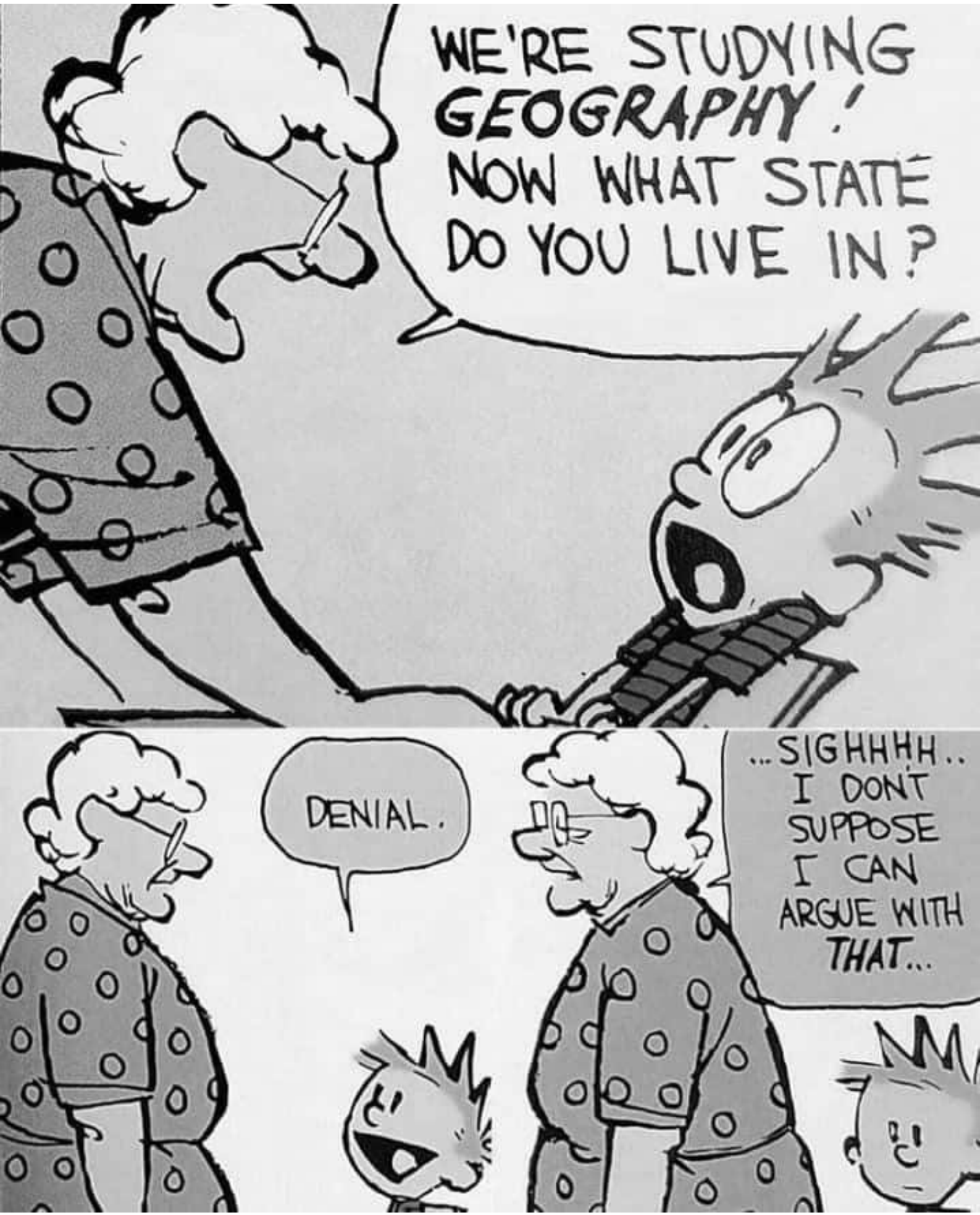


SYLLABUS
[Academic Session: 2016–17]

CRYPTOGRAPHY AND NETWORK SECURITY [ETIT–403]

Instructions to Paper Setters:

1. *Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 25 marks.*
2. *Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be of 12.5 marks.*

Objectives: Syllabus should be proposed so as to be covered in 42 to 45 lectures (assuming 14 or 15 weeks session). Syllabus should be evenly divided into 4 Units only.

UNIT–I

Basic Cryptographic Techniques, Computational Complexity, Finite Fields, Number Theory, DES and AES, Public Key Cryptosystems, Traffic Confidentiality ,Cryptanalysis, Intractable (Hard) Problems, Hash Functions, OSI Security Architecture Privacy of Data.

[T1, T2][No. of Hrs: 11]

UNIT–II

Linear Cryptanalysis, Differential Cryptanalysis, DES, Triple DES, Message Authentication and Digital Signatures, Attacks on Protocols, Elliptic Curve Architecture and Cryptography, Public Key Cryptography and RSA, , Evaluation criteria for AES, Key Management, Authentication requirements Digital forensics including digital evidence handling: Media forensics, Cyber forensics, Software forensics, Mobile forensics. **[T1, T2][No. of Hrs: 11]**

UNIT–III

Buffer Flow attack, Distributed Denial of service attack, Weak authentication, Design of Substitution Boxes (SBoxes), Hash Functions , Security of Hash Functions, Secure Hash Algorithm, Authentication applications, Kerberos, IP security, Pretty Good Privacy (PGP), Web Security Light weight cryptography for mobile devices, Side channel attacks.

[T1, T2][No. of Hrs: 11]

UNIT–IV

System security, Security Standards, Intruders, and Viruses, Firewalls, Malicious software, Intrusion Detection System, Intrusion Prevention System, Trusted Systems, Virus Counter measures, Authentication Strategies. **[T1, T2][No. of Hrs: 11]**

MODEL TEST PAPER–I
FIRST TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 1.30 hrs. **M.M. : 30**

Note: *Question no.1 is compulsory and attempt any two from the rest. In all attempt 3 questions.*

Q.1. (a) What is the Public Key Encryption?

Ans. Public key encryption use public and private key for encryption and decryption. In this mechanism, public key is used to encrypt messages and only the corresponding private key can be used to decrypt them. To encrypt a message, a sender has to know recipient's public key.

Q.1. (b) What are the requirements of a hash function?

Ans. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup. Hash functions accelerate table or database lookup by detecting duplicated records in a large file. An example is finding similar stretches in DNA sequences. They are also useful in cryptography. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown; it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value. This is used for assuring integrity of transmitted data, and is the building block for HMACs, which provide message authentication.

Q.1. (c) What is the difference between a cryptographer and a cryptanalyst?

Ans. The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

In addition to mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation. . Cryptography referred almost exclusively to *encryption*, which is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text).Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text.

Q.1. (*d*) What do you mean by software forensics?

Ans. Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Q.2. (*a*) What do you mean by hash function? What are various applications of hash function?

Ans. A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is representative of the original string of characters, but is normally smaller than the original.

Hashing is done for indexing and locating items in databases because it is easier to find the shorter hash value than the longer string. Hashing is also used in encryption.

This term is also known as a hashing algorithm or message digests function. Hashing is used with a database to enable items to be retrieved more quickly. Hashing can also be used in the encryption and decryption of digital signatures. The hash function transforms the digital signature, then both the hash value and signature are sent to the receiver. The receiver uses the same hash function to generate the hash value and then compares it to that received with the message. If the hash values are the same, it is likely that the message was transmitted without errors.

One example of a hash function is called folding. This takes an original value, divides it into several parts, then adds the parts and uses the last four remaining digits as the hashed value or key. Another example is called digit rearrangement. This takes the digits in certain positions of the original value, such as the third and sixth numbers, and reverses their order. It then uses the number left over as the hashed value.

It is nearly impossible to determine the original number based on a hashed value, unless the algorithm that was used is known.

Q.2. (*b*) What do you mean by differential cryptanalysis?

Ans: Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key. Differential cryptanalysis is usually a chosen plaintext attack, meaning that the attacker must be able to obtain cipher texts for some set of plaintexts of his choosing. There are, however, extensions that would allow a known plaintext or even a cipher text-only attack. The basic method uses pairs of plaintext related by a constant difference; difference can be defined in several ways, but the exclusive OR (XOR) operation is usual. The attacker then computes the differences of the corresponding cipher texts, hoping to detect statistical patterns in their distribution. The resulting pair of differences is called a differential. Their statistical properties depend upon the nature of the S-boxes used for encryption, so the attacker analyses differentials (Δ_X, Δ_Y), where $\Delta_Y = S(X \square'' \oplus \Delta_X) \oplus'' S(X)$ ($\oplus''$ denotes exclusive or) for each such S-box S. In the basic attack, one particular cipher text difference is expected to be especially frequent; in this way, the cipher can be distinguished from random. More sophisticated variations allow the key to be recovered faster than exhaustive search.

In the most basic form of key recovery through differential cryptanalysis, an attacker requests the cipher texts for a large number of plaintext pairs, then assumes that the differential holds for at least $r - 1$ rounds, where r is the total number of rounds. The attacker then deduces which round keys (for the final round) are possible, assuming the difference between the blocks before the final round is fixed. When round keys are short, this can be achieved by simply exhaustively decrypting the cipher text pair's one round with each possible round key. When one round key has been deemed a potential round key considerably more often than any other key, it is assumed to be the correct round key.

For any particular cipher, the input difference must be carefully selected for the attack to be successful. An analysis of the algorithm's internals is undertaken; the standard method is to trace a path of highly probable differences through the various stages of encryption, termed a differential characteristic.

Since differential cryptanalysis became public knowledge, it has become a basic concern of cipher designers. New designs are expected to be accompanied by evidence that the algorithm is resistant to this attack, and many, including the Advanced Encryption Standard, have been proven secure against the attack.

Q.3. (*a*) What are various Security Services of Cryptography?

Ans. The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

Confidentiality: Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy. Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity: It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication: Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants "

- Message authentication identifies the originator of the message without any regard router or system that has sent the message.
- Entity authentication is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation: It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Q.3. (*b*) How do you use RSA for both authentication and secrecy?

Ans. RSA is a public key encryption algorithm. The RSA algorithms are based on the mathematical part that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.

For authentication: One can encrypt the hash (MD4/SHA) of the data with a private key. This is known as digital signature.

For Secrecy: Secrecy/confidentiality is achieved by encrypting the data with public key and decrypting with private key.

Q.4. Describe RSA Cryptosystem. Give suitable example.

Ans. RSA Cryptosystem: This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, **Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair: Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below "

- **Generate the RSA modulus (n)**
- Select two large primes, p and q.
- Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
- **Find Derived Number (e)**
- There must be no common factor for e and (p " 1)(q " 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.
- **Form the public key**
- The pair of numbers (n, e) form the RSA public key and is made public.
- Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.
- **Generate the private key**
- Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
- Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
- This relationship is written mathematically as follows –

$ed = 1 \bmod (p " 1)(q " 1)$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example: An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p " 1)(q " 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing –

$de = 29 \times 5 = 145 = 1 \bmod 72$

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption: Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as "

$C = P^e \bmod n$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get cipher text C "

$C = 10^5 \bmod 91$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair

(n, e) has received a cipher text C.

- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

Plaintext = $C^d \bmod n$

- Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29 –

Plaintext = $82^{29} \bmod 91 = 10$

MODEL TEST PAPER–I
SECOND TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 1.30 hrs. **M.M. : 30**

Note: *Ques no.1 is compulsory and attempt any two from the rest. In all attempt 3 ques.*

Q.1. (a) List three approaches to secure user authentication in distribution environment.

Ans. 1. Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID).

2. Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user.

3. Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

Q.1. (b) What are the five principle services provided by PGP?

Ans. Authentication, confidentiality, compression, e-mail compatibility, and segmentation.

Q.1. (c) What is difference between transport mode and tunnel mode?

Ans. Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Tunnel mode provides protection to the entire IP packet.

Q.1. (d) Give examples of applications of IPSec.

Ans. Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

Q.1. (e) What is a circuit-level gateway?

Ans. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

Q.2. What is Denial of Service Attacks? Compare DoS and DDoS Attack.

Ans. Cyber attacks have become a fact of life, with data breaches of high-profile businesses and organizations making headline news practically on a daily basis. One common type of cyber threat is a denial of service (DoS) that—as its name implies—renders websites and other online resources unavailable to intended users.

DoS threats come in many flavors, with some directly targeting the underlying server infrastructure. Others exploit vulnerabilities in application and communication protocols.

Unlike other kind of cyber attacks, which are typically launched to establish a long-term foothold and hijack sensitive information, denial of service assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legitimate users. In some cases, however, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances (e.g., web application firewalls).

A successful DoS attack is a highly noticeable event impacting the entire online user base. This makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists and anyone else looking to make a point or champion a cause.

DoS assaults often last for days, weeks and even months at a time, making them extremely destructive to any online organization. They can cause loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause you to suffer long-term reputation damage.

DoS vs. DDoS: The differences between DoS and DDoS are substantive and worth noting. In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU).

On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic.

DDoS attacks also differ in the manner of their execution. Broadly speaking, DoS attacks are launched using homebrewed scripts or DoS tools (e.g., Low Orbit Ion Canon), while DDoS attacks are launched from botnets—large clusters of connected devices (e.g., cellphones, PCs or routers) infected with malware that allows remote control by an attacker.

Q.3. (a) What do you mean by Intrusion prevention systems? What are various types of IPS?

Ans. Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.[1] An IPS can also correct Cyclic Redundancy Check (CRC)

errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Intrusion prevention systems can be classified into four different types

1. Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless intrusion prevention systems (WIPS): monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.

4. Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Q.3. (*b*) What do you mean by side channel attack?

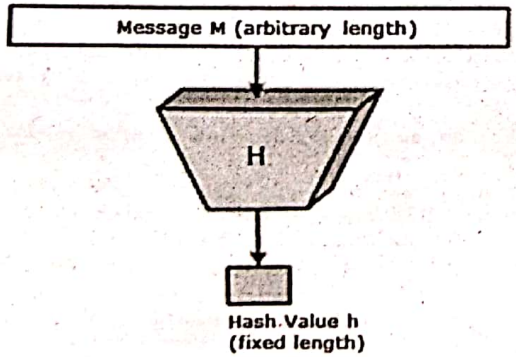
Ans. In cryptography, a **side-channel attack** is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited to break the system. Some side-channel attacks require technical knowledge of the internal operation of the system on which the cryptography is implemented, although others such as differential power analysis are effective as black-box attacks

Q.4. (*a*) Describe Hash functions. Explain various Features of Hash Functions.

Ans. Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function "



Features of Hash Functions

The typical features of hash functions are –

- **Fixed Length Output (Hash Value)**

- Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
- Since a hash is a smaller representation of a larger data, it is also referred to as a digest.
- Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
- Generally for any hash function h with input x, computation of h(x) is a fast operation.
- Computationally hash functions are much faster than a symmetric encryption.

Q.4. (*b*) What is firewall? What are characteristics of firewall?

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

FIREWALL CHARACTERISTICS

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.

3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

MODEL TEST PAPER–I
END TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 3 hrs. **M.M. : 75**

Q.1. (*a*) What are the differences among encoding, encryption and hashing?

Ans. Encoding: Basically encoding is used to protect the integrity of data as it crosses through communication network to keep its original message upon arriving. It is primarily an insecure function because it is easily reversible.

Encryption: Encryption is basically designed for confidentiality and data integrity and reversible only if you have the appropriate key.

Hashing: With hashing the operation is one-way i.e. non-reversible. It takes an input (or ,message) and returns a fixed-size string, which is called the hash value.

Q.1. (*b*) What is Authentication Header and how it provides the protection to IP header?

Ans. Basically Authentication Header protects IP header and provides the complete authenticity to the IP packets.

AH may work in two ways: transport mode and tunnel mode.

In tunnel mode; AH protects the IP header using two IP header layers inner and outer. Inner IP header is used to contain the source and destination addresses, and the outer IP header is used to contain the security gateway information.

Q.1. (*c*) What is Cryptanalysis?

Ans. The art and science of breaking the cipher text is known as cryptanalysis.

Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Q.1. (*d*) What is firewall? What are characteristics of firewall?

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

FIREWALL CHARACTERISTICS

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.

3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Q.2. Describe Playfair Cipher with suitable example.

Ans. In this scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher.

In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

The sender and the receiver deicide on a particular key, say 'tutorials'. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be –

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

Process of Playfair Cipher

• First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message "hide money". It will be written as –

HI DE MO NE YZ

• The rules of encryption are –

• If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)

T U O R I
A L S B C
D E F G H 'H' and 'I' are in same column, hence take letter below them to replace. HI → QC
K M N P Q
V W X Y Z

• If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

T U O R I
A L S B C
D E F G H 'D' and 'E' are in same row, hence take letter to the right of them to replace. DE → EF
K M N P Q
V W X Y Z

• If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

T	U	O	R	I	'M' and 'O' nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row MO-> NU
A	L	S	B	C	
D	E	F	G	H	
K	M	N	P	Q	
V	W	X	Y	Z	

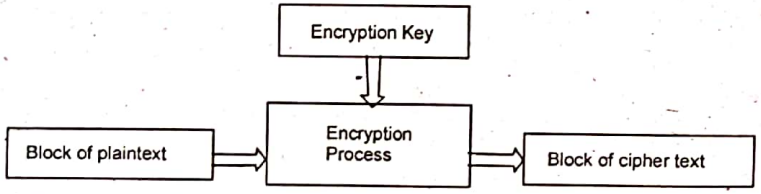
Using these rules, the result of the encryption of 'hide money' with the key of 'tutorials' would be "

QC EF NU MF ZV

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Q.3. (*a*) What is block cipher? What are basic criteria for selecting size of block cipher?

Ans. The basic scheme of a block cipher is depicted as follows "



A block cipher takes a block of plaintext bits and generates a block of cipher text bits, generally of same size. The size of block is fixed in the given scheme. The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends upon the key length.

Block Size: Though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.

•**Avoid very small block size.** – Say a block size is m bits. Then the possible plaintext bits combinations are then 2^m. If the attacker discovers the plain text blocks corresponding to some previously sent cipher text blocks, then the attacker can launch a type of 'dictionary attack' by building up a dictionary of plaintext/cipher text pairs sent using that encryption key. A larger block size makes attack harder as the dictionary needs to be larger.

• **Do not have very large block size.** – With very large block size; the cipher becomes inefficient to operate. Such plaintexts will need to be padded before being encrypted.

• **Multiples of 8 bit.** – A preferred block size is a multiple of 8 as it is easy for implementation as most computer processor handle data in multiple of 8 bits.

Q.3. (*b*) Compare DES and AES.

Ans. DES (Data Encryption Standard) is a rather old way of encrypting data so that the information could not be read by other people who might be intercepting traffic. DES is rather quite old and has since been replaced by a newer and better AES (Advanced Encryption Standard). The replacement was done due to the inherent weaknesses in DES that allowed the encryption to be broken using certain methods of

attack. Common applications of AES, as of the moment, are still impervious to any type of cracking techniques, which makes it a good choice even for top secret information.

The inherent weakness in DES is caused by a couple of things that are already addressed in AES. The first is the very short 56 bit encryption key. The key is like a password that is necessary in order to decrypt the information. A 56 bit has a maximum of 256 combinations, which might seem like a lot but is rather easy for a computer to do a brute force attack on. AES can use a 128, 192, or 256 bit encryption key with 2^128, 2^192, 2^256 combinations respectively. The longer encryption keys make it much harder to break given that the system has no other weaknesses.

