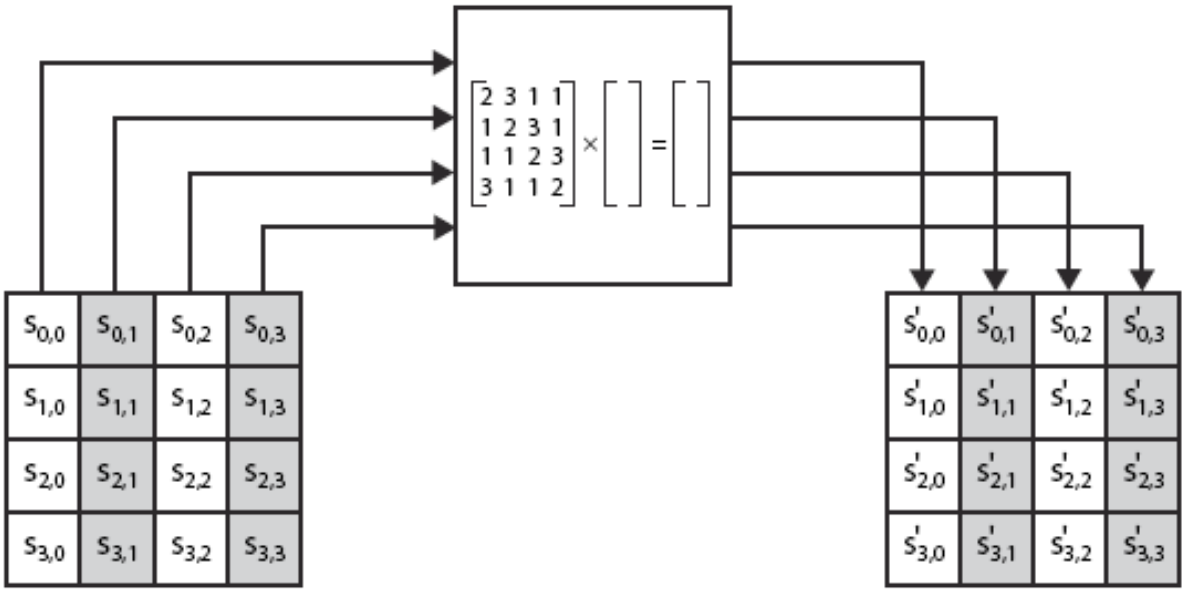
→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

MIX COLUMNS:

- **each column is processed separately**
- **each byte is replaced by a value dependent on all 4 bytes in the column**
- **effectively a matrix multiplication in GF(2^8) using prime poly m(x) =$x^8+x^4+x^3+x+1$**

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$



87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$$(\{02\} \bullet \{87\}) \oplus (\{03\} \bullet \{6E\}) \oplus \{46\} \oplus \{A6\} = \{47\}$$

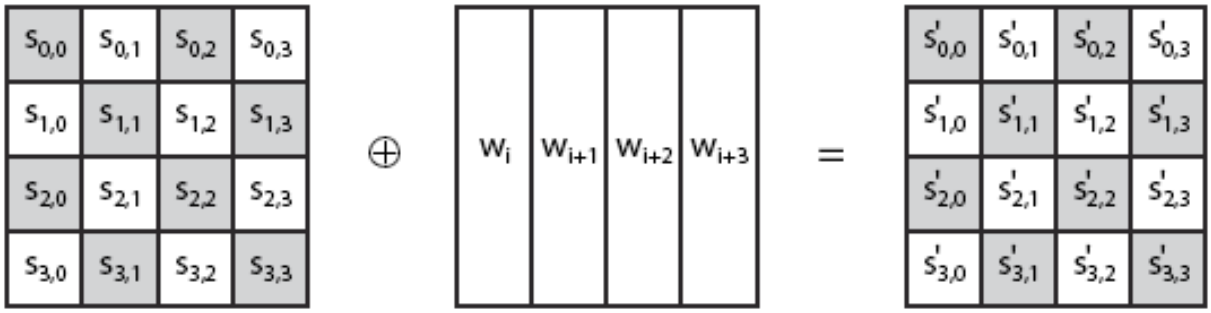
$$\{87\} \oplus (\{02\} \bullet \{6E\}) \oplus (\{03\} \bullet \{46\}) \oplus \{A6\} = \{37\}$$