Another problem is the small block size used by DES, which is set at 64 bits. In comparison, AES uses a block size that is twice as long at 128 bits. In simple terms, the block size determines how much information you can send before you start having identical blocks, which leak information. People can intercept these blocks and use read the leaked information. For DES with 64 bits, the maximum amount of data that can be transferred with a single encryption key is 32GB; at this point another key needs to be used. With AES, it is at 256 exabytes or 256 billion gigabytes. It is probably safe to say that you can use a single AES encryption key for any application.

In terms of structure, DES uses the Feistel network which divides the block into two halves before going through the encryption steps. AES on the other hand, uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block.

Summary:

DES is really old while AES is relatively new

DES is breakable while AES is still unbreakable

DES uses a much smaller key size compared to AES

DES uses a smaller block size compared to AES

DES uses a balanced Feistel structure while AES uses substitution-permutation.

Q.4. Describe RSA Cryptosystem. Give suitable example.

Ans. RSA Cryptosystem: This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars **Ron Rivest, Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair: Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below –

• **Generate the RSA modulus (n)**

• Select two large primes, p and q.

• Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

• **Find Derived Number (e)**

• Number e must be greater than 1 and less than (p –1)(q – 1).

• There must be no common factor for e and (p – 1)(q –1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

• **Form the public key**

• The pair of numbers (n, e) form the RSA public key and is made public.

• Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

• **Generate the private key**

• Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.

• Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1) (q - 1).

•This relationship is written mathematically as follows –

$ed = 1 \bmod (p - 1)(q - 1)$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

• Let two primes be p = 7 and q = 13. Thus, modulus $n = pq = 7 \times 13 = 91$.

• Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, except for 1.

• The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.

• Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.

• Check that the d calculated is correct by computing –

$de = 29 \times 5 = 145 = 1 \bmod 72$

• Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption: Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

• Suppose the sender wish to send some text message to someone whose public key is (n, e).

• The sender then represents the plaintext as a series of numbers less than n.

• To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as –

$C = P^e \bmod n$

• In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.

• Returning to our Key Generation example with plaintext P = 10, we get cipher text C "

$C = 10^5 \bmod 91$

RSA Decryption:

• The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair

(n, e) has received a cipher text C.

• Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$Plaintext = C^d \bmod n$

• Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29 –

$Plaintext = 82^{29} \bmod 91 = 10$

Q.5. (a) What is IDS. Explain its type.

Ans. Intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

Intrusion detection systems are of two main types, network based (NIDS) and host based (HIDS) intrusion detection systems.

Network Intrusion Detection Systems: Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the designing of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.[4]

Host Intrusion Detection Systems: Host Intrusion Detection Systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

All Intrusion Detection Systems use one of two detection techniques:

Statistical anomaly-based IDS: An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured.[2]

Rule based intrusion detection: It detect intrusion by observing events in the system and applying a set of rules that lead to the decision regarding whether a given pattern of activity is or is not suspicious. It has two types

1. Rule based anomaly detection
2. Rule based penetration detection

Q.5. (b) If we have to generate a hash function then what characteristics are needed in a secure hash function?

Ans. A secure hash function should have the following characteristics:

- The output generated by a hash function should be of a fixed length.
- It should be very easy to find out a hash function for a given message.
- If a hash value is given of a message than it is almost impossible to get that message.
- The two different messages should not have the same hash value; it is against the hash function property.

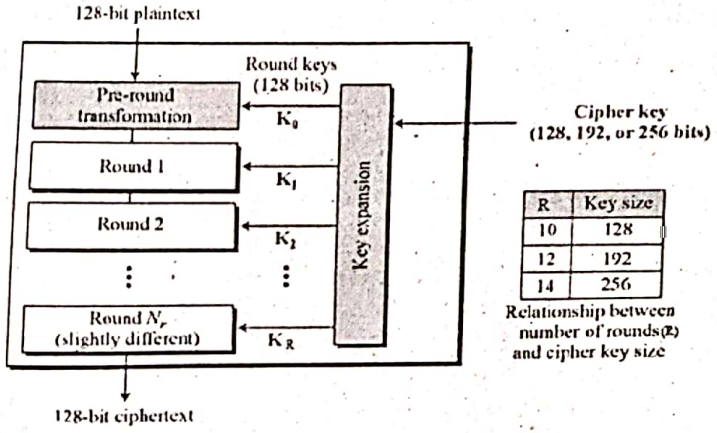
Q.6. Describe Operation of AES.

Ans: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four column and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bits keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit rund key, which is calculated from the original AES key.

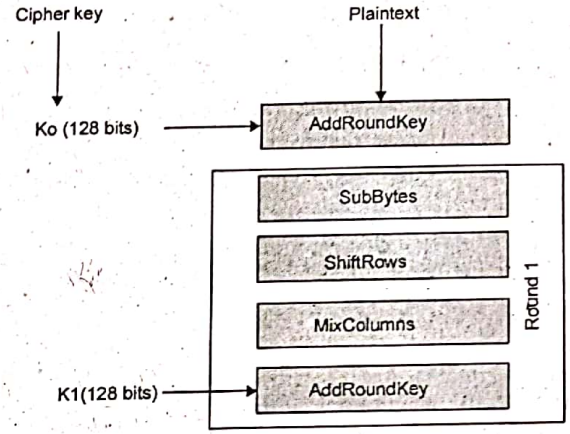
The schematic of AES structure is given in the following illustration.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Encryption Process: Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below.



Byte Substitution (SubBytes): The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add round key: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process: The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

AES Analysis: In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

Q.7. (*a*) Give advantages and disadvantages of transport and tunnel mode of IPSec.

Ans. Transport mode

- Pros
- Provides End to End security
- Lower overhead than tunnel mode
- Larger MTU
- Negotiation of connection-specific selectors is common practice
- Cons
- Requires IPsec to be implemented on the IPS entities
- Greater difficulties with NAT traversal (TCP checksum invalidation)

Tunnel mode

- Pros
- More compatible with existing VPN gateways
- Don't have to implement IPsec on the IPS entity
- Easier to traverse NATs
- Cons
- More overhead
- Smaller MTU
- Secure operation within IPS scenarios would require negotiation of connection-specific selectors – not current practice

Q.7. (*b*) Explain Buffer Flow attack.

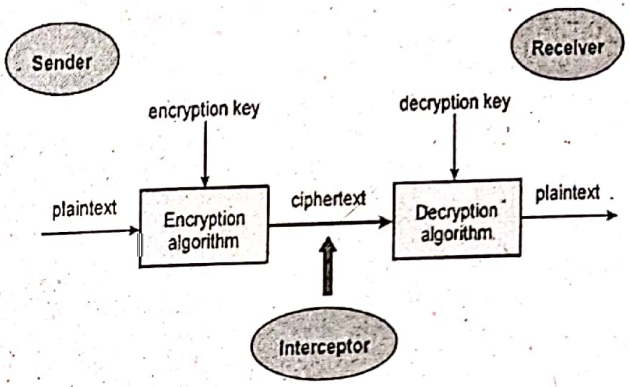
Ans. In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

Q.8. What do you mean by cryptosystem? What are various components of Components of a Cryptosystem?

Ans. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below –



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem: The various components of a basic cryptosystem are as follows –

- **Plaintext:** It is the data to be protected during transmission.
- **Encryption Algorithm:** It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.
- **Cipher text:** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called akey space.

An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems: Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

- Symmetric Key Encryption
- Asymmetric Key Encryption

Q.9. Explain various types of honeypots.

Ans. Pure honeypots are full-fledged production systems. The activities of the attacker are monitored by using a casual tap that has been installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, stealthiness of the defense mechanisms can be ensured by a more controlled mechanism.

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. Example:Honeynet.

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyd.

Malware honeypots: Malware honeypots are used to detect malware by exploiting the known replication and attack vectors of malware. Replication vectors such as USB flash drives can easily be verified for evidence of modifications, either through manual means or utilizing special-purpose honeypots that emulate drives. Malware increasingly is used to search for and steal cryptocurrencies, which provides opportunities for services such as Bitcoin Vigil to create and monitor honeypots by using small amount of money to provide early warning alerts of malware infection.

MODEL TEST PAPER–II
FIRST TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time: 1½ hrs. **M.M. :30**

Note: *Ques no.1 is compulsory and attempt any two from the rest. In all attempt 3 ques.*

Q.1. (a) What is the difference between differential and linear cryptanalysis?

Ans. Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting cipher text provide information that can be used to determine the encryption key. **Linear cryptanalysis** is based on finding linear approximations to describe the transformations performed in a block cipher.

Q.1. (b) What are two problems with the one time pad?

Ans. 1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.

2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Q.1. (c) What is the OSI security architecture?

Ans. The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

Q.1. (d) What is a KDC?

Ans. A key distribution center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

Q.2. (a) What are the principal elements of a public key cryptosystem?

Ans. Plaintext: This is the readable message or data that is fed into the algorithm as input. **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext. Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the encryption algorithm depend on the public or private key that is provided as input. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts. **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Q.2. (b) What is public key certificate.

Ans. A public-key certificate contains a public key and other information, is created by a certificate authority, and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

Q.3. (a) Briefly explain Diffie-Hellman key exchange.

Ans. Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

Q.3. (b) What is an elliptic curve?

Ans. An elliptic curve is one that is described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, cubic equations for elliptic curves take the form

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where a, b, c, d, and e are real numbers and x and y take on values in the real numbers

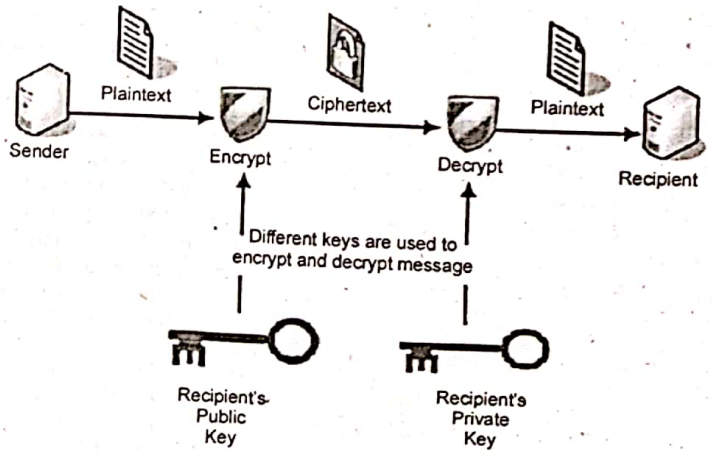
Q.4. Describe public key cryptography.

Ans. 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.

MODEL TEST PAPER–II
SECOND TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 1½ hrs. **M.M. : 30**

Note: *Ques no.1 is compulsory and attempt any two from the rest. In all attempt 3 ques.*

Q.1. (a) What types of attacks are addressed by message authentication?

Ans. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient. **Content modification:** Changes to the contents of a message, including insertion, deletion, transposition, and modification. **Sequence modification:** Any modification to a sequence of messages between parties, including insertion, deletion, and reordering. **Timing modification:** Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

Q.1. (b) What services are provided by IPSec?

Ans. Access control; connectionless integrity; data origin authentication; rejection of replayed packets (a form of partial sequence integrity); confidentiality (encryption); and limited traffic flow confidentiality.

Q.1. (c) What is a reply attack.

Ans. A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

Q.1. (d) What is the difference between a packet filtering router and stateful inspection packet filter?

Ans. A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context. A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory

Q.2. (a) What is a DDoS.

Ans. A denial of service (DoS) attack 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 is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. 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 target.

Q.2. (b) What is a circuit- level gateway?

Ans. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

Q.3. (a) What are benefits that can be provided by an IDS.

Ans. The benefits that can be provided by an IDS are:

1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.

2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.

3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Q.3. (b) Explain various types of honeypots.

Ans. Pure honeypots are full-fledged production systems. The activities of the attacker are monitored by using a casual tap that has been installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, stealthiness of the defense mechanisms can be ensured by a more controlled mechanism.

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. Example:Honeynet.

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyd.

Malware honeypots: Malware honeypots are used to detect malware by exploiting the known replication and attack vectors of malware. Replication vectors such as USB flash drives can easily be verified for evidence of modifications, either through manual means or utilizing special-purpose honeypots that emulate drives. Malware increasingly is used to search for and steal cryptocurrencies, which provides opportunities for services such as Bitcoin Vigil to create and monitor honeypots by using small amount of money to provide early warning alerts of malware infection.

Q.4. What is IPS? What are various applications of IPS.

Ans. Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/ or system activities for malicious activity. The main functions of intrusion prevention

systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.[2]:273[3]:289 More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.[4] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Intrusion prevention systems can be classified into four different types:

1. Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless intrusion prevention systems (WIPS): monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.

4. Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

MODEL TEST PAPER–II
END TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 3 hrs. **M.M. : 75**

Q.1. (*a*) Compare monoalphabetic substitution cipher and polyalphabetic substitution cipher.

Ans. A monoalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet. A polyalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

Q.1. (*b*) What services provided by IPSec?

Ans. Access control; connectionless integrity; data origin authentication; rejection of replayed packets (a form of partial sequence integrity); confidentiality (encryption); and limited traffic flow confidentiality

Q.1.(*c*) What is the difference between Statistical anomaly detection and Rule-Based Detection.

Ans. Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior. **Rule-Based Detection** involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

Q.1. (*d*) What is MIME?

Ans. MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.

Q.1. (*e*) Describe stream cipher and block cipher.

Ans. A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Block cipher is an algorithm that converts a block of plaintext into ciphertext. It takes two inputs, n bits of fixed length of blocks and a secret key and output is n bits of ciphertext. Stream cipher is symmetric encryption algorithm with takes one bit or one byte as input and encrypted with a secret key called keystream.

Q.2. Describe Differential Cryptanalysis and Linear Cryptanalysis for DES?

Ans. Differential Cryptanalysis: However, if one is fortunate enough to have a large quantity of corresponding plaintext and ciphertext blocks for a particular unknown key, a technique called differential cryptanalysis, developed by Eli Biham and Adi Shamir, is available to obtain clues about some bits of the key, thereby shortening an exhaustive search.

After two rounds of DES, knowing both the input and output, it is trivial to determine the two subkeys used, since the outputs of both f-functions are known. For each S-box,

there are four possible inputs to produce the known output. Since each subkey is 48 bits long, but the key is only 56 bits long, finding which of the four possibilities is true for each group of six bits in the subkeys is a bit like solving a crossword puzzle.

Once the number of rounds increases to four, the problem becomes much harder. However, it is still true that the output depends on the input and the key. For a limited number of rounds, it is inevitable, without the need for any flaws in the S-boxes, that there will be some cases where a bit or a combination of bits in the output will have some correlation with a simple combination of some input bits and some key bits. Ideally, that correlation should be absolute with respect to the key bits, since there is only one key to solve for, but it can be probabilistic with respect to the input and output bits, since there need to be many pairs to test.

As the number of rounds increases, though, the simple correlations disappear. Differential cryptanalysis represents an approach to finding more subtle correlations.

Instead of saying "if this bit is 1 in the input, then that bit will be 0 (or 1) in the output", we say "changing this bit in the input changes (or does not change) that bit in the output".

Linear Cryptanalysis: Linear cryptanalysis, invented by Mitsuru Matsui, is a different, but related technique. Instead of looking for isolated points at which a block cipher behaves like something simpler, it involves trying to create a simpler approximation to the block cipher as a whole.

For a great many plaintext-ciphertext pairs, the key that would produce that pair from the simplified cipher is found, and key bits which tend to be favored are likely to have the value of the corresponding bit of the key for the real cipher. The principle is a bit like the summation of many one-dimensional scans to produce a two-dimensional slice through an object in computer-assisted tomography.

Q.3. What is firewall? Explain different types of firewall.

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

There are three main classes of firewalls: packet filters, application and circuit gateways (proxies), and stateful inspection (or smart filter) firewalls.

Proxy Servers: A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy. All communication between a user and the actual server occurs through the proxy server. Thus, a proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions. Proxy servers can operate at either the application layer or the transport layer. Thus, there are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

Application Gateways: An application gateway is a proxy server that provides access control at the application layer. It acts as an application-layer gateway between the protected network and the untrusted network. Because it operates at the application layer, it is able to examine traffic in detail and, therefore, is considered the most secure type of firewall. It can prevent certain applications, such as FTP, from entering the protected network. It can also log all network activities according to applications for both accounting and security audit purposes. Application gateways can also hide information. Since all requests for services in the protected network pass through the application gateway, it can provide network address translation (or IP address hiding) functionality and conceal IP addresses in the protected network from the Internet by

replacing the IP address of every outbound packet (that is, packets going from the protected network to the Internet) with its own IP address. Network address translation also permits unregistered IP addresses to be freely used in the protected network because the gateway will map them to its own IP address when the users attempt to communicate with the outside world.

Circuit-Level Gateways: A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied. A circuit level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders. Unlike a circuit-level gateway, an application gateway can differentiate the applications that need to be blocked from those that can be allowed to pass through the gateway.

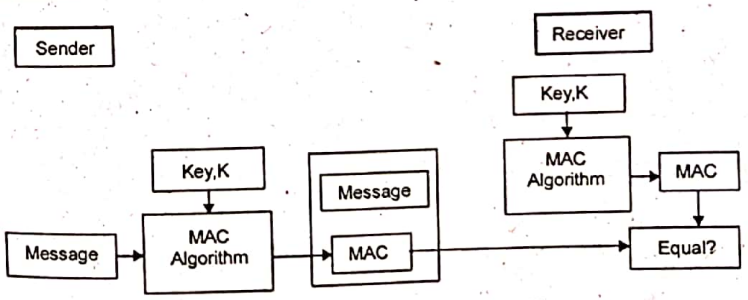
Stateful Packet Filters: Although the application gateway provides the best security among the preceding firewalls, its intensive processing requirement slows down network performance. A stateful packet filtering gateway attempts to provide tight security without compromising performance. Unlike the application gateway, it checks the data that passes through at the network layer but does not process it. The firewall maintains state information for each session, where session states include a combination of communication phase and the endpoint application state. When a stateful packet filtering gateway receives a data packet, it checks the packet against the known state of the session. If the packet deviates from the expected session state, the gateway blocks the rest of the session.

Q.4. What do you mean by Message Authentication Code (MAC). Explain Limitations of MAC.

Ans. MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.

Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

The process of using MAC for authentication is depicted in the following illustration –



Let us now try to understand the entire process in detail –

• The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.

• Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output. The major difference between hash and MAC is that MAC uses secret key during the compression.

•The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.

• On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.

• The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.

• If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.

Limitations of MAC: There are two major limitations of MAC, both due to its symmetric nature of operation –

• **Establishment of Shared Secret.**

• It can provide message authentication among pre-decided legitimate users who have shared key.

• This requires establishment of shared secret prior to use of MAC.

• **Inability to Provide Non-Repudiation**

• Non-repudiation is the assurance that a message originator cannot deny any previously sent messages and commitments or actions.

• MAC technique does not provide a non-repudiation service. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender.

• Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

Q.5. Describe OSI Security Architecture in detail.

Ans. To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for computer and network security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

ITU-T4 Recommendation X.800, Security Architecture for OSI, defines such a systematic approach.5 The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts that this book deals with.The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

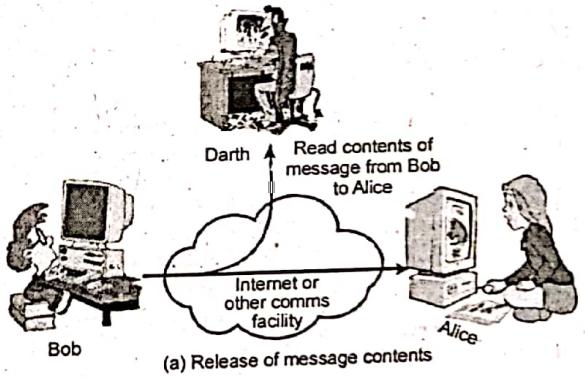
• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

SECURITY ATTACKS:

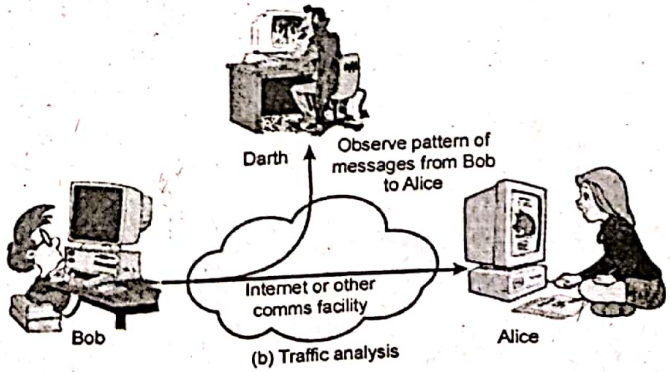
A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.

The goal of the opponent is to obtain information that is being transmitted.Two types of passive attacks are the release of message contents and traffic analysis.



(a) Release of message contents



(b) Traffic analysis

The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

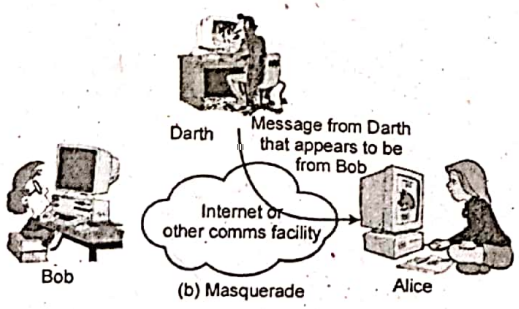
This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A masquerade takes place when one entity pretends to be a different entity (Figure (a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

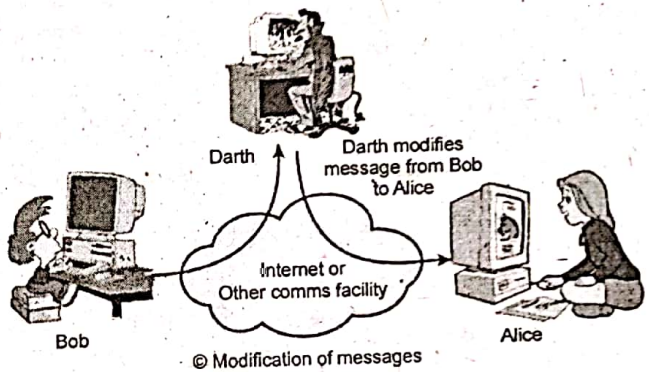
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure (b). Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure (c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts.–



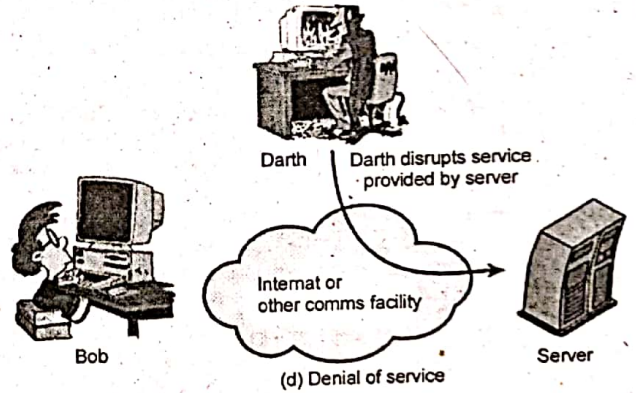
(b) Masquerade

The denial of service prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the

security audit service). Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.



© Modification of messages



(d) Denial of service

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. If the detection has a deterrent effect, it also may contribute to prevention.

Q.6. What is Elliptic curve cryptography. What are various cryptographic schemes?

Ans: 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.

For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation

$y^2 = x^3 + ax + b$, {\ along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.)

This set together with the group operation of elliptic curves is an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

$Div^0(E) \rightarrow Pic^0(E) = E$

Cryptographic schemes: As is the case for other popular public key cryptosystems, no mathematical proof of security has been published for ECC as of 2009.

Several discrete logarithm-based protocols have been adapted to elliptic curves, replacing the group an elliptic curve:

- The elliptic curve Diffie–Hellman (ECDH) key agreement scheme is based on the Diffie–Hellman scheme,
- The Elliptic Curve Integrated Encryption Scheme (ECIES), also known as Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme,
- The Elliptic Curve Digital Signature Algorithm (ECDSA) is based on the Digital Signature Algorithm,
- The Edwards-curve Digital Signature Algorithm (EdDSA) is based on Schnorr signature and uses twisted Edwards curves,
- The ECMQV key agreement scheme is based on the MQV key agreement scheme,
- The ECQV implicit certificate scheme.

At the RSA Conference 2005, the National Security Agency (NSA) announced Suite B which exclusively uses ECC for digital signature generation and key exchange. The suite is intended to protect both classified and unclassified national security systems and information.

Recently, a large number of cryptographic primitives based on bilinear mappings on various elliptic curve groups, such as the Weil and Tate pairings, have been introduced. Schemes based on these primitives provide efficient identity-based encryption as well as pairing-based signatures, sign encryption, key agreement, and proxy re-encryption.

Application: Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

Q.7. (*a*) What are various block cipher schemes?

Ans. There is a vast number of block ciphers schemes that are in use. Many of them are publically known. Most popular and prominent block ciphers are listed below.

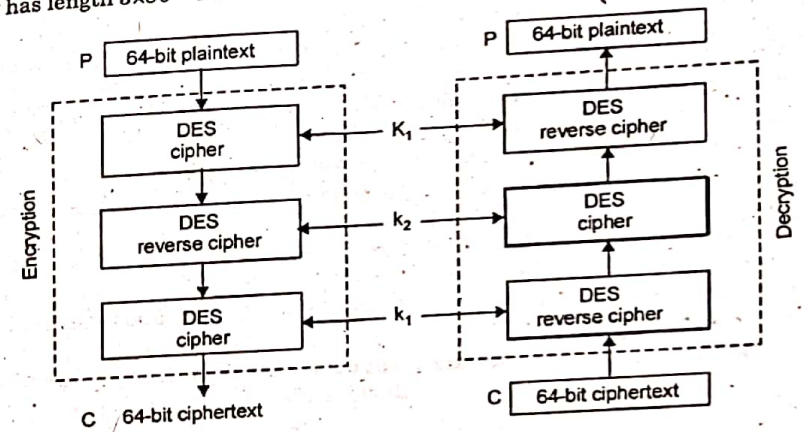
- **Digital Encryption Standard (DES)** – The popular block cipher of the 1990s. It is now considered as a 'broken' block cipher, due primarily to its small key size.
- **Triple DES** – It is a variant scheme based on repeated DES applications. It is still a respected block ciphers but inefficient compared to the new faster block ciphers available.
- **Advanced Encryption Standard (AES)** – It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.
- **IDEA** – It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early versions of Pretty Good Privacy (PGP) protocol. The use of IDEA scheme has a restricted adoption due to patent issues.

- **Twofish** – This scheme of block cipher uses block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.

Serpent – A block cipher with a block size of 128 bits and key lengths of 128, 192, or 256 bits, which was also an AES competition finalist. It is a slower but has more secure design than other block cipher.

Q.7. (*b*) Describe Triple DES

Ans. Before using 3TDES, users first generates and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows



- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K_3 is replaced by K_1. In other words, user encrypts plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

Q.8. (*a*) What are various security services of cryptography?

Ans. Security Services: X.800 defines a security service as a service provided by a protocol layer of communication open system, which ensures adequate security of the system or of data transfers.

X.800 divides these services into five categories and fourteen specific services.

(1) Authentication

(2) Access Control

(3) Data confidentially or Privacy

(4) Data integrity

(5) Non- reputation

(1) Authentication: Corroboration of the identity of an entity. Two specific authentication services are defined in the standard.

• **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.

• **Data Origin Authentication:** In connection less transfer, provides assurance that the source of received data is as claimed.

(2) Access Control: In the context of network security, access control is the ability to limit and control the access to host system and application via communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

(3) Data Confidentially Or Privacy: The protection of data from unauthorized disclosure. Four specific services of confidentially are

• **Connection Confidentially:** The protection of all user data on a connection.

• **Connectionless Confidentially:** The protection of all user data in a single data book.

• **Selective Field Confidentially:** The confidentially of selected fields within the user data on a connection or in a single data book.

• **Traffic - flow confidentiality:** The protection of information that might be derived from observation of traffic flow.

(4) Data Integrity: The assurance that data received is exactly as sent by an authorized entity. That means no modification insertion, deletion or replay. There are five types of specific services.

• **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or reply-of any data within entries data sequence, with recovery attempted.

• **Connection Integrity Without Recovery:** As above, but provides only detection without recovery.

• **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.

• **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

• **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of a whether the selected fields have been modified.

(5) Non-repudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. There are two types of specific services in Non-repudiation.

• **Non-repudiation, origin:** Proof that the specific parties sent the massage.

• **Non-repudiation, Destination:** Proofs that the massage was receive by the specific parties.

Q.8. (*b*) Describe Caesar Cipher with suitable example.

Ans. It is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext. It is a simplest form of substitution cipher scheme.

This cryptosystem is generally referred to as the Shift Cipher. The concept is to replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25.

For this type of scheme, both sender and receiver agree on a 'secret shift number' for shifting the alphabet. This number which is between 0 and 25 becomes the key of encryption.

The name 'Caesar Cipher' is occasionally used to describe the Shift Cipher when the 'shift of three' is used.

Process of Shift Cipher:

•In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.

• The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext 'tutorial' is encrypted to the ciphertext 'WXWRULDO'. Here is the ciphertext alphabet for a Shift of 3 "

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

• On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.

•He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence the ciphertext 'WXWRULDO' is decrypted to 'tutorial'. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown below –

Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Q.9. (*a*) What do you mean by linear cryptanalysis?

Ans: In cryptography, linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

There are two parts to linear cryptanalysis. The first is to construct linear equations relating plaintext, ciphertext and key bits that have a high bias; that is, whose

probabilities of holding (over the space of all possible values of their variables) are as close as possible to 0 or 1. The second is to use these linear equations in conjunction with known plaintext-ciphertext pairs to derive key bits.

Constructing linear equations: For the purposes of linear cryptanalysis, a linear equation expresses the equality of two expressions which consist of binary variables combined with the exclusive-or (XOR) operation. For example, the following equation, from a hypothetical cipher, states the XOR sum of the first and third plaintext bits (as in a block cipher's block) and the first ciphertext bit is equal to the second bit of the key.

In an ideal cipher, any linear equation relating plaintext, ciphertext and key bits would hold with probability 1/2. Since the equations dealt with in linear cryptanalysis will vary in probability, they are more accurately referred to as linear *approximations*.

The procedure for constructing approximations is different for each cipher. In the most basic type of block cipher, a substitution-permutation network, analysis is concentrated primarily on the S-boxes, the only nonlinear part of the cipher (i.e. the operation of an S-box cannot be encoded in a linear equation). For small enough S-boxes, it is possible to enumerate every possible linear equation relating the S-box's input and output bits, calculate their biases and choose the best ones. Linear approximations for S-boxes then must be combined with the cipher's other actions, such as permutation and key mixing, to arrive at linear approximations for the entire cipher. The piling-up lemma is a useful tool for this combination step. There are also techniques for iteratively improving linear approximations.

Q.9. (*b*) Write short notes on Cryptography Primitives.

Ans. Cryptography Primitives: Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services "

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

The following table shows the primitives that can achieve a particular security service on their own.

Primitives Service	Encryption	Hash Function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non Reputation	No	No	Sometimes	Yes

SEVENTH SEMESTER [B.TECH.]
FIRST TERM EXAMINATION [SEPT. 2016]
CRYPTOGRAPHY AND NETWORK SECURITY
(ETIT–403)

Time : 1.5 hrs. **M.M. : 30**

Note: ***Q. No. 1 is compulsory. Attempt any two more questions from the rest.***

Q.1. (*a*) What do you mean by differential cryptanalysis? **(2)**

Ans: Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key. Differential cryptanalysis is usually a chosen plaintext attack, meaning that the attacker must be able to obtain cipher texts for some set of plaintexts of his choosing. There are, however, extensions that would allow a known plaintext or even a cipher text-only attack. The basic method uses pairs of plaintext related by a constant difference; difference can be defined in several ways, but the exclusive OR (XOR) operation is usual. The attacker then computes the differences of the corresponding cipher texts, hoping to detect statistical patterns in their distribution. The resulting pair of differences is called a differential. Their statistical properties depend upon the nature of the S-boxes used for encryption, so the attacker analyses differentials (Δ_X, Δ_Y), where $\Delta_Y = S(X \oplus \Delta_X) \oplus S(X)$ and $\oplus$ denotes exclusive or) for each such S-box S. In the basic attack, one particular cipher text difference is expected to be especially frequent; in this way, the cipher can be distinguished from random. More sophisticated variations allow the key to be recovered faster than exhaustive search.

Since differential cryptanalysis became public knowledge, it has become a basic concern of cipher designers. New designs are expected to be accompanied by evidence that the algorithm is resistant to this attack, and many, including the Advanced Encryption Standard, have been proven secure against the attack.

Q.1. (*b*) What is message authentication? **(2)**

Ans: In cryptography, a message authentication code (MAC) is a short piece of information used toauthenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed (sometimes known as a tag).

Message authentication is typically achieved by using message authentication codes (MACs), authenticated encryption (AE) or digital signatures.

Some cryptographers distinguish between "message authentication without secrecy" systems — which allow the intended receiver to verify the source of the message, but don't bother hiding the plaintext contents of the message from authenticated encryption systems. A few cryptographers have researched subliminal channel systems that send messages that appear to use a "message authentication without secrecy" system, but in fact also transmit a secret message.

Q.1. (c) What is hash function? (2)

Ans: Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values.

Q.1. (d) Explain triple DES. (2)

Ans: Before using 3TDES, users first generates and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits.

The encryption-decryption process is as follows–

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Q.1. (e) What do you mean by software forensics? (2)

Ans: Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Q.2. (a) What are various Security Services of Cryptography? (5)

Ans: X.800 defines a security service as a service provided by a protocol layer of communication open system, which ensures adequate security of the system or of data transfers.

X.800 divides these services into five categories and fourteen specific services.

(1) Authentication

(2) Access Control

(3) Data confidentially or Privacy

(4) Data integrity

(5) Non- reputation

(1) Authentication: - Corroboration of the identity of an entity. Two specific authentication services are defined in the standard.

- **Peer Entity Authentication:** - Used in association with a logical connection to provide confidence in the identity of the entities connected.
- **Data Origin Authentication:** - In connection less transfer, provides assurance that the source of received data is as claimed.

(2) Access Control: - In the context of network security, access control is the ability to limit and control the access to host system and application via communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

(3) Data Confidentially Or Privacy: - The protection of data from unauthorized disclosure. Four specific services of confidentially are

- **Connection Confidentially:** - The protection of all user data on a connection.
- **Connectionless Confidentially:** - The protection of all user data in a single data book.
- **Selective Field Confidentially:** - The confidentially of selected fields within the user data on a connection or in a single data book.
- **Traffic - flow confidentiality:** - The protection of information that might be derived from observation of traffic flow.

(4) Data Integrity: - The assurance that data received is exactly as sent by an authorized entity. That means no modification insertion, deletion or replay. There are five types of specific services.

- **Connection Integrity with Recovery:** - Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or reply-of any data within entries data sequence, with recovery attempted.
- **Connection Integrity Without Recovery:** - As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity:** - Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.
- **Connectionless Integrity:** - Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity:** - Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of a whether the selected fields have been modified.

(5) Non-repudiation: -

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. There are two types of specific services in Non-repudiation.

- **Non-repudiation, origin:** - Proof that the specific parties sent the massage.
- **Non-repudiation, Destination:** - Proofs that the massage was receive by the specific parties.

Q.2. (b) What is the difference between a cryptographer and a cryptanalyst? (5)

Ans: The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

A Cryptographer develops algorithms, ciphers and security systems to encrypt sensitive information. Cryptographers help protect confidential information and may

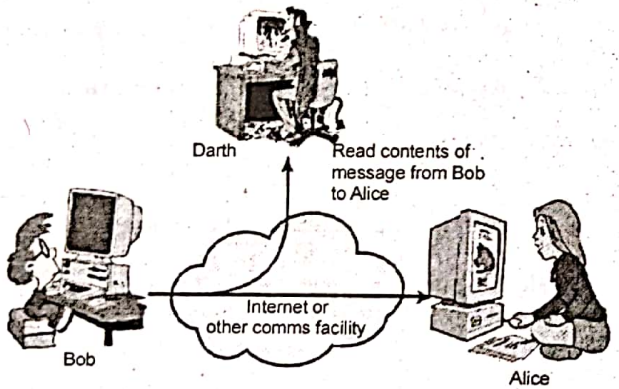
work to protect military, financial or political data. They may be involved in encrypting information or decrypting information. Cryptographers are required to pass a background check and possess at least a bachelor's degree in computer science, mathematics, or a related field.

Q.3. (a) Differentiate active attacks and passive attacks. **(5)**

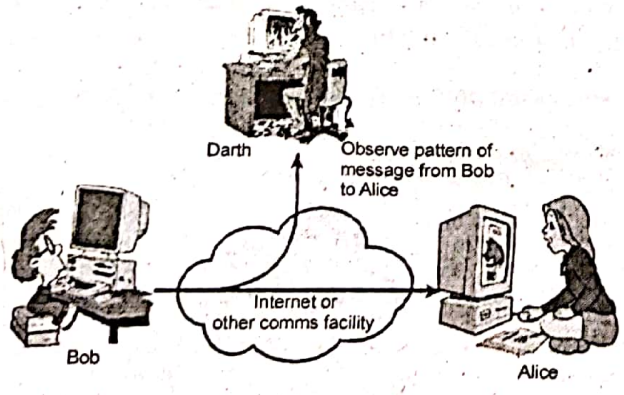
Ans: A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. Anactive attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.Two types of passive attacks are the release of message contents and traffic analysis



(a) Release of message contents



(b) Traffic analysis

The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent still might be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A masquerade takes place when one entity pretends to be a different entity Figure. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

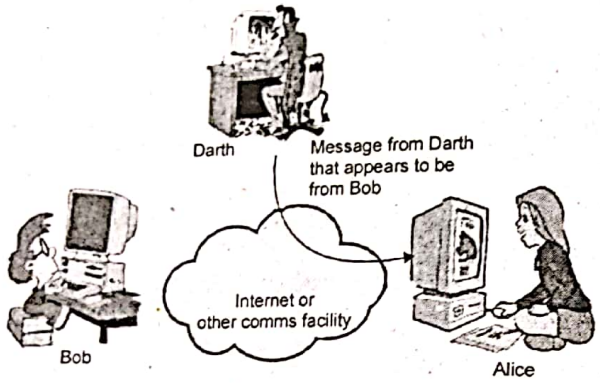
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure)

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

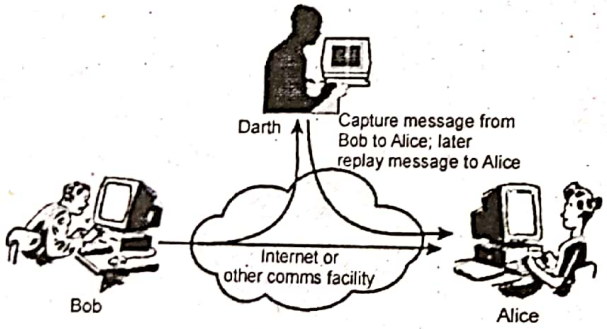
The denial of service prevents or inhibits the normal use or management of communications facilities (Figure). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite characteristics of passive attacks.