$$\{87\} \oplus \{6E\} \oplus (\{02\} \bullet \{46\}) \oplus (\{03\} \bullet \{A6\}) = \{94\}$$

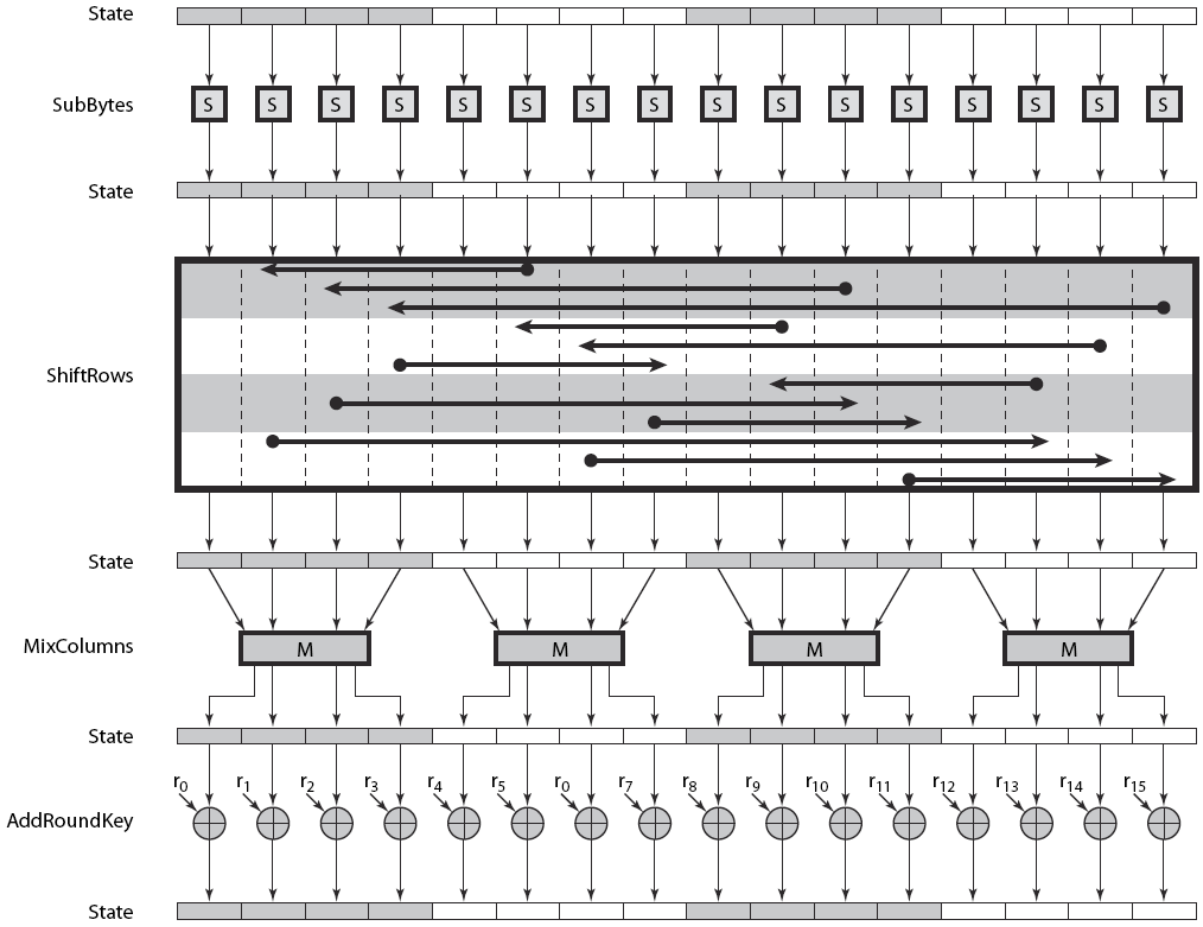
$$(\{03\} \bullet \{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\} \bullet \{A6\}) = \{ED\}$$