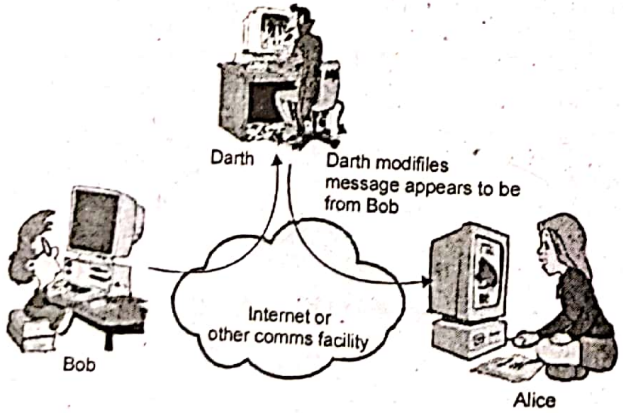
Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it also may contribute to prevention.



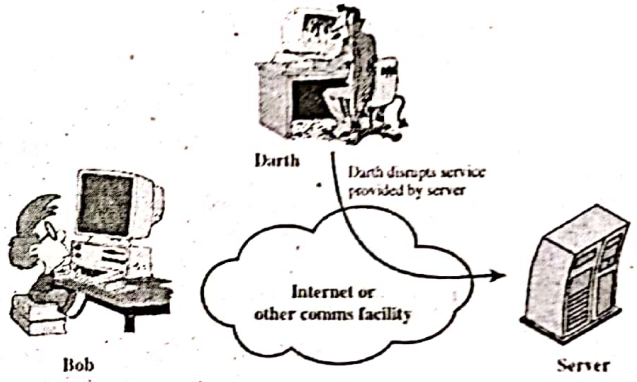
(a) Masquerade



(b) Replay



(c) Masquerade



(d) Denial of service

Q.3. (*b*) What are the differences between symmetric and asymmetric encryption algorithm. (5)

Ans: Symmetric is one way, and asymmetric is a two way function. Symmetric uses one key to both encrypt and decrypt, and asymmetric uses one key to encrypt and another to decrypt. Symmetric encryption is strong and asymmetric encryption is weak. Symmetric does not use a key, and asymmetric makes use of keys. Symmetric Encryption uses a single secret key that needs to be shared among the people who needs to receive the message while Asymmetric encryption uses a pair of public key, and a private key to encrypt and decrypt messages when communicating.

- Symmetric Encryption is an age old technique while Asymmetric Encryption is relatively new.
- Asymmetric Encryption was introduced to complement the inherent problem of the need to share the key in symmetric encryption model eliminating the need to share the key by using a pair of public-private keys.

Q.4. (*a*) Describe RSA algorithm. Give suitable example. (7)

Ans: This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below–

- Generate the RSA modulus (n)
  - o Select two large primes, p and q.
  - o Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

- Find Derived Number (e)
  - o Number e must be greater than 1 and less than (p – 1)(q – 1).
  - o There must be no common factor for e and (p – 1)(q – 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.
- Form the public key
  - o The pair of numbers (n, e) form the RSA public key and is made public.
  - o Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.
- Generate the private key
  - o Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - o Number d is the inverse of e modulo (p – 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
  - o This relationship is written mathematically as follows –

ed = 1 mod (p – 1)(q – 1)

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be $p = 7$ and $q = 13$. Thus, modulus $n = pq = 7 \times 13 = 91$.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, except for 1.
- The pair of numbers $(n, e) = (91, 5)$ forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input $p = 7$, $q = 13$, and $e = 5$ to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing–

de = 29 × 5 = 145 = 1 mod 72

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as–

$C = P^e \bmod n$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get cipher text C

$C = 10^5 \bmod 91$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

Plaintext = $C^d \bmod n$

- Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29.

Plaintext = $82^{29} \bmod 91 = 10$

Q.4. (b) Compare DES and AES. **(3)**

Ans: DES is a symmetric block cipher (shared secret key), with a key length of 56-bits. AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

Comparing DES and AES

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

SEVENTH SEMESTER [B.TECH.]
END TERM EXAMINATION [DEC. 2016]
CRYPTOGRAPHY AND NETWORK SECURITY
(ETIT–403)

Time : 3 hrs. **M.M. : 75**

Note: *Q. No. 1 is compulsory. Attempt five more questions from the rest.*

Q.1. Attempt any 7 out of 8 parts: **(7×5=35)**

(a) What is Cyber Forensics? Is ethical Hacking part of the Digital Hacking? Justify your answer.

Ans. Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence - for civil purposes or, in many cases, to prove and legally prosecute cyber crime. With technology changing and evolving on a daily basis, cyber forensic professionals must continually keep pace and educate themselves on the new techniques to collect this data. They are tasked with being an expert in forensic techniques and procedures, standards of practice, and legal and ethical principles that will assure the accuracy, completeness and reliability of the digital evidence.

Ethical hacking is key to strengthening network security, and it's one of the most desired stills for any IT security professional. Ethical hackers coming from this area of expertise also have knowledge in problem-solving strategies for security breaches, and can collect and analyze data to monitor and interpret weaknesses.

Q.1. (b) Describe the Security challenges in Wireless Networks/ Mobile Devices?

Ans. There are following Security challenges in Wireless Networks/ Mobile Devices.

- Limited memory and storage
- Limited power
- Unreliability of communication
- Deployment and immense scale
- Operation unattended

There are following security challenges in wireless networks/ Mobile devices.

- **Limited memory and storage:** Networks of low-power communicating devices suffer from a small storage memory space. One of the challenges is to guarantee robust data storage in WSNs and eventually collecting data from temporary storage locations to the backend databases.
- **Limited power:** More scalable for large WSNs having limited power resources. Complex analyses of massive amount of sensor data demand high processing power and large storage memory space. These constraints impose forwarding the sensor data from the WSN to powerful backend machines, where they are stored and processed for different analyses
- **Unreliability of communication:** Unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The network protocol consists of routing that is the selection of paths in the WSN along which messages are sent. The transport layer provides end-to-end communication services and the application layer consists of user service.

- **Deployment and immense scale:** In networks where beacon deployment is sparse enough that location estimations cannot be made directly by each sensor in the network. Large gains in network lifetime can be seen when considering the importance of a node to the overall sensing task when making routing decisions if the sensor deployment is such that there is a high variation in the density in different subregions of the environment. While providing security to small to large networks here is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiently.
- **Operation unattended:** Due to the lack of data storage and power sensor networks introduce severe resource constraints. These are the obstacles to the implementation of traditional computer security techniques in a WSN. Security defenses harder in WSN due to the unreliable communication channel and unattended operation. As a result these networks require some unique security policies.

Q.1. (c) What is the difference between Symmetric and Asymmetric Cryptgraphy.

Ans. •Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.

- Symmetric encryption is an old technique while asymmetric encryption is relatively new.
- Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
- Asymmetric encryption takes relatively more time than the symmetric encryption.

Q.1. (d) Differentiate between Additive Cipher and Affine Cipher with examples.

Ans. Additive Ciphers

The simplest code is an additive cipher. Each coded letter is simply shifted a certain number of spaces from the plaintext letter. The number of spaces the letter has been shifted is called the key.

Mathematically, any additive cipher can be expressed by the following equation:

$c = (p + a) \bmod 26$

where p is the position of the plaintext letter, a is the key, and c is the position of the resulting ciphertext letter.

Affine cipher

The affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function $(ax + b) \bmod 26$, where b is the magnitude of the shift.

Q.1. (e) What is the Playfair Cipher?

Ans. In this scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher.

In playfair cipher, initially a key table is created. The key table is a 5x5 grid o alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabet must be unique and one letter of the alphabet (usually J) is omitted from the table as w need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I

The sender and the receiver deicide on a particular key, say 'tutorials'. In a key table the first characters (going left to right) in the table is the phrase, excluding the duplicat letters. The rest of the table will be filled with the remaining letters of the alphabet, i natural order. The key table works out to be–

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

Process of Playfair Cipher

- First, a plaintext message is split into pairs of two letters (digraphs). If there i an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt th message "hide money". It will be written as

HI DE MO NE YZ

- The rules of encryption are

o If both the letters are in the same column, take the letter below each one (goin back to the top if at the bottom)

T	U	O	R	I	
A	L	S	B	C	
D	E	F	G	H	'H' and 'I' are in same column, hence take lette below them to replace. HI → QC
K	M	N	P	Q	
V	W	X	Y	Z	

• If both letters are in the same row, take the letter to the right of each one (goin back to the left if at the farthest right)

T	U	O	R	I	'D' and 'E' are in same row, hence take letter to the right of them to replace. DE → EF
A	L	S	B	C	
D	E	F	G	H	
K	M	N	P	Q	
V	W	X	Y	Z	

• If neither of the preceding two rules are true, form a rectangle with the two letter and take the letters on the horizontal opposite corner of the rectangle.

T	U	O	R	I	'M' and 'O' nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row MO-> NU .
A	L	S	B	C	
D	E	F	G	H	
K	M	N	P	Q	
V	W	X	Y	Z	

Using these rules, the result of the encryption of 'hide money' with the key of 'tutorials' would be –

QC EF NU MF ZV

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Q.1. (*f*) What is Security System Development and life cycle? Describe it with example.

Ans. Most organizations have a well-oiled machine with the sole purpose to create, release, and maintain functional software. However, the increasing concerns and business risks associated with insecure software have brought increased attention to the need to integrate security into the development process. Implementing a proper Secure Software Development Life Cycle (SDLC) is important now more than ever.Generally speaking, an Secure SDLC is set up by adding security-related activities to an existing development process. Small changes in the software development life cycle can substantially improve security without breaking the bank or the project schedule.

For example, writing security requirements alongside the collection of functional requirements, or performing an architecture risk analysis during the design phase of the SDLC.

Q.1. (*g*) Use Vigenere Cipher to encrypt the message "Information Security" using the 3 character word "Ant."

Ans. Vigenere Cipher:

Keyword: ANT ANTANTANTANTANT A

Plaintext: INF ORM ATI ONS ECU RIT Y

Ciphertext: IAY OEF AGB OAL EPN RVM Y

Q.1. (*h*) Assume that Ram and Shyam agreed to use an autokey cipher with initial key value $k = 12$. Now Ram wants to send Shyam the message "GGSIPU DELHI." Enciphering is done character by character. What would be the Ciphertext for the same.

Ans. Given plain text= GGSIPU DELHI

Plaintext:	G	G	S	I	P	U	D	E	L	H	I
P's Values:	06	06	18	08	15	20	03	04	11	07	08
Key stream:	12	06	06	18	08	15	20	03	04	11	07
C's Values:	18	12	24	00	23	09	23	07	15	18	15
Ciphertext:	S	M	Y	A	X	J	X	H	P	S	P

Q.2. Define Crypt Analysis? How is it different from the Network Attacks? Categorize and describe the different type of attacks that are handled as part of Network Security. (10)

Ans. Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

In computer and computer **networks** an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Different types of Network Attacks:

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

Eavesdropping: In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Data Modification: After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

Identity Spoofing (IP Address Spoofing): Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

Password-Based Attacks: A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

Denial-of-Service Attack: Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-Middle Attack: As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack: A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Sniffer Attack: A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Application-Layer Attack: An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

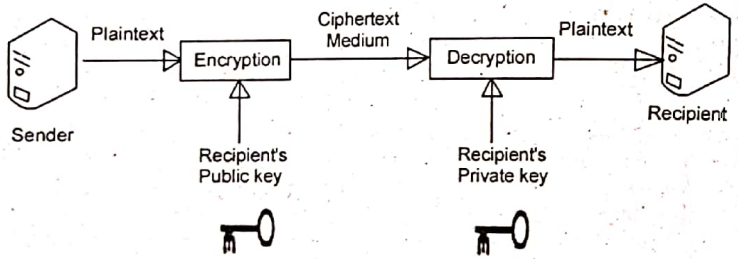
- Read, add, delete, or modify your data or operating system.

- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

Q.3. Differentiate between Public and Private key Cryptography. Taking an example of any algorithm of your choice, (example: DES and RSA etc). **(10)**

Ans. Difference between public and private key Cryptography:

There are two basic types of encryptions viz. symmetric key and asymmetric key. The symmetric key encryption uses same key at sender and receipient. The asymmetric key encryption uses different keys at sender and receipient machines.



Figure

The figure depicts simple encryption and decryption system.

• As shown transmit side converts plain text into encrypted text before transmission over the medium. The transmit side uses public key shared by receipient.

• As shown receive side converts encrypted text back to the plain text form. The receive side uses private key as generated by receipient itself.

As this is asymmetric encryption type, public key transported over the medium can not be used to decrypt the encrypted message nor it can be used to derive private key.

Examples of RSA:

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below "

- **Generate the RSA modulus (n)**
  - o Select two large primes, p and q.
  - o Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
- **Find Derived Number (e)**
  - o Number e must be greater than 1 and less than (p – 1)(q – 1).
  - o There must be no common factor for e and $(p-1)(q-1)$ except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

- **Form the public key**
  - o The pair of numbers (n, e) form the RSA public key and is made public.
  - o Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.
- **Generate the private key**
  - o Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - o Number d is the inverse of e modulo $(p-1)(q-1)$. This means that d is the number less than $(p-1)(q-1)$ such that when multiplied by e, it is equal to 1 modulo $(p-1)(q-1)$.
  - o This relationship is written mathematically as follows –

    $ed = 1 \bmod (p-1)(q-1)$

    The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be p = 7 and q = 13. Thus, modulus $n = pq = 7 \times 13 = 91$.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p-1)(q-1) = 6 \times 12 = 72$, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input $p = 7$, $q = 13$, and $e = 5$ to the Extended Euclidean Algorithm. The output will be $d = 29$.
- Check that the d calculated is correct by computing–

  $de = 29 \times 5 = 145 = 1 \bmod 72$
- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption—

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as–

  $C = P^e \bmod n$
- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.

- Returning to our Key Generation example with plaintext P = 10, we get cipher text C –

$C = 10^5 \bmod 91$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$\text{Plaintext} = C^d \bmod n$

- Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29–

$\text{Plaintext} = 82^{29} \bmod 91 = 10$

Q.4. (*a*) Explain diffusion and confusion property in encryption. (5)

Ans. Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.

Encryption is based on two principles: confusion and diffusion. Confusion means that the process drastically changes data from the input to the output. For example, by translating the data through a non-linear table created from the key. We have lots of ways to reverse linear calculations (starting with high school algebra), so the more non-linear it is, the more analysis tools it breaks.

Diffusion means that changing a single character of the input will change many characters of the output. Done well, every part of the input affects every part of the output, making analysis much harder. No confusion process is perfect: it always lets through some patterns. Good diffusion scatters those patterns widely through the output, and if there are several patterns making it through they scramble each other. This makes patterns vastly harder to spot, and vastly increases the amount of data to analyze to break the cipher.

One aim of confusion is to make it very hard to find the key even if one has a large number of plaintext-ciphertext pairs produced with the same key. Therefore, each bit of the ciphertext should depend on the entire key, and in different ways on different bits of the key. In particular, changing one bit of the key should change the ciphertext completely.

The simplest way to achieve both diffusion and confusion is a substitution-permutation network. In these systems, the plaintext and the key often have a very similar role in producing the output, hence it is the same mechanism that ensures both diffusion and confusion.

Q.4. (*b*) Explain various type of malicious codes such as viruses, worms etc. (5)

Ans. Various types of malicious code:

- **Viruses:** Pieces of code that attach to host programs and propagate when an infected program executes. A computer virus is a self replicating computer program which can attach itself to other files/programs, and can execute secretly when the host program/file is activated. When the virus is executed, it can perform a number of tasks, such as

erasing your files/hard disk, displaying nuisance information, attaching to other files, etc.

- **Worms:** Particular to networked computers, carry out pre-programmed attacks to jump across the network.

A worm is a self-replicating program that does not need to attach to a host program/file. Unlike viruses, worms can execute themselves. Worms have the ability to spread over a network and can initiate massive and destructive attacks in a short period of time.

- **Trojan Horses:** Hide malicious intent inside a host program that appears to do something useful.

A trojan horse is a non-replicating program that appears legitimate, but actually performs malicious and illicit activities when executed. Attackers use trojan horses to steal a user's password information, or they may simply destroy programs or data on the hard disk.A trojan horse is hard to detect as it is designed to conceal its presence by performing its functions properly.Some recent examples are:

1. Trojan horses embedded into online game plug-ins which will help online gamer to advance their game characters; however, the online game account and password are also stolen. The gamer's cyber assets are therefore stolen.
2. Trojan horses are embedded into popular commercial packages and uploaded to websites for free download or to be shared across peer-to-peer download networks.
3. Trojan horses are particularly dangerous due to the fact that they can also open a back door into a system and allow an attacker install further malicious programs on your computer. Back Orifice and SubSeven are two well-known remote access trojan horses that allow attackers to take control of a victim's computer.

- **Attack scripts:** Programs written by experts to exploit security weaknesses, usually across the network
- **Java attack applets:** Programs embedded in Web pages that gain foothold through a browser
- **ActiveX controls:** Program components that allow malicious code fragment to control applications or the OS

Q.5. What is an IDS (Intrusion Detection System)? Explain the need for Intrusion monitoring and detection. Explain at least 05 steps you would recommend to be adopted to improve the network security of any organization. (10)

Ans. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

IDS is one of many complementary layers of IT security technology. Several security layers exist because no one layer can provide all the security measures itself. IDS does several things that basic firewalls, for instance, cannot do:

- Identify anomalous packet content or patterns of traffic that are different from normal for any particular company's network.

• Identify patterns, called signatures, of malicious content within packets coming into or leaving a company's network.

• Identify changes in the security health or "state" of corporate servers.

Intrusion detection systems are of two main types, network based (NIDS) and host based (HIDS) intrusion detection systems.

Types of IDS:

(*a*) Network Intrusion Detection Systems: Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the designing of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

(*b*) Host Intrusion Detection Systems: Host Intrusion Detection Systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

All Intrusion Detection Systems use one of two detection techniques:

(*i*) Statistical anomaly-based IDS: An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured.

(*ii*) Rule based intrusion detection: It detect intrusion by observing events in the system and applying a set of rules that lead to the decision regarding whether a given pattern of activity is or is not suspicious. It has two types

1.Rule based anomaly detection

2.Rule based penetration detection

Improving Network Security of an Organisation

1. Understand your organization's business priorities.

How important is network security in relation to these goals? Would the implications of a data breach have a major impact on achieving those goals? If the answer is yes, then this is a critical area to address for your organization.

2. Identify the key stakeholders involved with protecting the network: At the end of the day, do you know who needs to be involved or consulted in making changes and who needs to be informed of these changes? Conducting an audit on which departments use the network and how will give you an understanding of the scope of players involved.

3. Determine what level of access users need to the network: Who needs to access the network on an individual level to do their job? Once you know this, you can determine if authentication is necessary, how strict it needs to be and how it will be done.

4. Assess the endpoints on your network: What endpoints are on your network? Are they corporate-owned or not? It is essential to understand exactly what is on the network so you can make sure all of these endpoints are protected.

5. Don't overlook non-computing endpoints on your network such as IoT devices: Are you looking at ALL endpoints on your network? Many organizations do not have complete visibility to every endpoint touching their network – which creates vulnerable blind spots. Non-computing endpoints that are unmonitored can be easy targets for attackers.

Q.6. Attempt any two parts: **(5×2=10)**

(*a*) PGP Protocol: Pretty Good Privacy (PGP) encryption program provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server. PGP can be used to send messages confidentially. PGP supports message authentication and integrity checking.

Q.6. (*b*) Hashing Techniques:

Ans. A cryptographic hash function is a kind of algorithm that can be run on a piece of data, like an individual file or a password, producing a value called a checksum.

The main use of a cryptographic hash function is to verify the authenticity of a piece of data. Two files can be assured to be identical only if the checksums generated from each file, using the same cryptographic hash function, are identical.

Some commonly used cryptographic hash functions include MD5 and SHA-1, though many others also exist.

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum').

The ideal hash function has three main properties:

1. It is extremely easy to calculate a hash for any given data.

2. It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.

3. It is extremely unlikely that two slightly different messages will have the same hash.

Q. 6. (c) Digital Signature

Ans. Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. Similarly, a digital signature is a technique that binds a person/entity to the digital data.

To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature.

The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

FIRST TERM EXAMINATION [SEPT. 2017]
SEVENTH SEMESTER [B.TECH]
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 1.30 hrs. **M.M. : 30**

Note: *Attempt any three question in all and Q.1 is compulsory.*

Q. 1. (a) Define Cyber Forensics. **(2)**

Ans. Cyber forensics is a branch of digital forensic science and an electronic discovery technique used to determine and reveal technical criminal evidence. It often involves electronic data storage extraction for legal purposes. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Q. 1. (b) Define Hash Function. **(2)**

Ans. A hash function is a cryptographic algorithm which is used to transform large random size data to small fixed size data. The basic operation of hash functions does not need any key and is impossible to compute the input from a particular output. The primary application of hash functions in cryptography is message integrity.

Q. 1. (c) Difference between Public key and Private key cryptography. **(2)**

Ans.

Private Key	Public Key
(i) Also Known as Symmetric Key Cryptography	Also Known as Asymmetric Key Cryptography
(ii) Same key is used for encryption and decryption purpose.	Different keys are used for encryption and decryption purpose.
(iii) Key agreement is the problem	There is no issue of key agreement
(iv) It is Scalable algorithm due to varied key size	Scalability does not exist
(v) Large amount of memory is used	Small memory size is required
(vi) Processing speed is fast for encryption and decryption	Its processing speed is slow for encryption as well as decryption
(vii) Private Key is truly private. Confidentiality is high.	Confidentiality is low.
(viii) No factorization is required to select the key	Factorization is required to calculate the key for example: RSA

Q. 1. (d) Difference between active and passive attack. **(2)**

Ans.

Active Attacks	Passive attacks
(i) In active attacks the attacker intercepts the connection and modifies the information	In passive attack, the attacker intercepts the transit information with the intention of reading and analyzing the information not for altering it

(ii) These are threat to Integrity and Availability	Threat to Confidentiality
(iii) Active attacks are easier to detect.	Passive attacks are difficult to detect.
(iv) There are four types of active attacks- • Masquerade • Replay • Modification of message • Denial of service	There are two types of passive attacks. • Release of message content. • Traffic analysis
(v) These attacks cannot be prevented easily.	These attacks can be prevented by encryption of data.
(vi) The attacker needs to gain the physical control of the media.	The attacker needs to observe the conversation.

Q. 1. (c) Explain the concept of Playfair cipher. (2)

Ans. The Playfair cipher is a manual symmetric encryption technique and was developed in 1854. It is also called Playfair square or Wheatstone-Playfair cipher. It involves the use of keys that arrange alphabetical letters in geometric patterns in order to encode messages. The Playfair cipher's essential method involves creating key tables that arrange the letters of the alphabet into a square grid. With these key tables, the user separates the text of a message into two-letter bits. The Playfair cipher uses a few simple rules relating to where the letters of each diagraph are in relation to each other. The rules are:

- If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle

For example: Suppose the key is 'hello world' and we want to encrypt 'Hide the Gold'.

Firstly a key table is created such that first characters (going left to right) in the table will be the phrase, with duplicate letters removed. The rest of the table will be filled with the remaining letters of the alphabet, in order. The key table would look like:

H E L O W
R D A B C
F G I J K
M N P S T
U V X Y Z

The result of the encryption of "hide the gold" with the key of "hello world" would be "LF GD MW DN WO CV"

Q. 2. (a) Describe the security challenges in wireless network/ Mobile Devices. (4)

The main benefits of wireless networking are its low cost and convenience. But the major drawbacks are speed and security. Network security issues fall into three main categories:

- **Availability:** is the network available to users whenever it is supposed to be.
- **Confidentiality** : is the information being sent across the network transmitted in such a way that only the intended recipients can read it
- **Integrity:** is the information reaching the recipient intact

Confidentiality

The main way to ensure that data is not disclosed to unauthorized users is by encrypting it during transit, and wireless networks are able to do this in just the same way as wired networks. However, encryption is meaningless without authentication, since an unauthorized user could authenticate themselves onto the network and then be given the key with which to decrypt the data. The traditional model for authorization is to have some form of centralized system which stores access control lists. This model is fine for use in networks which have a relatively static set of users, and is suitable for Wi-Fi, but in other networks such as Bluetooth networks, which are much more ad-hoc in nature, this approach becomes impractical. In ad-hoc networks, not only does the dynamically changing set of users make updating access control lists infeasible in terms of cost, but there is also no guarantee that these devices would be able to access any central system.

Integrity: Because packets of data in wireless networks are sent through the air, they can be intercepted and modified quite easily by malicious users. This means that wireless networks are more vulnerable to attacks on the integrity of data. However, the current methods used by wired networks to ensure the integrity of packets, such as checksums, are perfectly adequate for ensuring the integrity of packets in wireless networks, and so no novel solutions have been adopted.

Availability: Wireless networks are particularly susceptible to DoS (Denial of Service) attacks. Unlike wired networks, which require the attacker to be physically connected to the network in some way before they can launch such an attack, with wireless networks an attacker only has to be within a certain range of the network (usually 100m) to be able to launch such an attack. These kind of attacks are particularly difficult to stop since network providers want to allow legitimate users to initiate communications with the network, and cannot stop malicious users from exploiting this to cause a denial of service.

Another way in which malicious users can potentially restrict the availability of the wireless networks is through radio jamming. This involves sending out a lot of noise on the same frequency as the network uses. However, there are techniques, such as frequency hopping which can make this kind of attack more difficult.

Q. 2. (b) Compare DES and AES (4)

Ans.

DES	AES
(i) In DES the data block is divided into two halves.	In AES the entire data block is processed as a single matrix
(ii) DES work on Feistel Cipher structure.	AES works on Substitution and Permutation Principle
(iii) Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits
(iv) 16 rounds	10 rounds for 128-bit algo12 rounds for 192-bit algo14 rounds for 256-bit algo
(v) DES has a smaller key which is less secure	AES has large secret key comparatively hence, more secure

(vi) DES is comparatively slower	AES is faster
(vii) Expansion Permutation, Xor, S-box, P-box, Xor and Swap	Sub bytes, Shiftrows, Mix columns, Add roundkey
(viii) Vulnerable to Differential and linear crypt analysis, Weak substitution tables	Strong against Differential,Truncated differential, linear, interpolation, square attacks

Q. 2. (c) What are various cryptographic techniques? (2)

Ans. Cryptographic techniques are of 2 types:

1. Symmetric Encryption Algorithm: For example: DES, AES, Blow Fish

2. Asymmetric Encryption Algorithm: For example: RSA, Diffie-Hellman, Elliptic Curve cryptography, Digital Signature

Q. 3. (a) Differentiate between Linear and Differential Cryptanalysis. (3)

Ans. Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. It is also known as Known plaintext attack. Linear cryptanalysis is a type of known plaintext attack that uses a linear approximation to describe how a block cipher Known plaintext attacks depend on the attacker being able to discover or guess some or all of an encrypted message, or even the format of the original plaintext. Linear cryptanalysis, a linear equation expresses the equality of two expressions which consist of binary variables combined with the exclusive-or (XOR)

Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. It is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key (cryptography key). Differential cryptanalysis requires chosen plaintexts, which, depending on the context, may or may not be a significant problem for the attacker.

Q. 3. (b) What does RSA stands for? Explain it with algorithm and example. (5)

Ans. RSA Stands for Rivest-Shamir-Adleman. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. It is a Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Key Generation	Encryption
1. Generate two large prime numbers, p and q	cipher = (message)^e mod n
2. Let n = pq	
3. Let m = Φ(n) = (p–1)(q–1)	Decryption
	message = (cipher)^d mod n

4. Choose a small number e, co prime to m, with GCD (Φ(n), e)–1; 1<e<Φ(n)	x mod y means the remainder of x divided by y
5. Find d, such that de mod Φ(n) = 1 Publish e and n as the public key. Keep d and m as the secret key.	

Example:

Key Generation :

1. Select 2 prime numbers -> p = 17 and q = 11
2. Calculate $n = p \times q = 17 \times 11 = 187$
3. Calculate = 16 × 10 = 160 Select 'e' such that e is relatively prime to (n)=160 and 1 < e < n
4. Determine d such that :

de =1 mod ϕ(n)

d × 7 = 1 mod 160

↓

161

d = e^{-1} mod ϕ(n)[161/7 = div.(d)23 and remainder (mod) =1

d = 23

Then the resulting keys are public key :

PU = {7, 187 }

PR = {23, 187 }

Let M = 88 for encryption

C = 88^7 mod(187)

88mod187 = 88

88^2mod187 = 7744mod187 = 77

88^4mod187 = 59969536mod187 = 132

88^7mod87 = (88^4mod187) × (88^2mod187) × (88mod187)mod187

= (132 × 77 × 88)mod187

= 894432mod187

= 11

• For Decryption:

M = C^dmod187

= 11^{23} mod 187

11^1mod187 = 11

11^2mod187 = 121

11^4mod187 = 14641/187 = 55

11^8mod187 = 214358881mod187 = 33

11^{23}mod187 = (11^8mod187 × 11^8mod187 × 11^4mod187 × 11^2mod187 × 11^1mod187)mod187

$= (33 \times 33 \times 55 \times 81 \times 11) \bmod 187$

$= 79720245 \bmod 187$

$= 88$

Q. 3. (c) Explain different types of attacks addressed by message authentication. **(2)**

Ans. The types of attacks are addressed by message authentication are:

(i)Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.

(ii) Traffic analysis: Discovery of the pattern of traffic between parties. In a connection oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.

(iii) Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or no receipt by someone other than the message recipient.

(iv) Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.

(v) Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

(vi) Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

(vii) Source repudiation: Denial of transmission of message by source.

(viii) Destination repudiation: Denial of receipt of message by destination

Q.4. (a) Difference between block and stream cipher. **(3)**

Ans.

Block cipher	Stream cipher
(i) Processing or encoding of plain text is done as a fixed length block one by one. A block could be of 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size should be of one bit.
(ii) Same key is used to encrypt each of blocks	A different key is used to encrypt each of the bits.
(iii) Padding of bits is done if the size of the block is short	No padding is required as bits are processed one by one as a chain.
(iv) More complex and slower in operation	Very simple and much faster
(v) Most block ciphers are based on fiestel cipher in structure	Statistically random
(vi) Example: Lucifer, DES, Blowfish5 etc	Examples: Fish, RC4, SEAL, SNOW etc

Q. 4. (b) Define Digital Signature.

Ans. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document and uses encryption techniques to provide proof of original and unmodified documentation. Digital signatures are used in e-commerce, software distribution, financial transactions and other situations that rely on forgery or tampering detection techniques. A digital signature is also known as an electronic signature.

A digital signature is applied and verified, as follows

- The document or message sender (signer) or public/private key supplier shares the public key with the end user.
- The sender, using his private key, appends the encrypted signature to the message or document.
- The end user decrypts the document and verifies the signature, which lets the end user know that the document is from the original sender

Q. 4. (c) What is Elliptic curve Cryptography? What are the various cryptographic schemes? Explain. **(4)**

Ans. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. ECC offers the same security than RSA but at a smaller footprint , also it's less cpu intensive so it's ideal for mobile devices and faster acting networks. ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths.

Following are the various cryptographic schemes:

(1) ECC Diffie-Hellman

The elliptic curve analog of Diffie-Hellman key exchange, which is a close analogy given elliptic curve multiplication equates to modulo exponentiation.

- Can do key exchange analogous to D-H
- Users select a suitable curve $E_q(a, b)$
- Select base point $G = (x_1, y_1)$
- With large order n s.t. $nG = O$
- A & B select private keys $n_A < n$, $n_B < n$
- Compute public keys: $P_A = n_A G$, $P_B = n_B G$
- Compute shared key: $K = n_A P_B$, $K = n_B P_A$

Example:

$p=211$; $E_q(0, -4) \rightarrow y^2 = x^3 - 4$; and $G = (2, 2)$ $240G = 0$.

A: Private key $n_A = 121$, Public key $P_A = 121(2, 2) = (115, 48)$

B: Private key $n_B = 203$, Public key $P_A = 203(2, 2) = (130, 203)$

Shared secret key: $121(130, 203) = 203(115, 48) = (161, 69)$

Globe Public Elements	
$E_q(a, b)$	elliptic curve with parameters a, b, and q where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation	
Select private n_A	$n_A < n$
Calcuate public P_A	$P_A = n_A \times G$

User B Key Generation	
Select private n_B	$n_A < n$
Calcuate public P_B	$P_B = n_B \times G$

Calculation of secret key by user A

$$k = n_A \times P_B$$

Calculation of secret key by user B

$$k = n_B \times p_A$$

2. ECC Encryption/Decryption

The sender must first encode any message m as a point on the elliptic curve P_m the ciphertext is a pair of points on the elliptic curve. The sender masks the message using random k, but also sends along a "clue" allowing the receiver who know the private-key to recover k and hence the message. For an attacker to recover the message, the attacker would have to compute k given G and kG, which is assumed hard.

→ First encode any message m as a point on the elliptic curve P_m

→ Select suitable curve w and point G as in $D - H$

→ A and B select private keys $n_A < n, n_B < n$

→ Compute public keys: $P_A = n_A G, P_B = n_B G$

→ A encrypts P_m : $C_m = \{kG, P_m + kP_B\}$,

k : random positive integer

P_B : B's public key

→ B decrypts C_m compute:

$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m$

Example:

p=751; $E_q(-1, 188) \rightarrow y^4 = x^2 - x + 188$; and G = (0, 376).

A → B; P_m = (562, 210)

A selects the random number k = 386.

B's Public key: PB = (201, 5).

A computes: 386 (0, 376) = (676, 558) and

(562, 201) + 386(201, 5) = (385, 328)

A sends the cipher text: {(676, 558), (385, 328)}.

3. The Digital Signature Algorithm: The Digital Signature Algorithm (DSA) was proposed in August of 1991 by the U.S. National Institute of Standards and Technology (NIST) and became a U.S. Federal Information Processing Standard (FIPS 186) in 1993. It was the first digital signature scheme to be accepted as legally binding by a government. The algorithm is a variant of the ElGamal signature scheme. It exploits small subgroups in Z_p^* = { 1, 2,..., p–1} in order to decrease the size of signatures.

Global Public Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \le L \le 1024$ and L a multiple of 64 i.e, bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of (p–1) where $2^{159} < q < 2^{160}$ ie., bit length of 160 bits

$g = h^{(p-1)/q} \bmod p$ where h is any integer with $1 < h < (p-1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudo integer with 0 < s <q

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with 0 < k < q

Signing

$r = (g^k \bmod p) \bmod p$

$s = [k^{-1}(H(M) + xr)] \bmod q$

Signature = (r, s)

Verifying

$w = (s-1)^{-1} \bmod q$

$u_1 = [H(M)w] \bmod q$

$u_2 = (r)w \bmod q$

$v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$

TEST : v = r

M = message to be signed
H(M) = hash of M using SHA-1
Mrs = received versions of M.r.t

Since r and s are each integers less than q, DSA signatures are 320 bits in length. The security of the DSA relies on two distinct discrete logarithm problems. One is the discrete logarithm problem in Z_p *where the number field sieve algorithm applies. Since p is a 1024-bit prime, the DSA is currently not vulnerable to this attack. The second discrete logarithm problem works to the base g: given p, q, g, and y, find x such that ya" $g^x \pmod p$. For large p (1024 bits, for example), the best-known algorithm for this problem is the Pollard rho-method, which takes about Sqrt.

πq / 2 steps. Since 160 q H^{-} /d^{-}/2 , the DSA is not vulnerable to this attack.

4. The Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA is the elliptic curve analogue of the DSA and works on an elliptic curve group $E(Z_p)$.

The ECDSA is currently being standardized by the ANSI X9F1 and IEEE P1363 standards committees.

END TERM EXAMINATION [DEC. 2017]
SEVENTH SEMESTER [B.TECH]
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five questions including Q.1 is compulsory.*

Q. 1. (a) What is the difference between virus,worms,Trojan horses and botnets? (2.5)

Ans. Virus: A computer virus attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Some virus can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you run or open the malicious program.The computer virus spreads by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

Worms: A worm is similar to a virus by its design and is considered to be a sub-class of a virus. Worms spread from computer to computer, and it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. Due to this nature,the worm consumes too much system memory, causing Web servers, network servers and individual computers to stop responding.

Trojan Horse: A Trojan horse is not a virus. Trojan horses are those files that claim to be something desirable but are malicious. It is a destructive program that looks as a genuine application. Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users or programs access to your system, allowing confidential and personal information to be theft.

Botnets: A botnet is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system. The term botnet is derived from the words robot and network. A bot in this case is a device infected by malware, which then becomes part of a network, or net, of infected devices controlled by a single attacker or attack group. The objective for creating a botnet is to infect as many connected devices as possible, and to use the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices.

Q. 1. (b) Distinguish between Linear and Differential cryptanalysis. Which one is chosen-plaintext attack and which one is known-plaintext attack? (2.5)

Ans. Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. It is also known as Known plaintext attack. Linear cryptanalysis is a type of known plaintext attack that uses a linear approximation to describe how a block cipher Known plaintext attacks depend on the attacker being able to discover or guess some or all of an encrypted message, or even the format of the original plaintext. Linear cryptanalysis, a linear equation expresses the equality of two expressions which consist of binary variables combined with the exclusive-or (XOR)

Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. It is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key. Differential cryptanalysis requires chosen plaintexts.

Differential cryptanalysis is a chosen plantext attack whereas linear cryptanalysis is a known plaintext attack.