Add Round Key

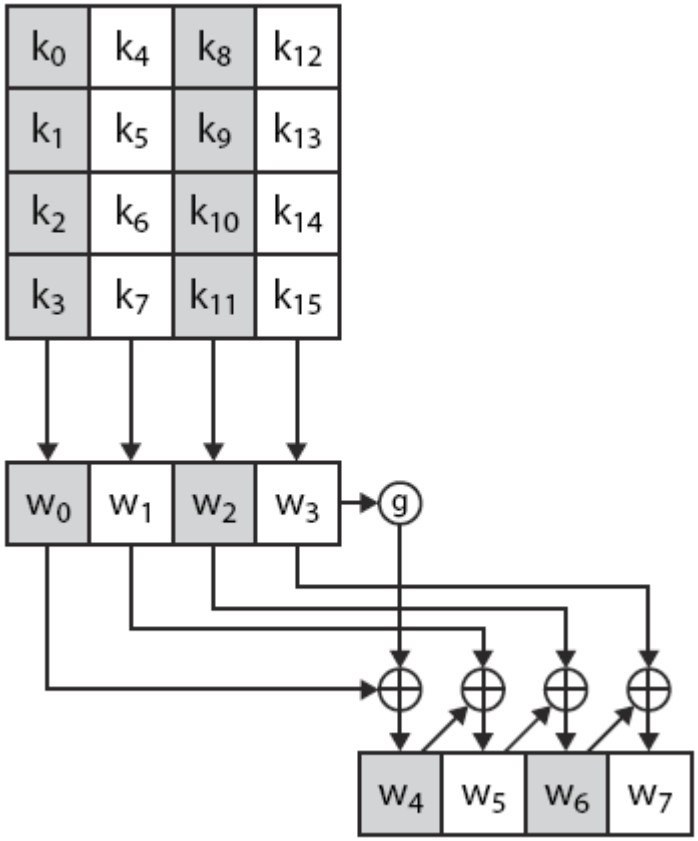
- XOR state with 128-bits of the round key
- again processed by column (though effectively a series of byte operations)
- inverse for decryption identical
  - since XOR own inverse, with reversed keys
- designed to be as simple as possible
  - a form of Vernam cipher on expanded key
  - requires other stages for complexity / security