Q. 1. (c) Compare active and passive attacks. List the various types of active and passive attacks. (2.5)

Ans. Refer Q.1. (c) First Term Examination 2017.

Q. 1. (d) Explain the difference between stream cipher and block cipher with the help of examples. (2.5)

Ans. Refer Q.1. (d) First Term Examination 2017.

Q. 1. (e) What is SSL and explain the role of SSL in information secutiy. (2.5)

Ans. Secure Sockets Layer (SSL) is a computer networking protocol for securing connections between network application clients and servers over an insecure network, such as the internet. SSL is used used to secure authentication and encryption for communication at the network transport layer. SSL uses a combination of public key and symmetric key encryption to secure a connection between two machines and a client system, communicating over the internet or another TCP/IP network. SSL runs above the transport layer and the network layer, which are responsible for the transport of data between processes and the routing of network traffic over a network between client and server, respectively, and below application layer protocols such as HTTP and the Simple Mail Transport Protocol. The "sockets" part of the term refers to the sockets method of passing data between a client and a server program in a network or between processes in the same computer.

Role of SSL in Information Security:

SSL supports the following information security principles:

- **Encryption**: protect data transmissions (e.g. browser to server, server to server, application to server, etc.).

The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can understand it. This is important because the information you send on the Internet is passed from computer to computer to get to the destination server. When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to. This protects it from hackers and identity thieves.

- **Authentication**: Authentication means you can be sure that you are sending information to the right server and not to an imposter trying to steal your information. This can be prevented by this by using a proper Public Key Infrastructure (PKI), and getting an SSL Certificate from a trusted SSL provider.
- **Data integrity**: ensure that the data that is requested or submitted is what is actually delivered.

SSL providers will also give you a trust seal that instills more trust in your customers.

SSL can be used to secure:

- Online credit card transactions or other online payments.
- Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
- Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
- The connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
- System logins to applications and control panels like Parallels, cPanel and others.
- Workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.
- Hosting control panel logins and activity like Parallels, cPanel and others

Q. 1. (f) List and explain the security services provided by digital signature. **(2.5)**

Ans. A **digital signature** is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit.

Following are the security services provided by digital signature:

- **Message authentication** " When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** " In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** " Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

Q. 1. (g) What is cyber forensics? How hacking is different from cracking? **(2.5).**

Ans. Cyber forensics is a branch of digital forensic science and an electronic discovery technique used to determine and reveal technical criminal evidence. It often involves electronic data storage extraction for legal purposes. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Hacking	Cracking
• Hacking, is the act of stealing personal or private data, without the owner's knowledge or consent. It include stealing passwords, creating a bot net, or pretty much any act that breaches someone's privacy, without their knowledge, or consent	Cracking is where edit a program's source code, or you could create a program, like a key generator patch, or some sort of application that tricks an application in to thinking that a particular process has occurred

• Hacking uses extensive knowledge of computer logic and code for malicious purposes	Cracking looks for back doors in programs, and exploits those back doors
• Hacking is more harmful	Cracking is less harmgul
• Hacking is not illegal	Cracking is illegal and is often termed as piracy.

Q. 1. (h) List four kinds of cryptanalysis attacks. **(2.5)**

Ans. Following are the types of cryptanalysis attacks:

- Ciphertext only attacks
- Known plaintext attacks
- Chosen plaintext attacks
- Chosen ciphertext attacks
- Man-in-the-middle attacks
- Side channel attacks
- Brute force attacks
- Birthday attacks

1. **Ciphertext Only Attack:** A ciphertext only attack (COA) is a case in which only the encrypted message is available for attack, but because the language is known a frequency analysis could be attempted. In this situation the attacker does not know anything about the contents of the message, and must work from ciphertext only.

2. **Known Plaintext Attack:** A known plaintext attack (KPA) both the plaintext and matching ciphertext are available for use in discovering the key. The attacker knows or can guess the plaintext for some parts of the ciphertext. For example, maybe all secure login sessions begin with the characters LOGIN, and the next transmission may be PASSWORD. The task is to decrypt the rest of the cipher text blocks using this information. This may be done by determining the key used to encrypt the data, or via some shortcut.

3. **Man-in-the-Middle Attack:** Cryptographic communications and key exchange protocols are susceptible to an attack in which the attacker is able to place himself on the communication line between two parties. In this "man-in-the-middle attack" the attacker is able to position himself to intercept the key exchange between two parties. He performs his own key exchange with each. Then, with both parties thinking they have set up a secure channel; the attacker decrypts any communications with the proper key, and encrypts them with the other key for sending to the other party. The parties think that they are communicating securely, but in fact the adversary is reading everything. Preventing a man-in-the-middle attack is possible if both sides compute a cryptographic hash function of the key exchange, sign it using a digital signature algorithm, and send the signature to the other side. The recipient then verifies that the hash matches the locally computed hash and the signature came from the desired other party.

4. **Brute Force Attack:** A brute force attack involves trying all possible keys until hitting on the one that result in plaintext. This can involve significant costs related to the amount of processing required to try quadrillions (in the case of DES) of keys. The time required is a factor of how many keys can be tried per unit of time, which is a factor of how many computers can be assigned to the task in parallel.

Q.2. (a) What is Kerberos? Discuss Kerberos version 4 in detail. What is S/MIME and its main function? **(7)**

Ans. Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos requests an encrypted ticket via an authenticated server sequence to use services. Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

S/MIME (Secure/Multipurpose Internet Mail Extensions) S/MIME, or Secure/Multipurpose Internet Mail Extensions, is a technology that allows you to encrypt your emails. S/MIME is based on asymmetric cryptography to protect your emails from unwanted access. It also allows you to digitally sign your emails to verify you as the legitimate sender of the message, making it an effective weapon against many phishing attacks out there. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape. S/MIME incorporates three public-key algorithms, DSS for digital sigantures, Diffie-Hellman for encyrpting session keys, or RSA. It uses SHA1 or MD5 for calculating digests, and three-key triple DES for message encryption. In an ideal situation, a S/MIME sender has a list of preferred decrypting capabilities from an intended recipient, in which case it chooses the best encryption. Otherwise, if the sender has received any previous mail from the intended recipient, it then chooses the same encryption mechanism.

Functions

S/MIME provides the following functions:

- Enveloped data: This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
- Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

Q. 2. (b) How intrusions can be detected? Explain intrusion prevention system in brief. **(8)**

Ans. Intrusions can be detected by monitoring network traffic for suspicious activity and issues alerts when such activity is discovered. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Detecting intrusions requires three elements:

- The capability to log security-relevant events
- Procedures to ensure the logs are monitored regularly
- Procedures to properly respond to an intrusion once detected

An **Intrusion Prevention System** (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. The IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. The IPS is placed inline i.e. in the direct communication path between source and destination, actively analyzing and taking automated actions on all traffic flows that enter the network. As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives. IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. IPS products have ability to implement firewall rules, but it is not a core function of IPS. Also IPS offers deeper watch and monitor into network operations like bad logons, inappropriate content and many other network and application layer functions. IPS use signatures and it detect intrusions on the analysis of the traffic. The IPS prevents a large amount of downtime that would occur if it were not there, this is done by it stopping any damage that may have made its way to the databases from internal or even external attacks. The IPS also makes it easier for the administrators to see where attacks are coming from so that they can address them and prevent any further attacks from that location. IPS is a system that protects the following:

(a) Confidentiality: that it protect the information that stored on a computer and it prevent unauthorized use of that information.

(b) Integrity: IPS protects the integrity of information and prevents the alteration on that information from unauthorized users.

(c) Availability: Protecting the availability of computing resource, network, system or stored information and it prevent any use or access by unauthorized users.

Q. 3. (a) Compare MD-5 and SHA-1 Algorithm used for hashing. **(7)**

Ans.

	MD-5	SHA-1
(*i*)	MD5 is uses to create a message digest for digital signatures.It creates a fixed 128-bit output that,when summed, total 32 characters long .	SHA-1 is used to create digital signatures.It produces a 160-bit message digests.
(*ii*)	2^{128} bit operations required to find the original message	2^{160} bit operations required to find the original message
(*iii*)	MD5 is less stronger hash algorithm as it outputs a 128-bit message digest	SHA -1 is considered a stronger hash algorithm as it outputs a 160-bit message digest.
(*iv*)	It's output performance is 335 MiB/s	It's output performance is 192 MiB/s
(*v*)	It is less secure	It is more secure against Brute Force attack
(*vi*)	MD 5 is vulnerable against cryptanalysis	MD 5 is vulnerable against cryptanalysis

Q. 3. (b) Perform encryption and decryption using *RSA* algorithm for $P = 3$, $Q = 17$, $e = 7$ and $M = 5$. (8)

Ans. $P = 3, Q = 17, M = 5, e = 7$ (Given)

Calculate n : $\quad n = P \times Q = 3 \times 17$

$$\boxed{n = 51}$$

Calculate $\phi(n)$:

$$\phi(n) = (P-1)(Q-1)$$
$$= (3-1)(17-1)$$
$$= 2 \times 16$$
$$= 32$$

Now, to calculate d. $\quad ed = 1 \bmod \phi(n)$

$$\boxed{d = e^{-1} \bmod \phi(n)}$$

This e^{-1} can be calculated using extended euclidean algo.

$$ed = 1 \bmod \phi(n)$$
$$7 * d = 1 \bmod 32 \Rightarrow 7d \bmod 32 = 1$$

Suppose $\quad 32x + 7y = 1 \quad ...(i)$

$$32 = 4(7) + 4 \quad ...(ii)$$
$$7 = 1(4) + 3 \quad ...(iii)$$
$$4 = 1(3) + 1$$

Calculate until u get + 1

Now, back substitutes the values

$$1 = 4 - 1(3)$$
$$1 = 4 - 1[7 - 1(4)] \quad \text{from eqn.}$$
$$1 = 1(4) - 1(7) - 1(4)$$
$$= 2(4) - 1(7)$$
$$= 2[32 - 4(7)] - 1(7) \quad \text{from eqn. } (ii)$$
$$1 = 2(32) - 8(7) - 1(7)$$
$$1 = 2(32) - 9(7)$$
$$d = 32 - 9$$

$$\boxed{d = 23}$$

Public key $PU(e, n)$ *i.e.*, $(7, 51)$

Private key (d, n) *i.e.*, $23, 51)$

Encryption is with Public key, $M = 5$(Given)

$$C = M^e \bmod n$$
$$C = 5^7 \bmod 51$$
$$C = 78125 \bmod 51$$

$$\boxed{C = 44}$$

Decryption is with Private key

$$M = C^d \bmod n$$
$$= 44^{23} \bmod 51$$
$$44^1 \bmod 51 = 44$$
$$44^2 \bmod 51 = 49$$
$$44^4 \bmod 51 = 4$$

$$44^8 \bmod 51 = 16$$

$M = 44^{23} \bmod 51$ can be written as

$$= (44^8 \bmod 51 \times 44^8 \bmod 51 \times 44^4 \bmod 51 \times 44^2 \bmod 51 \times 44^1 \bmod 51) \bmod 51$$
$$= (16 \times 16 \times 4 \times 49 \times 44) \bmod 51$$

$$\boxed{M = 5}.$$

Q. 4. (a) Encrypt the message "The house is being sold tonight" using the following ciphers. Ignore the space between the words. Also decrypt the message to get back the original plaintext. (7)

Ans. (*i*) Vignere cipher with key: dollar

(*ii*) Auto key cipher with key=7

Vignere cipher table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The keyword is repeated until it matches the length of the plaintext.

For encryption, the first letter of the plaintext **T** is paired with **d** the first letter of the key. Use row **d** and column **T** of the Vigenère square, you will get **W and so on.**

Message:

t h e h o u s e i s b e i n g s o l d t o n i g h t

d o l l a r s d o l l a r s d o l l a r s d o l l a

For Encryption: WVPSOLKHWDMEZFJGZWDKGQWRST

For Decryption: Decryption is performed by going to the row in the table corresponding to the key, finding the position of the cipher text letter in this row, and then using the column's label as the plaintext.

d o l l a r s d o l l a r s d o l l a r s d o l l a

W V P S O L K H W D M E Z F J G Z W D K G Q W R S T

In row D (from cipher text dollars) the ciphertext W the ciphertext appears in column in T and so on, we retrieve: "thehouseisbeingsoldtonight"

Autokey Cipher with key = SEVEN

Plaintext t h e h o u s e i s b e i n g s o l d t o n i g h t

Keystream s e v e n t h e h o u s e i s b e i n g s o l d t o

Ciphertext l l z l b n z i p g v w m v y t s t q z g b t j a n

Q. 4. (b) Explain the following types of attacks: Phishing, DNS Spoofing, DDOS and SQL Injection. (8)

Ans. Phishing : Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. It is a cyber crime.

DNS Spoofing: DNS Spoofing is a type of computer attack wherein a user is forced to navigate to a fake website disguised to look like a real one, with the intention of diverting traffic or stealing credentials of the users. DNS spoofing is done by replacing the IP addresses stored in the DNS server with the ones under control of the attacker. There are mainly two methods by which DNS spoofing is carried out

a. DNS cache poisoning

b. DNS ID spoofing.

DDOS: A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

Types of DDoS attacks:

- Volumetric Attacks:
- TCP State-Exhaustion Attacks:
- Application Layer Attacks
- ICMP Flood
- IP/ICMP Fragmentation
- BGP Hijacking

SQL Injection: SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database. For example: on a Web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied.

Q. 5. (a) Using "GGSIP University" as a key for playfair cipher, encrypt the message " Cryptography and Network Security". (8)

Ans. Play fair cipher example

G	S	I	P	U
N	V	E	R	T
Y	A	B	C	D
F	H	K	L	M
O	Q	W	X	Z

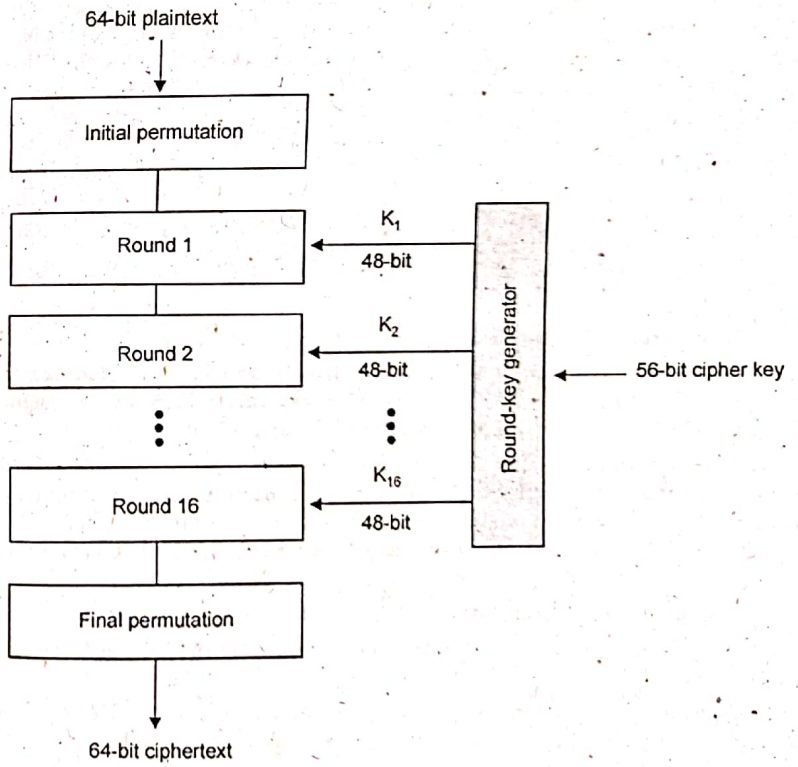
CR YP TO GR AP HY AN DN ET WO RK SE CU RI TY

LC CG NZ NPCSFA YV YTRNXQELIVDPEPND

Q. 5. (b) Explain DES function in detail. (8)

Ans. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm



Q.6. Short notes:

Q. 6. (a) PGP Protocol. (3)

Ans. Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files. It was developed by Philip R. Zimmermann in 1991 and has become a de facto standard for email security.

Pretty Good Privacy uses a variation of the public key system. In this system, each user has an encryption key that is publicly known and a private key that is known only to that user. Encryption of a message is done by public key and on receiving end decryption is done using their private key. PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message. When sending digital signatures, PGP uses an efficient algorithm that generates a hash from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version uses the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version uses the SHA-1 algorithm to generate the hash code.

PGP consists of the following five services:

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility
5. Segmentation

Q. 6. (b) Types of Firewalls: (4)

Ans. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall can be hardware, software, or both

(i) Packet Filters: Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header. The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts

- **Selection criteria**: It is a used as a condition and pattern matching for decision making.
- **Action field**: this part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules. As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets.

(ii) Application Gateways: An application-level gateway acts as a relay node for the application-level traffic. They intercept incoming and outgoing packets, run proxies that copy and forward information across the gateway, and function as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. The proxies are application specific. They can filter packets at the application layer of the OSI model. An application-specific proxy accepts **packets generated by only specified** application for which they are designed to copy, forward, and filter. For example, only a Telnet proxy can copy, forward, and filter Telnet traffic.

If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services that have no proxies configured. For example, if a gateway runs FTP and Telnet proxies, only packets generated by these services can pass through the firewall. All other services are blocked.

(iii) Circuit-Level Gateway: The circuit-level gateway is an intermediate solution between the packet filter and the application gateway. It runs at the transport layer and hence can act as proxy for any application.

Similar to an application gateway, the circuit-level gateway also does not permit an end-to-end TCP connection across the gateway. It sets up two TCP connections and relays the TCP segments from one network to the other. But, it does not examine the application data like application gateway. Hence, sometime it is called as 'Pipe Proxy'. For example: SOCKS refers to a circuit-level gateway. It is a networking proxy mechanism that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side without requiring direct IP reachability. The client connects to the SOCKS server at the firewall. Then the client enters a negotiation for the authentication method to be used, and authenticates with the chosen method.

Q. 6. (c) IDS: (3)

Ans. An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Types of Intrusion detection systems :

- **A network intrusion detection system** (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- **Host intrusion detection systems** (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates

from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.

- **Signature-based intrusion detection** systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.

- **Anomaly-based intrusion detection** systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

FIRST TERM EXAMINATION [SEP. 2018]
SEVENTH SEMESTER [B.TECH]
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 1.5 hrs. M.M. : 30

Note: Q. No. 1 is compulsory. Attempt any two more Questions from the rest.

Q. 1. Attempt all parts

(a) What is the difference between Cryptography and Cryptanalysis. (2)

Ans. Difference between cryptography and cryptanalysis.

Cryptography is the art of hiding messages by converting them into hidden texts. It is generally done in order to transmit a message over insecure channels. The process of transforming information into nonhuman readable form is called encryption. The process of reversing encryption is called **decryption**. Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages.

Cryptanalysis is the art of decrypting or obtaining plain text from hidden messages over an insecure channel. It is also known as code cracking. The success of cryptanalysis attacks depends on–

- Amount of time available
- Computing power available
- Storage capacity available

Following are commonly used Cryptanalysis attacks: **Brute force attack, Dictionary attack, Rainbow table attack.**

Q. 1. (b) Differentiate between Stream Cipher and Block Cipher. (2)

Ans. Refer Q. 4. (c) First Term Examination 2018.

Q. 1. (c) Explain ciphertext-only attacks. (2)

Ans. In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. He does not have access to corresponding plaintext. Ciphertext Only Attack is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.

Q. 1. (d) What are the different security goals. (2)

Ans. The primary security goals are:

Confidentiality – The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality makes sure that the data is available only to the intended and authorized persons.

Integrity– This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

Availability– The function of availability is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

Q. 1. (e) What is the difference between Symmetric and Asymmetric Cryptography. (2)

Ans. The fundamental difference that distinguishes symmetric and asymmetric encryption is that **symmetric encryption** allows encryption and decryption of the message with the same key. On the other hand, **asymmetric encryption** uses the public key for the encryption, and a private key is used for decryption.

The symmetric encryption is used for bulk data transmission whereas the asymmetric encryption is often used for securely exchanging secret keys.

The most commonly used symmetric encryption algorithms include DES, 3DES,AES, and RC4. 3DES and AES and The most common asymmetric encryption algorithm is RSA.

Q. 2. Explain RSA algorithm with example. **(10)**

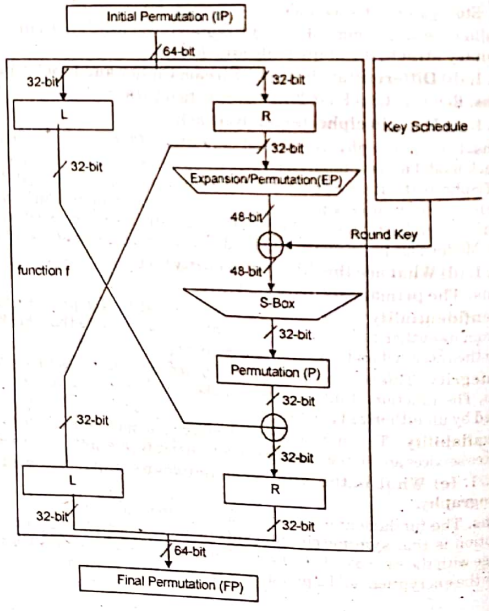
Ans. Refer Q. 3. (b) First Term Examination 2017.

Q. 3. What is modern block cipher. Explain DES algorithm with block diagram and explain each block. **(10)**

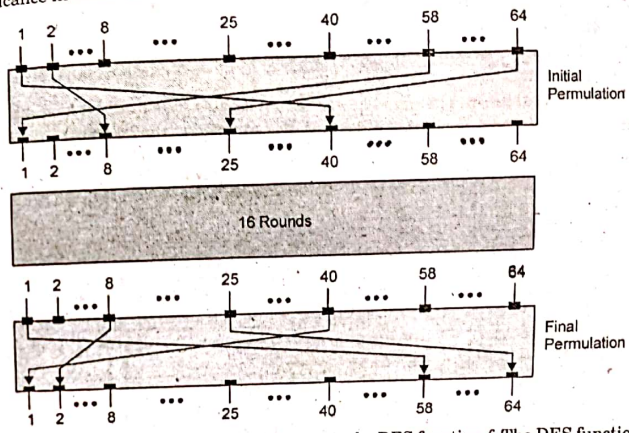
Ans. A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called a *block*, with an unvarying transformation that is specified by a symmetric key. The modern design of block ciphers is based on the concept of an iterated product cipher. Product ciphers effectively improving security by combining simple operations such as substitutions and permutations. Iterated product ciphers carry out encryption in multiple rounds, each of which uses a different subkey derived from the original key.

DES: The Data Encryption Standard (DES) is a symmetric-key block cipher. DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm. Since DES is based on the Feistel Cipher, all that is required to specify DES is –

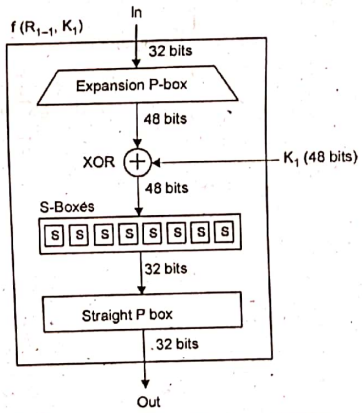
- Round function
- Key schedule
- Any additional processing– Initial and final permutation



Initial and Final Permutation: The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –



Round Function: The heart of this cipher is the DES function *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

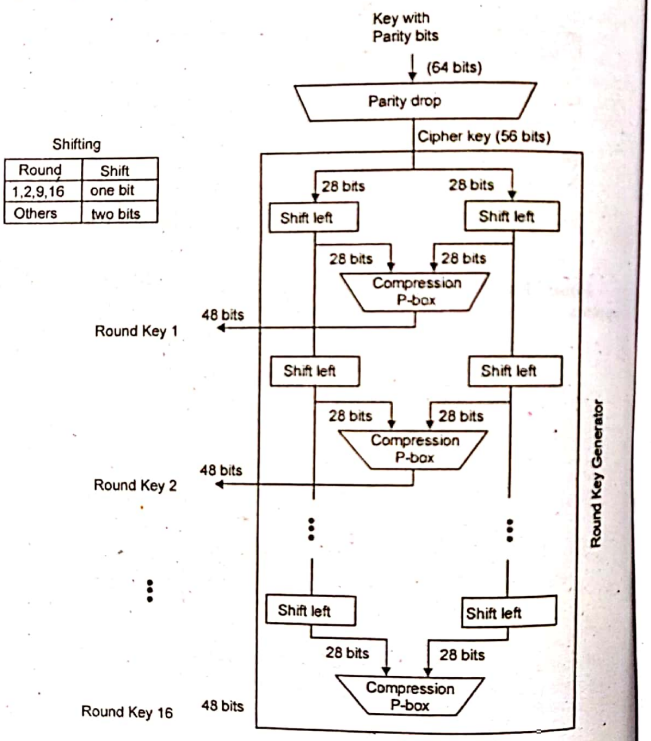


Expansion Permutation Box – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits.

- **XOR (Whitener):** After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

- **Substitution Boxes.** –The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.
- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- **Straight Permutation** – The 32 bit output of S-boxes is then subjected to the straight permutation

Key Generation: The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration



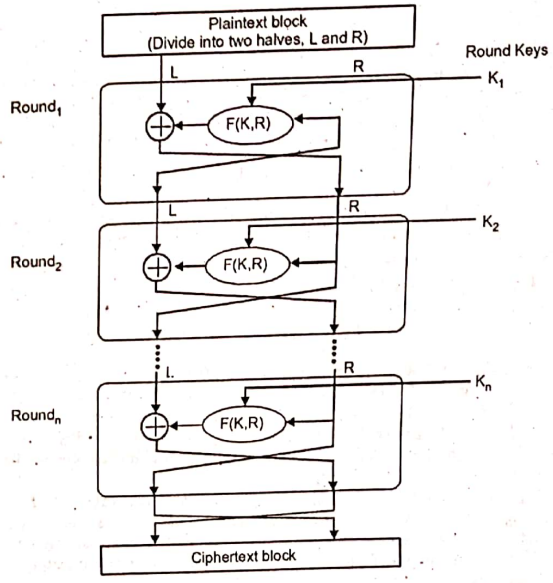
The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** – A small change in plaintext results in the very great change in the ciphertext.
- **Completeness** – Each bit of ciphertext depends on many bits of plaintext.

Q. 4. (a) Explain Feistel Ciphers. **(5)**

Ans. A Feistel cipher is a symmetric structure used in the construction of block ciphers, A Feistel cipher is a multi-round cipher that divides the current internal state of the cipher into two parts and operates only on a single part in each round of encryption or decryption. Between rounds, the left and right sides of the internal states switch sides.

Encryption Process: The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.



- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input " the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.

• Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.

• Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

Decryption Process: The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order. The final swapping of 'L' and 'R' in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds: The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

Q. 4. (b) What is Kerckhoff's principle? Explain different cryptanalysis attack. (5)

Ans. Kerckhoffs's principle is A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

Types of Cryptanalysis attacks:

• **Ciphertext Only Attacks (COA)** – In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext.

• **Known Plaintext Attack (KPA)** – In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information.

• **Chosen Plaintext Attack (CPA)** – In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key.

• **Dictionary Attack** – This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

• **Brute Force Attack (BFA)** – In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

• **Birthday Attack** – This attack is a variant of brute-force technique. It is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates.

• **Man in Middle Attack (MIM)** – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

• Host *A* wants to communicate to host *B*, hence requests public key of *B*.

• An attacker intercepts this request and sends his public key instead.

• Thus, whatever host *A* sends to host *B*, the attacker is able to read.

• In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to *B*.

• The attacker sends his public key as *A*'s public key so that *B* takes it as if it is taking it from *A*.

• **Side Channel Attack (SCA)** – This type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.

• **Timing Attacks** – They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.

• **Power Analysis Attacks** – These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.

• **Fault analysis Attacks** – In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

Q.4. (c) Difference between block and stream cipher. (3)

Ans.

Block cipher	Stream cipher
(i) Processing or encoding of plain text is done as a fixed length block one by one. A block could be of 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size should be of one bit.
(ii) Same key is used to encrypt each of blocks	A different key is used to encrypt each of the bits.
(iii) Padding of bits is done if the size of the block is short	No padding is required as bits are processed one by one as a chain.
(iv) More complex and slower in operation	Very simple and much faster
(v) Most block ciphers are based on fiestel cipher in structure	Statistically random
(vi) Example: Lucifer, DES, Blowfish5 etc	Examples: Fish, RC4, SEAL, SNOW etc

END TERM EXAMINATION [NOV-DEC 2018]
SEVENTH SEMESTER [B.TECH]
CRYPTOGRAPHY AND NETWORK SECURITY
[ETIT–403]

Time : 3 hrs. **M.M. : 75**

***Note:** Attempt any five questions including Q. No. 1 is compulsory.*

Q. 1. (a) List three Approaches to secure user Authentication in a Distributed Environment. (3)

Ans. 1. Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID).

2. Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user.

3. Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

Q. 1. (b) Compare and Contrast a Conventional Signature and a Digital Signature. (3)

Ans.

Basis For Comparison	Digital Signature	Electronic Signature
Basic	Digital signature can be visualised as an electronic "fingerprint", that is encrypted and identifies the person's identity who actually signed it.	Electronic signature could be any symbol, image, process attached to the message or document signifies the singer's identity and act an consent on it.
Authentication mechanism	Certificate-based digital ID	Veryfies signers identity through email, phone PIN, etc
Used for	Securing a document.	Verifying a document.
Validation	Performed by trusted certificate authorities or trust service provides.	No specific validation process.
Security	Highly secure	Vulnerable to tampering

Q. 1. (c) What are the two basic ways of transforming Plan Text into Cipher Text? (3)

Ans. There are two primary ways in which a plain text can be modified to obtain cipher text: Substitution Technique and Transposition Technique.

Substitution Technique: Substitution technique involves the replacement of the letters by other letters and symbols. In a more straightforward way, the characters of plaintext are replaced, and other substitute characters, numbers and symbols are used at their place.

Following are the types of substitution techniques: Caesar Cipher, Mono Alphabetic Cipher, Homophonic Substitution Cipher, Polygram Substitution Cipher, Vigenere Cipher

Transposition Technique: In transposition technique, the identity of the characters remains unchanged, but their positions are changed to create the ciphertext.

Types of Transpositional Techniques: Rail Fence Technique, Simple Columnar Transposition Technique, Vernam Cipher

Q. 1. (d) What is Masquerade? Which principle of security is breached because of that. (3)

Ans. A masquerade is a disguise.masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. two common masquerading attacks—IP spoofing and session hijacking.

Q. 1. (e) List the Parameters (Block Size, Key Size and Number of Rounds) for three AES Variants. (3)

Ans.

	AES-128	AES-192	AES-256
Block Size	128 bits	128 bits	128 bits
Key Size	16 byte keys	24 byte keys	32 byte keys
No. of rounds	10 rounds	12 rounds	14 rounds

Q. 1. (f) Distinguish between a Monoalphabetic Cipher and a Polyalphabetic Cipher. (2)

Ans.

Monolphabetic Cipher	Polyalphabetic cipher
1. Once a key is chosen, each alphabetic character of plaintext is mapped onto a unique alphabetic character of a ciphertext.	Each alphabetic character of plaintext can be mapped onto "m" alphabetic characters of a ciphertext.
2. The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
3. A stream cipher is a monoalphabetic if the value of keydoes depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of id does depend of the position of the plaintext character in the plaintext stream.
4. Monoalphabetic cipher includes additive multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.

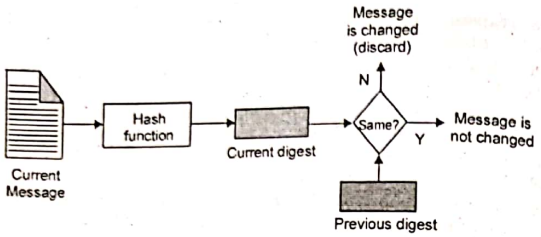
Q. 1. (g) Define the following terms: (4x2=8)

(i) Replay Attack **(ii) Message Intregrity**

(iii) Trojen Horses **(iv) DNS spoofing**

Ans. (i) Replay attack: A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently delay or repeat it. The delay or repeat of the data transmission is carried out by the sender or by the malicious entity, which intercepts the data and retransmits it. Replay attacks help attackers to gain access to a network, gain information which would not have been easily accessible or complete a duplicate transaction. A replay attack is also known as a playback attack.

(ii) Message Integrity: Message integrity means that a message has not been tampered with or altered. The most common approach is to use a hash function that combines all the bytes in the message with a secret key and produces a message digest that is difficult to reverse.

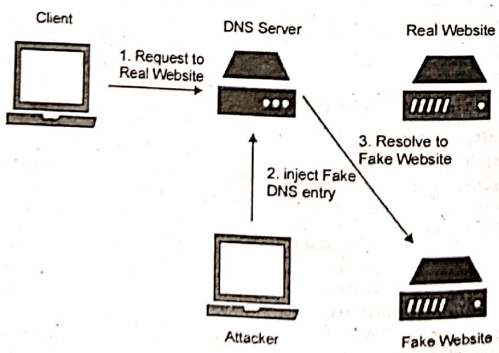


(iii) Trojen Horses: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. The seven main types of Trojan horses are:

- Remote Access Trojans
- Data Sending Trojans
- Destructive Trojans
- Proxy Trojans
- FTP Trojans
- security software disabler Trojans
- denial-of-service attack (DoS) Trojans

(iv) DNS Spoofing: Domain Name Server (DNS) spoofing is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. It is also called cache poisioning. Methods for executing a DNS spoofing attack include:

- **Man in the middle (MITM)** – The interception of communications between users and a DNS server in order to route users to a different/malicious IP address.
- **DNS server compromise** – The direct hijacking of a DNS server, which is configured to return a malicious IP address.



Q. 2. (a) Compare and Contrast Key management in PGP and S/MIME. (6)

Ans. • PGP is stands for the pretty good privacy.

• S/MIME is stands for the secured/multipurpose internet mail extension.

Following table describe the difference between the PGP and S/MIME.

	PGP	S/MIME
1.	PGP is the strong encryption standard.	S/MIME is also strong standard but there is some flaws in S/MIME
2.	Diffie hellman digital signature is used.	Elgamal digital signature is used.
3.	There are 4096 public keys in PGP	There is 1024 public keys in S/MIME
4.	It also used in virtual private networks.	But S/MIME is used in EMAIL services only.
5.	The digital certificate standard in PGP is PGP.	The digital certificate standard in S/MIME is X.509.

Q. 2. (b) Explain two Modes of IPSec. Discuss the Security Services provided by Authentication Header (AH) Protocol and Encapsulating Security Payload (ESP) Protocol. (6.5)

Ans. The IPsec standards define two distinct modes of IPsec operation, **transport mode** and **tunnel mode**. The modes do not affect the encoding of packets. The packets are protected by AH, ESP, or both in each mode. The modes differ in policy application when the inner packet is an IP packet, as follows:

- In transport mode, the outer header determines the IPsec policy that protects the inner IP packet.
- In tunnel mode, the inner IP packet determines the IPsec policy that protects its contents.

In transport mode, the outer header, the next header, and any ports that the next header supports, can be used to determine IPsec policy. In effect, IPsec can enforce different transport mode policies between two IP addresses to the granularity of a single port.

Tunnel mode works only for IP-in-IP datagrams. Tunneling in tunnel mode can be useful when computer workers at home are connecting to a central computer location. In tunnel mode, IPsec policy is enforced on the contents of the inner IP datagram. Different IPsec policies can be enforced for different inner IP addresses. That is, the inner IP header, its next header, and the ports that the next header supports, can enforce a policy. Unlike transport mode, in tunnel mode the outer IP header does not dictate the policy of its inner IP datagram.

Authentication Header (AH) is a protocol and part of the Internet Protocol Security (IPsec) protocol suite, which authenticates the origin of IP packets (datagrams) and guarantees the integrity of the data. The AH confirms the originating source of a packet and ensures that its contents (both the header and payload) have not been changed since transmission. AH provides authentication of the IP header and next-level protocol data. This can be applied in a nested fashion, or in conjunction with the IP encapsulating security payload (ESP). Security services are intiated between two communicating hosts, between two communicating security gateways or between a security gateway and a host.

AH provides data integrity using a checksum generated by an authentication code, similar to MD5. There is a secret shared key in the AH algorithm for data origin authentication. Using a sequence number field inside the AH header, relay protection is ensured.

AH can be used in tunnel or transport mode. In transport mode, the IP header of a datagram is the outermost IP header, followed by the AH header and the datagram.

This mode requires a reduced processing overhead compared to tunnel mode, which creates new IP headers and uses them in the outermost IP header of the datagram.

The fields within an AH header include:

- Next header
- Payload length
- Reserved
- Security parameters
- Sequence numbers
- Integrity check value

An Encapsulating Security Payload (ESP) is a protocol within the IPSec for providing authentication, integrity and confidentially of network packets data/payload in IPv4 and IPv6 networks. ESP provides message/payload encryption and the authentication of a payload and its origin within the IPSec protocol suite. An Encapsulating Security Payload is primarily designed to provide encryption, authentication and protection services for the data or payload that is being transferred in an IP network. ESP doesn't protect the packet header it can encrypt the entire packet residing inside another packet. Typically, in an IP network packet, the ESP header is placed after the IP header. The components of an ESP header include sequence number, payload data, padding, next header, an integrity check and sequenced numbers.

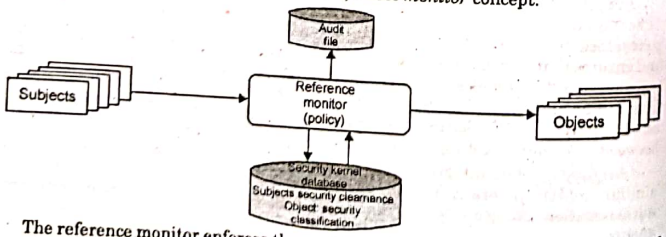
Q. 3. (a) Explain the Concept of Trusted systems. (6)

Ans. A **trusted system** is a system that is relied upon to a specified extent to enforce a specified security policy. A somewhat different but widely applicable requirement is to protect data or resources on the basis of levels of security. This is commonly found in the military, where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS), or beyond. This concept is equally applicable in other areas, where information can be organized into gross categories and users can be granted clearances to access certain categories of data. When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security**. The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or noncomparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated. A multilevel secure system must enforce the following:

→ **No read up:** A subject can only read an object of less or equal security level. This is referred in the literature as the Simple Security Property.