AES ROUND

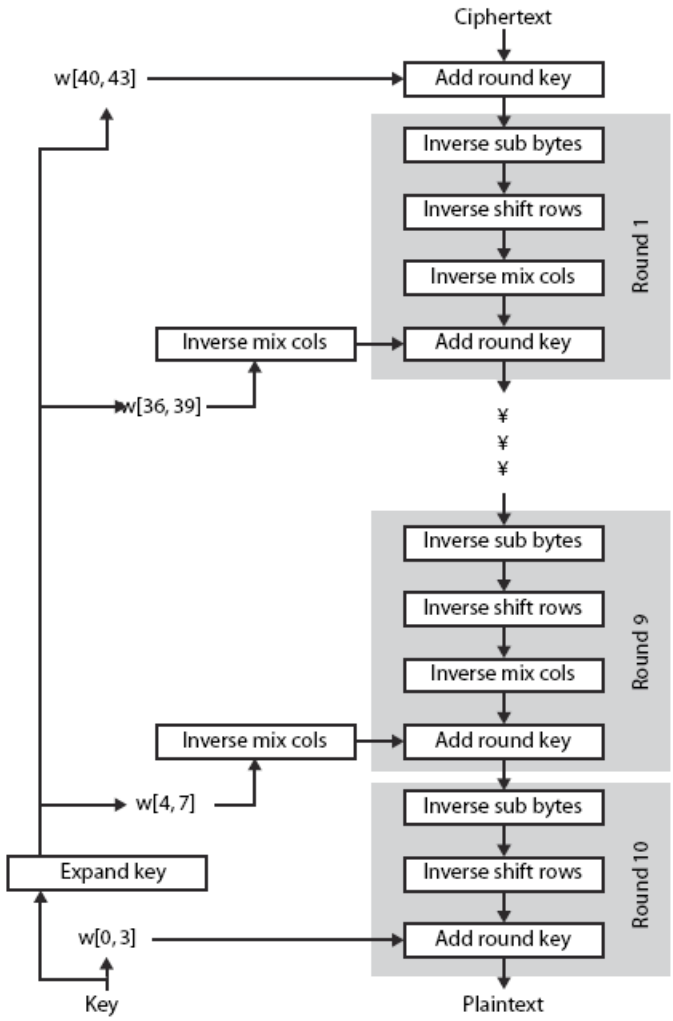


AES Key Expansion



AES Decryption

- AES decryption is not identical to encryption since steps done in reverse
- but can define an equivalent inverse cipher with steps as for encryption
    - but using inverses of each step
    - with a different key schedule
- works since result is unchanged when
    - swap byte substitution & shift rows
    - swap mix columns & add (tweaked) round key

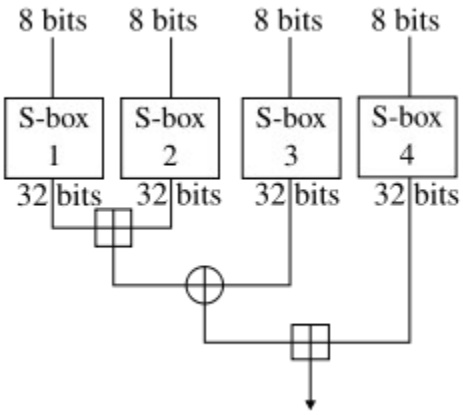


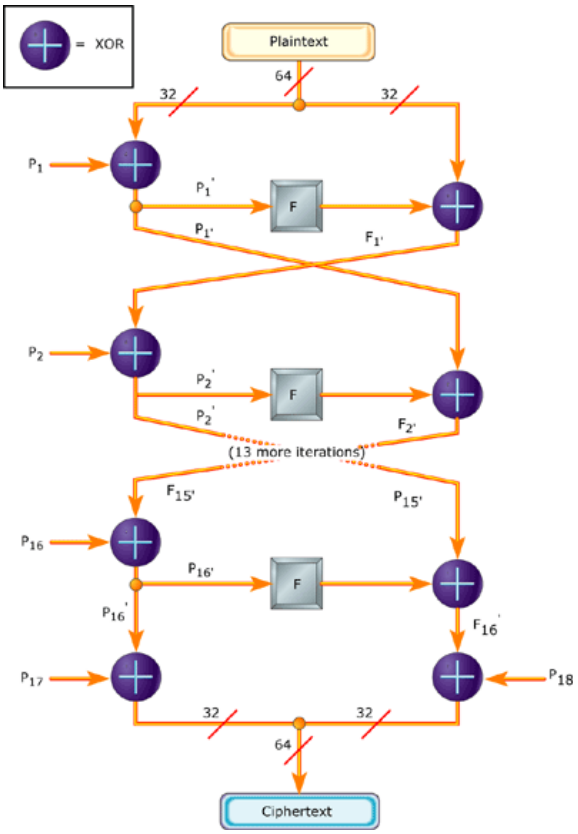
Q)What is BLOW FISH explain its encrypation procedure with Feistel cipher structure?

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention.

The Algorithm

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[2] It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes.





Q) Discuss about Key Distribution process in Symmetric Key cryptosystem?

- symmetric schemes require both parties to share a common secret key
- issue is how to securely distribute this key
- often secure system failure due to a break in the key distribution scheme
- given parties A and B have various **key distribution** alternatives:
  - A can select key and physically deliver to B
  - third party can select & deliver key to A & B

- if A & B have communicated previously can use previous key to encrypt a new key
- if A & B have secure communications with a third party C, C can relay key between A & B

Key Distribution Scenario

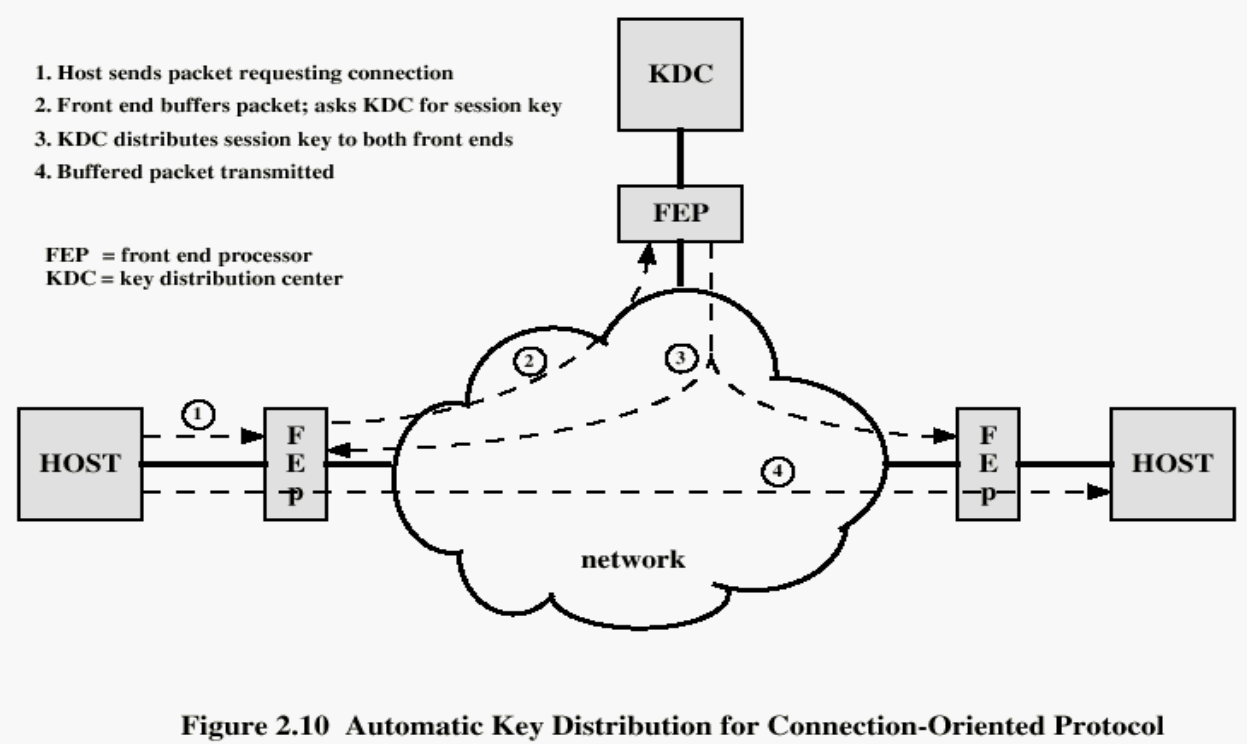


Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

- hierarchies of KDC's required for large networks, but must trust each other
- session key lifetimes should be limited for greater security
- use of automatic key distribution on behalf of users, but must trust system
- use of decentralized key distribution
- controlling purposes keys are used for

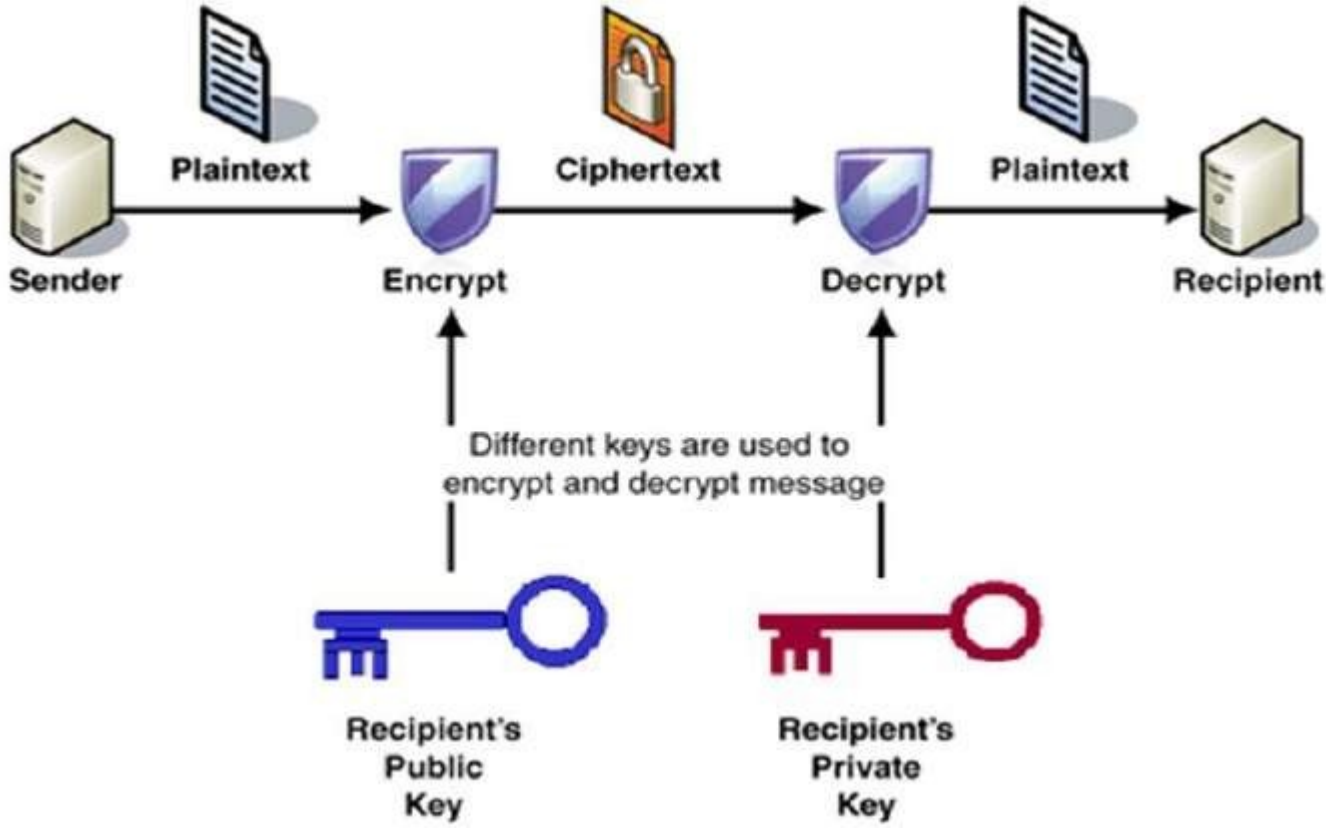
Q)What is Public Key Cryptography and distinguish public Vs private key?

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration −



The most important properties of public key encryption scheme are −

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.

- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Q.Discuss about RC4 Stream Cipher technique?

A proprietary cipher owned by RSA, designed by Ron Rivest in 1987.
Became public in 1994.
Simple and effective design.
Variable key size, byte-oriented stream cipher.
Widely used (web SSL/TLS, wireless WEP(Wired Equivalent Privacy)).

Encryption:

The cipher internal state consists of
–a 256-byte array S, which contains a permutation of 0 to 255 total number of possible states is 256! $\approx 2^{1700}$
–two indexes: i, j
i = j = 0
Loop
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
swap(S[i], S[j])
output (S[i] + S[j]) (mod 256)
End Loop

Key Generation

Generate the initial permutation from a key k;
maximum key length is 2048 bits
First divide k into L bytes
Then
for i = 0 to 255 do
S[i] = i
j = 0
for i = 0 to 255 do

j = (j + S[i] + k[i mod L])(mod 256)
swap (S[i], S[j])

Q) Explain RSA algorithm with an example?

A user of RSA creates and then publishes a public key based on two large prime, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.[2]Breaking RSA encryption is known as the RSA problem; whether it is as hard as the factoring problem remains an open question.

RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

Example Let's select: P =11 Q=3
The calculation of n and PHI is:
n=P × Q = 11 × 3 =33
PHI = (p-1)(q-1) = 20
The factors of *PHI* are 1, 2, 4, 5, 10 and 20. Next the public exponent e is generated so that the greatest common divisor of *e* and *PHI* is 1 (e is relatively prime with *PHI*). Thus, the smallest value for e is:
e = 3
Next we can calculate d from:
(3 x d) mod (20) = 1 [Link]
Thus the smallest value of d will be:
d = 7
Encryption key [33,3]
Decryption key [33,7]
Then, with a message of 4, we get:
Cipher = (m)e mod n
Cipher = (4)3 mod 33 = 31
Decoded = (cipher)d mod n
Decoded = 317 mod 33 = 4

Q) Explain about MD5 message digest algorithm?

The MD5 message-digest algorithm was developed by Ron Rivest at MIT and it remained as the most popular hash algorithm until recently. The algorithm takes as input, a message of arbitrary length and produces as output, a 128-bit message digest. The input is processed in 512-bit blocks. The processing consists of the following steps:

1.) *Append Padding bits*: The message is padded so that its length in bits is congruent to 448 modulo 512 i.e. the length of the padded message is 64 bits less than an integer multiple of 512 bits. Padding is always added, even if the message is already of the desired length. Padding consists of a single 1-bit followed by the necessary number of 0-bits.

2.) *Append length*: A 64-bit representation of the length in bits of the original message (before the padding) is appended to the result of step-1. If the length is larger than 264, the 64 least representative bits are taken.

3.) *Initialize MD buffer*: A 128-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as four 32-bit registers (A, B, C, D) and are initialized with A=0x01234567, B=0x89ABCDEF, C=0xFEDCBA98, D=0x76543210 i.e. 32-bit integers (hexadecimal values).

4.) *Process Message in 512-bit (16-word) blocks*: The heart of algorithm is the compression function that consists of four rounds of processing and this module is labeled HMD5 in the above figure and logic is illustrated in the following figure. The four rounds have a similar structure, but each uses a different primitive logical function, referred to as F, G, H and I in the specification. Each block takes as input the current 512-bit block being processed Yq and the 128-bit buffer value ABCD and updates the contents of the buffer.

5.) *Output*: After all L 512-bit blocks have been processed, the output from the Lth stage is the 128- bit message digest. MD5 can be summarized as follows:

CV0 = IV CVq+1 = SUM32(CVq,RFIYqRFH[Yq,RFG[Yq,RFF[Yq,CVq]]]]) MD = CVL

Where, IV = initial value of ABCD buffer, defined in step 3. Yq = the qth 512-bit block of the message

L = the number of blocks in the message

CVq = chaining variable processed with the qth block of the message.

RFx = round function using primitive logical function x.

MD = final message digest value SUM32 = Addition modulo 232 performed separately.