→ **No write down:** A subject can only write into an object of greater or equal security level. This is referred to in the literature as the *-Property star property

These two rules, if properly enforced, provide multilevel security. For a data processing system, the approach that has been taken, and has been the object of much research and development, is based on the *reference monitor* concept.



The reference monitor enforces the security rules (no read up, no write down) and has the following properties:

Complete mediation: The security rules are enforced on every access, not just, for example, when a file is opened.

- **Isolation:** The reference monitor and database are protected from unauthorized modification.
- **Verifiability:** The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation.

Q. 3. (b) Explain in detail about SSL Handshaking Protocol between a Server and Client Communication with an appropriate diagram. (6.5)

Ans. The SSL Handshake Protocol uses the SSL Record Protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection.

This exchange of messages is designed to enable the following actions:

→ Authenticate the server to the client.

→ Allow the client and server to select cryptographic algorithms, or ciphers, they both support.

→ Optionally authenticate the client to the server.

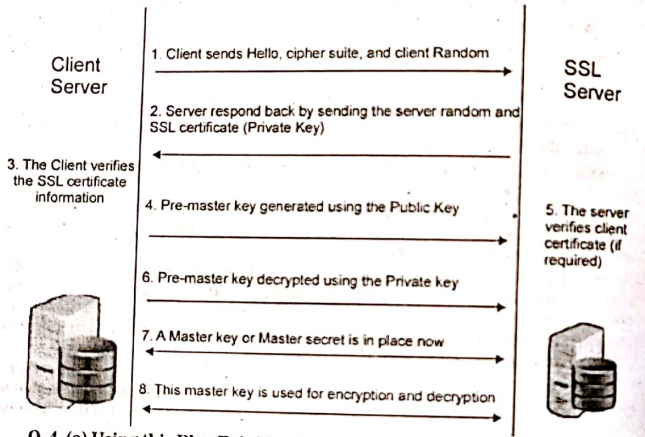
→ Use public key encryption to generate shared secret keys.

→ Establish an encrypted SSL connection.

SSL session always begins with an exchange of messages called the SSL handshake. Following are the steps involved in the SSL handshake:

1. The client sends the server the client's SSL version number, cipher settings, randomly generated data, and other information the server needs to communicate with the client using SSL.
2. The server sends the client the server's SSL version number, cipher settings, randomly generated data, and other information the client needs to communicate with the server over SSL. The server also sends its own digital certificate and, if the client is requesting a server resource that requires client authentication, requests the client's digital certificate.
3. The client uses the information sent by the server to authenticate the server. If the server cannot be authenticated, the user is warned of the problem that an encrypted and authenticated connection cannot be established. If the server can be successfully authenticated, the client proceeds.
4. Using all data generated in the handshake so far, the client creates the premaster secret for the session, encrypts it with the server's public key (obtained from the server's digital certificate), and sends the encrypted premaster secret to the server.
5. If the server has requested client authentication (an optional step in the hand shake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case the client sends both the signed data and the client's own digital certificate to the server along with the encrypted premaster secret.
6. If the server has requested client authentication, the server attempts to authenticate the client. If the client cannot be authenticated, the session is terminated. If the client can be successfully authenticated, the server uses its private key to decrypt the premaster secret, then performs a series of steps which the client also performs, starting from the same *premaster secret* to generate the *master secret*.

7. Both the client and the server use the *master secret* to generate session keys which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity.
8. The client informs the server that future messages from the client will be encrypted with the session key. It then sends a separate encrypted message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate encrypted message indicating that the server portion of the handshake is finished.
10. The SSL handshake is now complete, and the SSL session has begun. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.



Q. 4. (a) Using this Play Fair Matrix. **(6.5)**

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt the Message:

"Meet me at the usual place at ten rather than eight o clock"

[Note: Bogus Character to used- 'Z']

Ans. Play Fair Cipher: Encrypt the message "Meet me at the usual place at ten rather than

eight o clock"

ME UD
ET AD

ME UD
AT TH
TH HO
EU DZ
SU DN
AL RA
PL NR
AC GT
EA LR
TZ DW
TE DA
NR PL
AT TH
HE MA
RT AB
HA OT
NE UL
IG KR
HT OH
OC QT
LO NA
CK KQ

Q. 4. (b) Explain RSA Algorithm in detail. **(6)**

Ans. This cryptosystem is one of the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair: Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below–

- Generate the RSA modulus (n)

(i) Select two large primes, p and q.

(ii) Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

(iii) Find Derived Number (e)

(*a*) Number e must be greater than 1 and less than (p – 1)(q – 1).

(*b*) There must be no common factor for e and (p – 1)(q – 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

(iv) Form the public key

(*a*) The pair of numbers (n, e) form the RSA public key and is made public.

(*b*) Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

- Generate the private key

(a) Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.

(b) Number d is the inverse of e modulo (p – 1)(q – 1). This means that d is the number less than (p – 1)(q – 1) such that when multiplied by e, it is equal to 1 modulo (p – 1)(q – 1).

(c) This relationship is written mathematically as follows –

e d = 1 mod (p – 1)(q – 1)

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be $p = 7$ and $q = 13$. Thus, modulus $n = pq = 7 \times 13 = 91$.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, except for 1.
- The pair of numbers $(n, e) = (91, 5)$ forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input $p = 7$, $q = 13$, and $e = 5$ to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing–

de = 29 × 5 = 145 = 1 mod 72

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption: Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as–

$C = P^e \bmod n$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get cipher text C

$C = 10^5 \bmod 91$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

Plaintext = $C^d \bmod n$

- Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29.

Plaintext = $82^{29} \bmod 91 = 10$

Q. 5. (a) List the Main Features of SHA-512 Cryptographic Hash Function. What kind of Compression Function is used in SHA-512. **(6)**

Ans. SHA-512 is a variant of SHA-256 which operates on eight 64-bit words. The message to be hashed is first –

(1) padded with its length in suchaway that the result is a multiple of 1024 bits long, and then

(2) parsed into 1024-bit message blocks M(1) ; M(2) ;:::;M(N) .

The message blocks are processed one at a time: Beginning with a fixed initial hash value H(0) , sequentially compute

$H^{(i)} = H^{(i-1)} + C_M(i)\ (H^{(i-1)})$;

where C is the SHA-512 compression function and + means word-wise mod 2^{64} addition. $H^{(N)}$ is the hash of M.

The SHA-512 compression function operates on a 1024-bit message block and a 512-bit intermediate hash value. It is essentially a 512-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe:

(1) the SHA-512 compression function, and

(2) the SHA-512 message schedule

$\oplus$	bitwise XOR
$\wedge$	bitwise AND
$\vee$	bitwise OR
$\neg$	Bitwise complement
$+$	mod 2^{64} addition
R^n	right shift by n bits
S^n	right rotation by n bits

For SHA-512, all of these operators act on 64-bit words. The initial hash value H(0) is the following sequence of 64-bit words. Six logical functions are used in SHA-512. Each of these functions operates on 64-bit words and produces a 64-bit word as output. Each function is defined as follows:

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

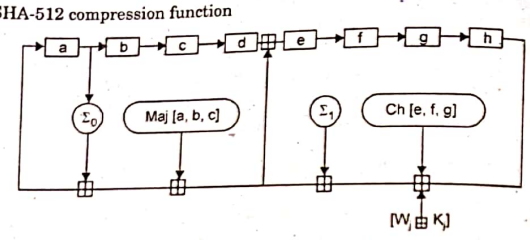
$$\Sigma_0(x) = S^{28}(x) \oplus S^{34}(x) \oplus S^{39}(x)$$

$$\Sigma_1(x) = S^{14}(x) \oplus S^{18}(x) \oplus S^{41}(x)$$

$$\sigma_0(x) = S^1(x) \oplus S^8(x) \oplus R^7(x)$$

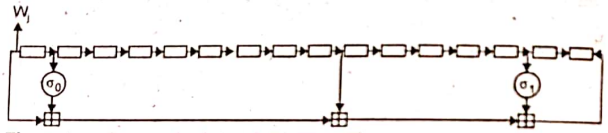
$$\sigma_1(x) = S^{19}(x) \oplus S^{61}(x) \oplus R^6(x)$$

The SHA-512 compression function



where the symbol ⊞ denotes mod 2^{64} addition.

The message schedule can be drawn as follows:



The registers here are loaded with $W_0, W_1, \ldots, W_{15}$.

Q. 5. (b)Alice and Bob want to establish a Secret Key using Diffie-Hellman Key Exchange Protocol. Assuming the values as N = 11, g = 5, x = 2 and y=3. Find out the values of A,B and Secret Key (K1 or K2). **(6.5)**

Ans.

1. Alice and Bob agree on a prime number N and a base g.
2. Alice chooses a secret integer x, then sends Bob
$$A = g^x \bmod N$$
3. Bob chooses a secret integer y, then sends Alice
$$B = g^y \bmod N$$
4. Alice computes
$$K_1 = B^x \bmod N$$
5. Bob computes
$$K_2 = A^y \bmod N$$
6. Alice and Bob now share a secret i.e. both Bob and Alice can use this number as their key.

Alice and Bob agree on a prime no. N = 11 and a base g = 5

$A = g^x \bmod N$,	$B = g^y \bmod N$
$A = 5^2 \bmod 11$,	$B = 5^3 \bmod 11$
$A = 3$,	$B = 4$
Key Received $= B = 4$,	Key Received $= A = 4$
$K_1 = B^x \bmod N$	$K_2 = A^y \bmod N$
$= 4^2 \bmod 11$	$= 3^3 \bmod 11$
$K_1 = 5$	$K_2 = 5$

Q. 6. Write short note on the following:

(a) Elliptic Curve Architecture **(4.5)**

Ans. 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-EC cryptography provide equivalent security. lliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

$$y^2 = x^3 + ax + b \mod p$$

Here, y, x, a and b are all within F_p, i.e. they are integers modulo p. The coefficients a and b are the so-called characteristic coefficients of the curve — they determine what points will be on the curve.

The curve coefficients have to fulfill one condition:

$$4a^3 + 27b^2 \neq 0$$

This condition guarantees that the curve will not contain any singularities.

Q. 6. (b) Buffer Flow Attack. **(4)**

Ans. Buffer overflow attack: In a **buffer-overflow attack,** the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.

Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input. There are two types of buffer overflows: stack-based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack: memory space used to store user input. Coding errors are typically the cause of buffer overflow.

Buffer Overflow Attack Example

```
print f ("\n correct Password \n");
pass = ;
}
if (pass)
{
prinf ("\n Root privileges given to the user \n");
}
return ;
```

Q . 6. (c) What is the difference between IDS and Firewall? (4)

Ans.

Firewall	IDS
(i) A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.	An Intrusion Detection System (IDS) is software of hardware device installed on the network (NIDS) or host (HIDS) to to detect and report intrusion attempts to the network.
(ii) A firewall can block an anauthorized access to network (E.g A watchman standing at gate can block a thief)	AN IDS can only report an intrusion; it cannot block it (E.g. A CCTV camera which can alert about a thief but cannot stop it)
(iii) A firewall cannot detect security breaches for traffic that does not pass through it (E.g. A gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems
(iv) Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
(v) No man-power is required to manage a firewall.	An administrator (man-power) is required to respond to threats issued by IDS
(vi) Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be first person attacked by a thief)	IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

Q. 7. (a) What are the various steps carried during cyber forensic. (4)

Ans. Computer forensics involves the preservation, identification, extraction, interpretation, and documentation of computer evidence. The field of computer forensics has different facets, and is not defined by one particular procedure. The primary phases in a computer forensics examination are:

- Discussion of suspicion and concerns of potential abuse by telephone
- Harvesting of all electronic data
- Identification of violations or concern
- Protection of the proof
- Confirming qualified, verifiable evidence
- Delivery of a written report and comments of the examiner

Steps in the Forensic Examination Process

Step 1: A chain of custody is established. The examiner makes sure they are aware at all times where any items related to the examination are located. A safe or cabinet is often used to secure items.

Step 2: All relevant information is cataloged. This includes active, archival, and latent data. Information that has been deleted will be recovered to whatever extent possible. Encrypted information and information that is password-protected is identified, as well as anything that indicates attempts to hide or obfuscate data. The integrity of the original media is maintained to the highest extent possible, which means that the original source of information should not be altered. An exact copy of a hard drive image is made and that image is authenticated against the original to make sure that it is indeed exact.

Step 3: Additional sources of information are obtained as the circumstances dictate. This includes firewall logs, proxy server logs, Kerberos server logs, sign-in sheets, etc.

Step 4: The information is analyzed and interpreted to determine possible evidence. Both exculpatory (they didn't do it) and inculpatory (they did it) evidence is sought out.

Step 5: A written report will be submitted to the client with the examiner's findings and comments.

Step 6: If necessary, the examiner will provide expert witness testimony at a deposition, trial, or other legal proceeding.

Q. 7. (b) Differentiate between Virus, worm, malware, ransom ware. (4)

Ans. Virus: Viruses also have the ability to replicate themselves, but they do damage files on the computer they attack. Their main weakness lies in the fact that viruses can get into action only if they have the support of a host program. Otherwise, they're just like a defeated warrior. They stick themselves to songs, videos, and executable files and travel all over the internet. W32.Sfc!mod, ABAP.Rivpas.A, Accept.3773 are some of the examples of virus programs.

The Virus Gang (Types of Computer Virus):

- File Viruses
- Macro Viruses
- Master Boot Record Viruses
- Boot sector Viruses
- Multi-Partite Viruses
- Polymorphic Viruses
- Stealth Viruses

Worms: Worms are malware computer programs which have the ability to replicate themselves. Their sole objective is to increase their population and transfer themselves to another computer via the internet or through storage media. They operate like spies involved in a top-secret mission, hiding their movement from the user.

Worms don't cause any harm to the computer; their replicating nature consumes hard drive space, thus, slowing down the machine. A couple of the infamous worms are SQL Blaster which slowed the internet for a small period and Code Red which took down almost 359,000 websites.

Malware: Malware is a type of software that aims to infiltrate or damage a computer or information system without the consent of its owner. Therefore, malware is the main term used to talk about all computer threats. Here are some reasons which might compel a coder to write malware programs:

- Take control of a person's computer for personal or professional reasons.
- To get financial benefits. This also includes hackers raising money for a cause. Last year, we heard about a ransomware attack where hackers were collecting money to feed people. But it doesn't mean what they were doing was right.
- To steal confidential data.
- To prove their point. For instance, by performing a security breach on a vulnerable system.
- To take down an individual computer or a complete network.

Ransomeware: Ransomware is a type of malware that can alter the normal operation of your machine. It encrypts the data and prevents you from using your

computer partially or wholly. Ransomware programs also display warning messages asking for money to get your device back to normal working condition. Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Q. 7. (c) What is denial of service attack. **(4.5)**

Ans. A denial-of-service attack is a security event that occurs when an attacker prevents legitimate users from accessing specific computer systems, devices, services or other IT resources. Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them.

While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding attacks can be more difficult to recover from. Recovering from a distributed denial-of-service (DDoS) attack, in which attack traffic comes from a large number of sources, can be even more difficult.

Signs of a DoS Attack

- degradation in network performance, especially when attempting to open files stored on the network or when accessing websites;
- an inability to reach a particular website;
- difficulty accessing a website; and
- a higher than usual volume of spam email.

Popular flood attacks include:

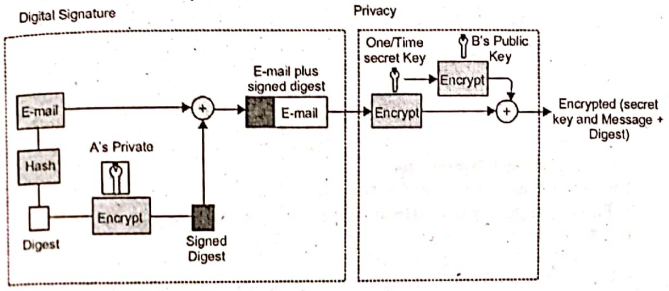
- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Q. 8. (a) With the help of a block diagram, draw a PGP protocol and explain. **(4)**

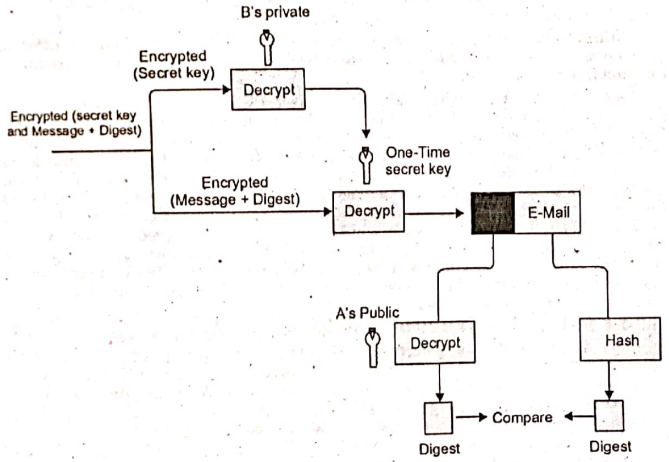
Ans. Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Pretty Good Privacy uses a variation of the public key system. In this system, each user has an encryption key that is publicly known and a private key that is known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses

the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

PGP at the Sender site (A)



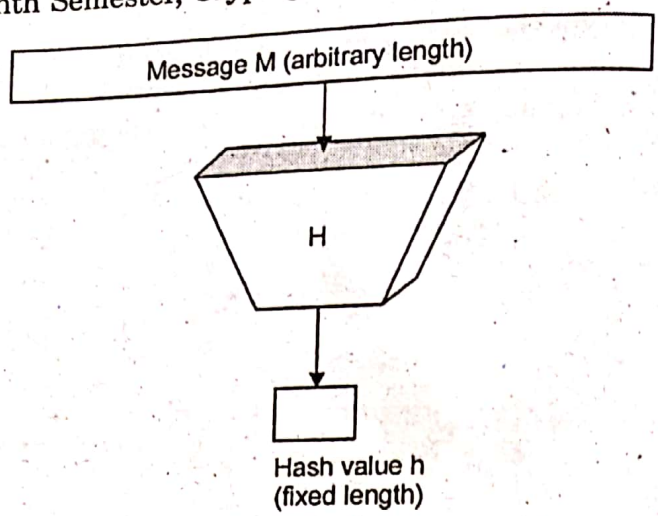
PGP at the Receiver site (B)



Q. 8. (b) What are hash functions? How they ensure security? Give example of a secure hash function. **(4)**

Ans. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function



Features of Hash Functions

The typical features of hash functions are

- **Fixed Length Output (Hash Value)**
- **Efficiency of Operation**

Properties of Hash Functions

Pre-Image Resistance: This property means that it should be computationally hard to reverse a hash function.

Second Pre-Image Resistance: This property means given an input and its hash, it should be hard to find a different input with the same hash.

Collision Resistance: This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-3, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of a specific user's hash value, rather than the actual password.

Q. 8. (c) Explain the functioning of light-weight cryptography. (4.5)

Ans. Lightweight cryptography is a **cryptographic** algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on. **Lightweight cryptography** also delivers adequate security. Lightweight cryptography does not always exploit the security-efficiency trade-offs. Functioning of lightweight cryptography:

1. Efficiency of end-to-end communication: In order to achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy consumption is important. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices.

2. Applicability to lower resource devices: The footprint of the lightweight cryptographic primitives is smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices.