MCA 305A: Cryptography and Network Security

UNIT I

Cryptography – Terminology, Conventional Encryption Model, Steganography, Classical Encryption Techniques, DES Data Encryption Standard, Block Cipher Design principles and Modes of Operation.

UNIT II

Conventional Encryption Algorithms: Triples DES, International Data Encryption Algorithm, Blowfish, RC5, Characteristics of advanced symmetric Block Ciphers, Confidentiality using Conventional Encryption.

UNIT III:

Public-Key Cryptography, Introduction to Number Theory: Prime Numbers, Modular Arithmetic, Euler's Theorem, Primary and Factorization, discrete logarithm, D-H Key sharing technique, RSA and its variants-Homomorphic Encryption Techniques Message Authentication and Hash Functions – Hash and MAC algorithms..

UNIT IV

Digital, Signatures and authentication Protocols, Digital Signature Standard, Network Security Practice, Authentication Applications. Basic overview of Electronic Mail Security: pretty Good Privacy's/MIME: IP Security, Web Security – Intruders, Viruses and Worms – Firewalls.

UNIT V

Mobile Security, Risk Model, Eco System, Service Risks, App Risks, Countermeasures- Cloud Computing Security- Threats-Security in Cloud Security at service layers. Introduction to Block chain, Crypto currency, Bit Coin Security and working, *Ethereum*.

Text Books

1. Cryptography and Network Security – by William Stallings, Principles and Practice, 7th Edition, Pearson
2. Cryptography and Network Security, by John Wiley, Edn,.2001

Reference Books

1. Bruce Schneier, Applied Cryptography, John Wiley, Second Edn,2001.
2. Charke Kaufman, Rodia Perlman and Mike Speciner, Network Security

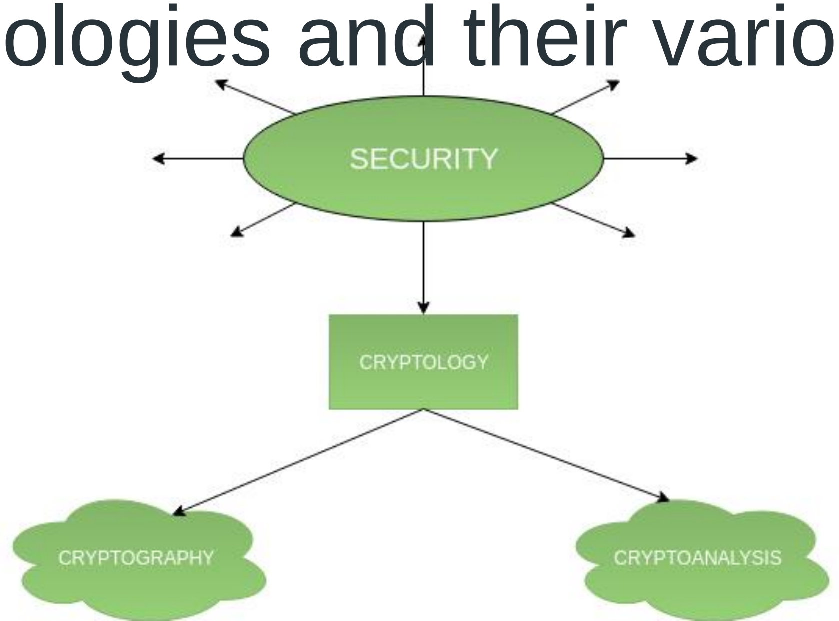
Cryptography And Network Security

LECTURE NOTES

Unit-1

Terminologies:

Cryptology is only one of the factors involved in securing networks. Cryptology refers to study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto-terminologies and their various types.



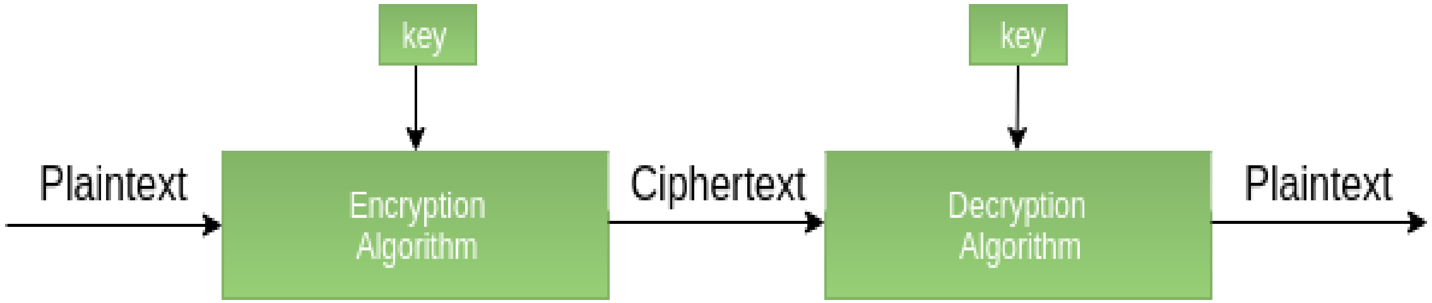
1. Cryptography:

Cryptography is the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

1. Symmetric-key cryptography
2. Hash functions.
3. Public-key cryptography

- **Symmetric key cryptography :**

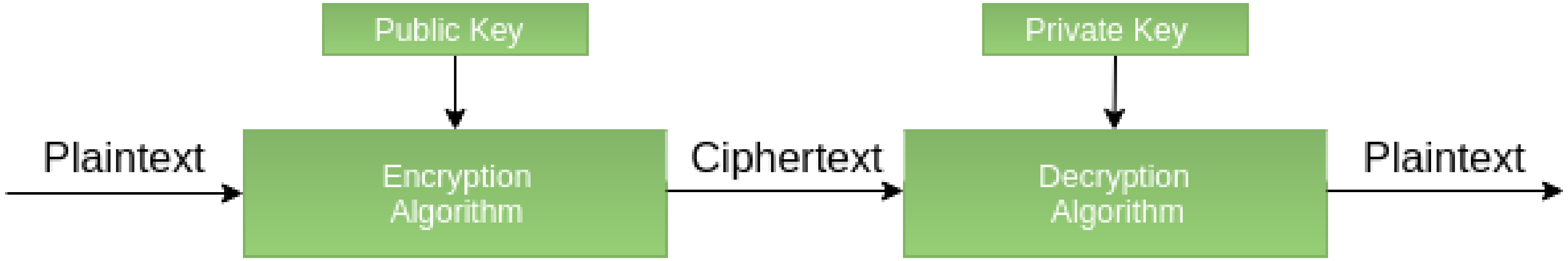
It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel..



SYMMETRIC KEY CRYTOGRAPHY

Asymmetric key cryptography :

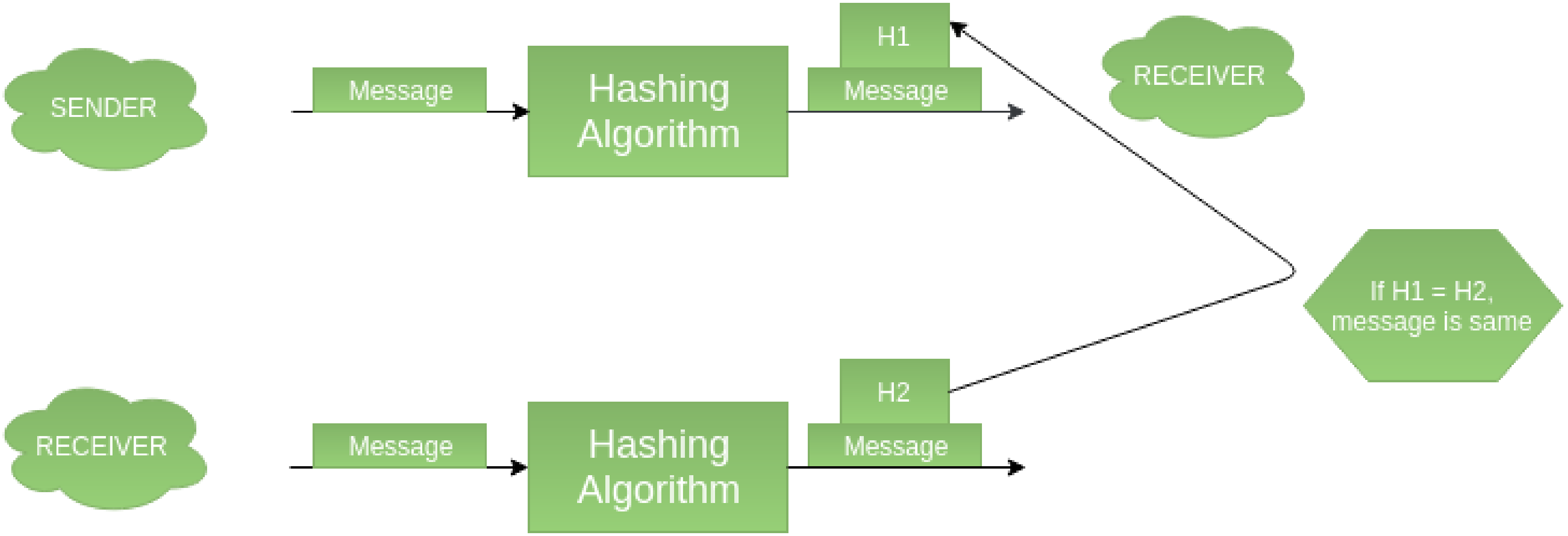
It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties uses different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



ASYMMETRIC KEY CRYTOGRAPHY

Hashing –

It involves taking the plain-text and converting it to a hash value of fixed size by a hash function. This process ensures integrity of the message as the hash value on both, sender\’s and receiver\’s side should match if the message is unaltered.



2. Cryptoanalysis

1. **Classical attacks –**

It can be divided into

a)Mathematical analysis and **b**) Brute-force attacks.

Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.

2. **Social Engineering attack –**

It is something which is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.

3. **Implementation attacks –**

Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

Convention Encryption Model

- Symmetric encryption is also referred to as **conventional encryption** or **single-key encryption.** It was the only type of encryption in use prior to the development of public-key encryption. It remains by far the most widely used of the two types of encryption.

A symmetric encryption scheme has five ingredients:

1. **Plain text:** This is the Original intelligible message or data that is fed in to the algorithm as input.
2. **Encryption Algorithm**: The encryption algorithm performs various substitutions and transformation on the plain text to convert it into ciphertext.
3. **Secret Key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plain text. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plain text and the secret key. For a given message, two different keys will produce different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
5. **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key as the input and produces the original plain text.

Steganography

- **Steganography** is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.
- One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file.
- For instance, in an image file each pixel is comprised of three bytes of data corresponding to the colors red, green, and blue (some image formats allocate an additional fourth byte to transparency, or ‘alpha’).
- LSB steganography changes the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you’ll need an eight-megabyte image file.
- Since modifying the last bit of the pixel value doesn’t result in a visually perceptible change to the picture, a person viewing the original and the steganographically modified images won’t be able to tell the difference.

Differences between steganography and cryptography

- Steganography is often compared to cryptography.
- While steganography hides information, cryptography focuses on rendering the data unreadable to everyone except its intended recipient.
- Once a stream of data is encrypted, only a person who has access to its decryption key will be able to unlock it.
- But if cryptography provides better protection for secret data, why use steganography at all?
- The presence of cryptography reveals that something is hidden, and in many cases, this is enough to get the sender in trouble.
- Sometimes, steganography and cryptography are used together.

Classical Encryption Techniques

Encryption is of 2 types

1. Asymmetric Encryption – Same key for encryption and decryption
2. Symmetric Encryption –different keys for encryption and decryption

- There are 2 types of classical encryption techniques are there they are

  1. Substitution Cipher
  2. Transposition Cipher

Substitution Cipher :

It is an encryption technique where the letters in the plain text are substituted/replaced by the letters or numbers or symbols

example:- plain text – ABCD

Cipher text – WXYZ

This substitution ciphers are divided into 5 types

1. Caser cipher
2. Mono alphabetic cipher
3. Poly alphabetic cipher
    1. Vigner cipher
    2. Vernam cipher
4. Play-fair cipher
5. Hill cipher

Transposition cipher:

The transposition cipher the characters or letters in the plain text are changed or rearranged in the zig-zag way.

- ❖ There is no replacement
- ❖There is no substitution

plane text – ABCDE
cipher text – CDAEB

They are divided into 2 components

1. Rail fence cipher
2. Row transposition cipher

Data Encryption Standard :

- **Data encryption standard (DES)** has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
- DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.
- The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.
- We have mention that DES uses a 56 bit key. Actually, the initial key consists of 64 bits.
- However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56 bit key.
- That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded. The basic idea is show in below figure.

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

Figure - discording of every 8th bit of original key

Block Cipher Design Principles

- **Block ciphers** are built in the Feistel cipher structure. Block cipher has a specific number of rounds and keys for generating ciphertext. For defining the complexity level of an algorithm few design principles are to be considered.
- These are explained as following below :
- **Number of Rounds –**
  The number of Rounds is regularly considered in design criteria, it just reflects the number of rounds to be suitable for an algorithm to make it more complex.
- In DES (Data Encryption Standard) we have 16 rounds ensuring it to be more secure while in AES (Advanced Encryption Standard) we have 10 rounds which makes it more secure.

1. Design of function F –

- The core part of the Feistel Block cipher structure is the Round Function.
- The complexity of cryptanalysis can be derived from the Round function i.e. the increasing level of complexity for the round function would be greatly contributing to an increase in complexity.
- To increase the complexity of the round function, the avalanche effect is also included in the round function, as the change of a single bit in plain text would produce a mischievous output due to the presence of avalanche effect.

2. Key schedule algorithm –

- In Feistel Block cipher structure, each round would generate a sub-key for increasing the complexity of cryptanalysis.
- The Avalanche effect makes it more complex in deriving sub-key. Decryption must be done very carefully to get the actual output as the avalanche effect is present in it

Modes of operation:

- Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher.
- **Block cipher** is an encryption algorithm which takes fixed size of input say *b* bits and produces a ciphertext of *b* bits again.
- If input is larger than *b* bits it can be divided further. For different applications and uses,
- there are several modes of operations for a block cipher.
  - **Electronic Code Book (ECB)**
  - **Cipher Block Chaining (CBC)**
  - **Cipher Feedback Mode (CFB)**
  - **Output Feedback Mode**

1. Electronic Code Book (ECB)

- Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted ciphertext. Generally, if a message is larger than *b* bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

2. Cipher Block Chaining (CBC)

Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.

3. Cipher Feedback Mode (CFB)

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as set of *s*and*b-s* bits the left hand side *s*bits are selected and are applied an XOR operation with plaintext bits. The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithm

4. Output Feedback Mode (OFM)

- The output feedback mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are send instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.

LONG ANSWER QUESTIONS:

1.Explain in detail about steganography.

2.Expalin in detail about Conventional Encryption Model.

3.Brief the strength of Data Encryption Algorithm and its modes of operations.

4.Explain in detail about Classical Encryption Techniques.

5.Write the differences between Block cipher design principles and modes of operarion.

SHORT ANSWER QUESTIONS

1.What is Cryptography?

2.write a short note on Conventional encryption model?

3.Define Steganography?

4.What is DES?

5.Write a short note on DES data encryption ?

Unit-2

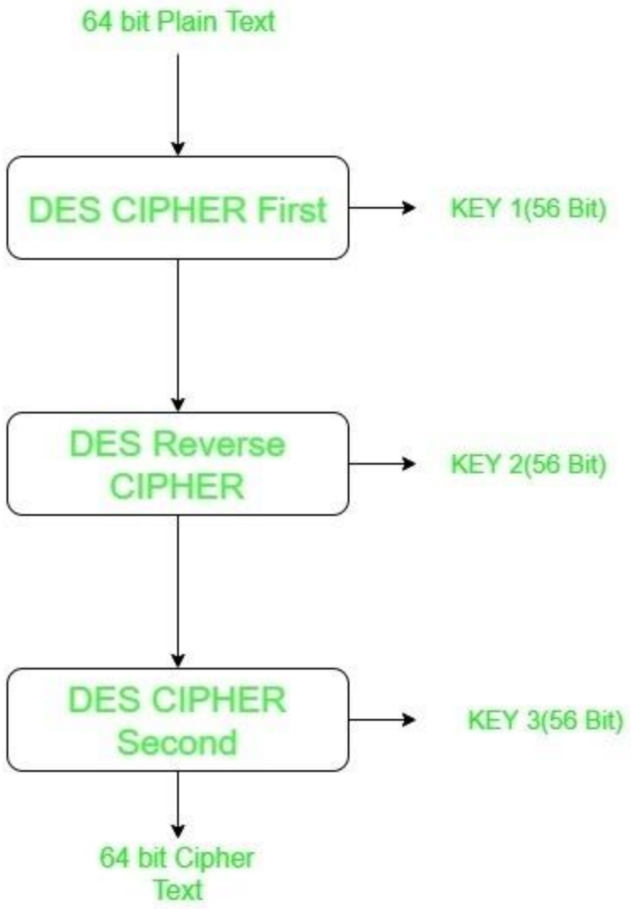
Conventional encryption algorithm

Conventional encryption algorithm:

- In cryptography variety of conventional encryption algorithms are available. They are **DES, AES, TDEA, IDEA, Blowfish, RC2, RC4, RC5, CAST 128**, etc. The Data Encryption Standard (DES) [2] developed by IBM early in 1970's and adopted by U.S National Institute of Standards and Technology (NIST).

Triple DES (Data Encryption Standard)

- In cryptography, Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is **a symmetric-key block cipher**, which applies the DES cipher algorithm three times to each data block.
- Triple DES is a encryption technique which uses three instance of DES on same plain text.
- It uses there different types of key choosing technique



- In first all used keys are different and In second two keys are same and one is different and in third all keys are same
- Triple DES is also vulnerable to meet-in-the middle attack because of which it give total security level of 2^112 instead of using 168 bit of key.
- The block collision attack can also be done because of short block size and using same key to encrypt large size of text.
- It is also vulnerable to sweet32 attack.

International Data Encryption Algorithm

- The International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES).
- It is a **symmetric-key block cipher** designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. ... IDEA was used in Pretty Good Privacy (PGP) v2.
- It consists block sizes of 64bits.
- Its contains 128 bits key sizes.

- International Data Encryption Algorithm (IDEA) is a once-proprietary free and open block cipher that was once intended to replace Data Encryption Standard (DES). Once called Improved Proposed Encryption Standard (IPES)I, DEA is a minor revision to the Proposed Encryption Standard (PES).
- IDEA uses similar processes for encryption and decryption, with some inverted ordering of round keys. It consists of a series of 8 rounds and operates on 64-bit blocks using a 128-bit key. IDEA suffered from weak keys until its key schedule was revised, and it may call for further revision in the future.
- IDEA has been and is optionally available for use with Pretty Good Privacy (PGP). IDEA has been succeeded by the IDEA NXT algorithm, itself once known as FOX.

Example:

> “Once brute-force techniques became stronger, the US government and encryption community looked to a replacement for the NIST-approved DES that was widely in use. IDEA was proposed as a replacement algorithm for DES, but it failed to do so and today, in the era of AES (Rijndael) which replaced DES, IDEA is obsolete.”

Blow Fish:

- Blowfish is a **symmetric encryption algorithm**, meaning that it uses the same secret key to both encrypt and decrypt messages.
- Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption.
- **Blowfish** is an encryption technique designed by **Bruce Schneier** in 1993 as an alternative to DES Encryption Technique.

- It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date.
- It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use.

1. **blockSize**: 64-bits
2. **keySize**: 32-bits to 448-bits variable size
3. **number of subkeys**: 18 [P-array]
4. **number of rounds**: 16
5. **number of subsitution boxes**: 4 [each having 512 entries of 32-bits each]

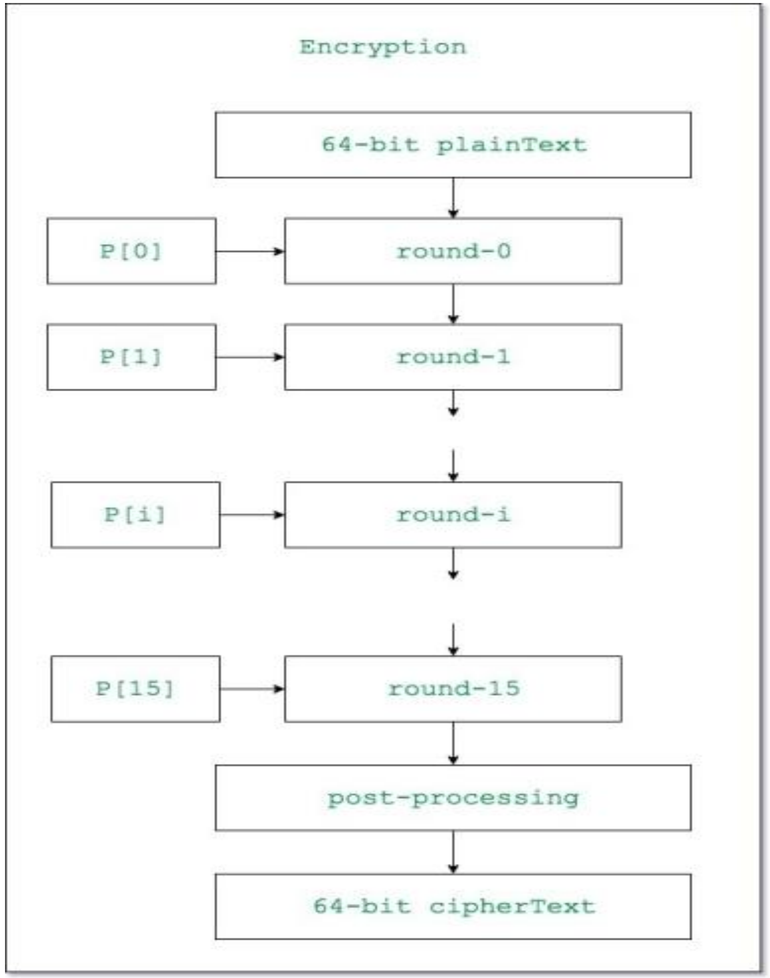
Advantages and Disadvantages of Blowfish Algorithm:

- Blowfish is a fast block cipher except when changing keys. Each new key requires a pre-processing equivalent to 4KB of text.
- It is faster and much better than DES Encryption.
- Blowfish uses a 64-bit block size which makes it vulnerable to birthday attacks.
- A reduced round variant of blowfish is known to be suceptible to known plain text attacks(2nd order differential attacks – 4 rounds).

Applications of Blowfish Algorithm:

- Bulk Encryption.
- Packet Encryption(ATM Packets)
- Password Hashing

Blowfish Encryption Algorithm



RC5:

- RC5 is **a symmetric-key block cipher** notable for its simplicity. Designed by Ronald Rivest in 1994,
- RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4).
- The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.
- It is notable for being simple, fast (on account of using only primitive computer operations like XOR, shift, etc.) and consumes less memory.

- RC5 is a block cipher and addresses two word blocks at a time.
- Depending on input plain text block size, number of rounds and key size, various instances of RC5 can be defined and each instance is denoted as RC5-w/r/b where w=word size in bits, r=number of rounds and b=key size in bytes.

Allowed values are:

Parameter	Possible Value
block/word size (bits)	16, 32, 64
Number of Rounds	0 – 255
Key Size (bytes)	0 – 255

Modes of RC5 Algorithm

There are 4 modes in RC5 which are as given below.

1. RC5 Block Cipher

This is also called an electronic codebook mode. It encrypts input blocks of a fixed size which is of 2w bits into a ciphertext block of the same length.

2. RC5 CBC

This is a cipher Chaining block for RC5. In this, plain text message whose length is equal to multiple of the RC5 block size is encrypted.

3. RC5 CBC Pad

This is the modified version of the CBC. Here input message can be of any length. The ciphertext is longer than the plain text by at the most the size of a single RC5 block. It uses padding to handle the mismatch of the length. This makes the length of the message equal to the multiple of 2w bits.

4. RC5 CTS

It is also called as a Ciphertext stealing mode. It is similar to an RC5 CBC pad. The length of the plain text message can be of any length and ciphertext is also equal of length.

Characteristics of advanced Symmetricblock ciphers

The characteristics of Advanced symmetric block ciphers are -

1) **Key dependent S-boxes** - S-box performs substitution and depicts the relationship between key and cipher text.

2) **Data dependent rotation** - Data dependent rotation results in differences in the amount of rotation.

3) Variable plain text or cipher text block length

4) Operations on both plain and ciphered data

S-Box:

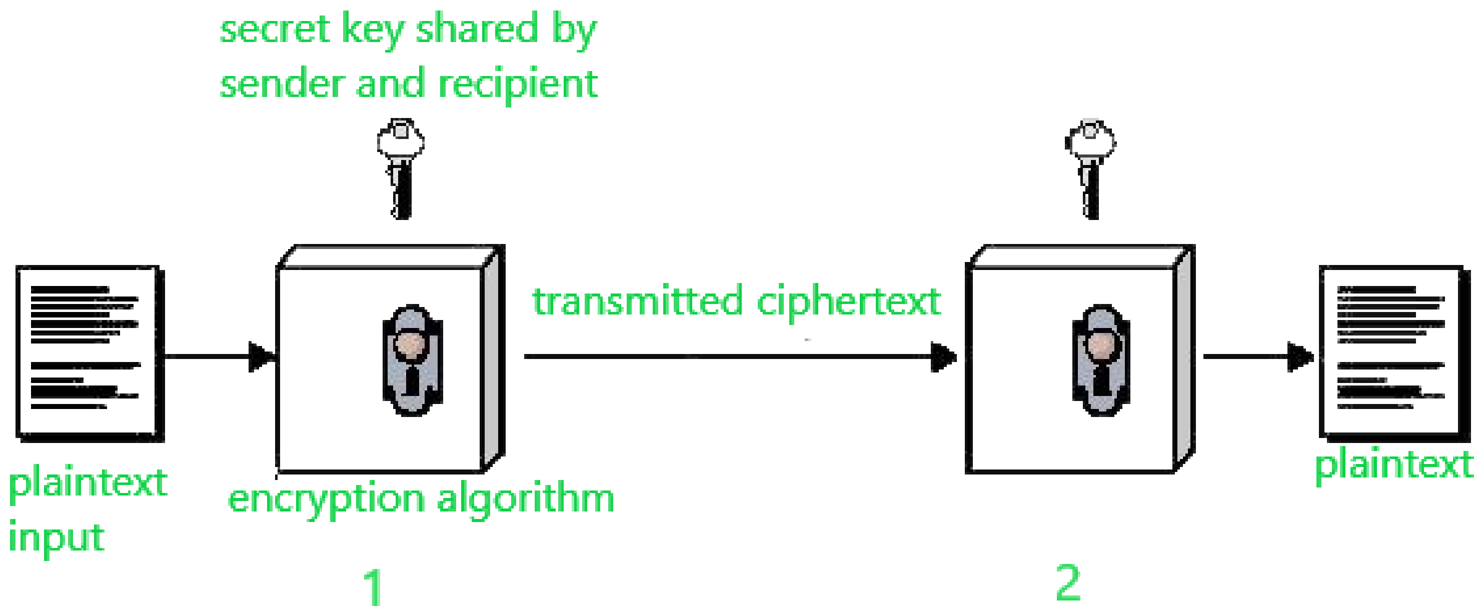
- In cryptography, an s-box is a basic component of symmetric key algorithm which perform **substitution.**
- This is called m*n S-Box and is often implemented as a lookup table.
- In block cipher, they are typically used to observe the relation ship between the key and the cipher text-Shannon’s property of confusion

- In general, S-Box takes m input bits and transforms them into n output bits, where n is not necessarily equal to m.
- This is called m*n S-Box and is often implemented as a lookup table.

- Fixed tables are normally used asin the data encryption standard (DES), but in some ciphers the tables are generated dynamically from the key.
- One good example of a fixed table is the S-Box from DES, mapping 64-bit input into 4-bit output.

Confidentiality Using Conventional Encryption:

- Conventional encryption is a cryptographic system that uses the same key used by the sender to encrypt the message and by the receiver to decrypt the message.
- It was the only type of encryption in use prior to the development of public-key encryption.
- It is still much preferred of the two types of encryption systems due to its simplicity.
- It is a relatively fast process since it uses a single key for both encryption and decryption In this encryption model, the sender encrypts plaintext using the receiver’s secret key, which can be later used by the receiver to decrypt the ciphertext. Below is a figure that illustrates this concept.



Confidentiality using encryption algorithm

- Suppose A wants to send a message to B, that message is called plaintext.
- Now, to avoid hackers reading plaintext, the plaintext is encrypted using an algorithm and a secret key (at 1).
- This encrypted plaintext is called ciphertext.
- Using the same secret key and encryption algorithm run in reverse(at 2), B can get plaintext of A, and thus the message is read and security is maintained.
- The idea that uses in this technique is very old and that’s why this model is called conventional encryption.

Conventional encryption has mainly 5 ingredients :

1. **Plain text –**
   It is the original data that is given to the algorithm as an input.

2. **Encryption algorithm –**
   This encryption algorithm performs various transformations on plain text to convert it into ciphertext.

3. **Secret key –**
   The secret key is also an input to the algorithm. The encryption algorithm will produce different outputs based on the keys used at that time.

4. **Ciphertext –**
   It contains encrypted information because it contains a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it. It is output from the algorithm.

5. **Decryption algorithm –**
   This is used to run encryption algorithms in reverse. Ciphertext and Secret key is input here and it produces plain text as output.

Requirements for secure use of conventional encryption :

1. We need a strong encryption algorithm.
2. The sender and Receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Advantages of Conventional Encryption :

1. **Simple –**
   This type of encryption is easy to carry out.

2. **Uses fewer computer resources –**
   Conventional encryption does not require a lot of computer resources when compared to public-key encryption.

3. **Fast –**
   Conventional encryption is much faster than asymmetric key encryption.

DisAdvantages of Conventional encryption model:

1. Origin and authenticity of the message cannot be guaranteed, since both sender and receiver use the same key, messages cannot be verified to have come from a particular user.

2. It isn’t much secured when compared to public-key encryption.

3. If the receiver lost the key, he/she cant decrypt the message and thus making the whole process useless.

4. This scheme does not scale well to a large number of users because both the sender and the receiver have to agree on a secret key before transmission.

LONG ANSWER QUESTIONS

1.Define Cryptography? Explain what is confidentiality using Conventional Encryption.

2.Explain characteristics of advanced Symmetric Block Ciphers.

3.Expalin International Data Encryption Algorithm.

4.Explain Triples DES Algorithm.

5.Explain About Blowfish.

SHORT ANSWER QUESTIONS

1.Write a short note on Conventional Encryption Algorithm?

2.Describe IDE Algorithm.

3.What is Blowfish.

4.Define RCS.

5.Define International Data encryption.

UNIT-3

Public key Cryptography:

- Public key cryptography is a class of cryptographic protocols based on algorithms.
- This method of cryptography requires two separate keys, one that is private or secret, and one that is public. Public key.
- cryptography uses a pair of keys to encrypt and decrypt data to protect it against unauthorized access or use.
- Network users receive a public and private key pair from certification authorities. If other users want to encrypt data, they get the intended recipient’s public key from a public directory.

- This key is used to encrypt the message, and to send it to the recipient. When the message arrives, the recipient decrypts it using a private key, to which no one else has access.
- The RSA (**Rivest-Sharmir-Adleman**) algorithm is the cryptography system that is used for public key cryptography, which is commonly used when sending secure, sensitive data over an insecure network like the internet.
- The **RSA algorithm** is popular because it allows both public and private keys to encrypt messages so their confidentiality and authenticity remain intact.

CHALLENGES OF PUBLIC KEY CRYPTOGRAPHY:

- Speed often is cited as the most common challenge associated with public key cryptography. Several private key cryptography methods are a great deal faster than the public key encryption method that currently is available. One way of overcoming this challenge with public key cryptography is to combine it with secret key systems to offer the security advantages of the public key system and the speed of the secret (private) key system.

BENEFITS OF PUBLIC KEY CRYPTOGRAPHY

- The increased data security provided by public key cryptography is its main benefit. Public key cryptography remains the most secure protocol (over private key cryptography) because users never need to transmit or reveal their private keys to anyone, which lessens the chances of cyber criminals discovering an individual’s secret key during the transmission.

- Public key cryptography also provides digital signatures that cannot be withhold. Public key cryptography requires each user to be responsible for protecting his private key, whereas private key systems require users to share secret keys and perhaps even trust third parties for transmission. With the secret key system, it is possible for senders to claim the shared secret key was compromised by one of the parties involved in the process.

Introduction to Number theory

Cryptography is also a means to ensure the integrity and preservation of data from tampering.
Modern cryptographic systems rely on functions associated with advanced mathematics, including a specialized branch of mathematics termed number theory that explores the properties of numbers and the relationships between numbers.

Prime Numbers:-

- Prime numbers are commonly referred to as the “atoms” of the numerical realm, for they are the fundamental, indivisible units that make up every number. For instance, 10 can be written as a product of 2 and 5, two prime numbers. Or, 150 as a product of 15 and 10, which can be further broken down and written as the product of 3, 5, 2 and 5 – all prime numbers. Or, a larger number such as 126, 356, which is composed of larger prime numbers 2,2,31 and 1019.
- This process of reducing a composite number to a product of prime numbers is known as prime factorization. For a computer, multiplying two prime numbers, each even 100 digits long, isn’t *that* difficult, however, factorizing the product back into its components is notoriously difficult, even for

supercomputers. It is this shortcoming that Rivest, Shamir and Adleman exploited to create RSA encryption in 1977.

Modular Arthimetic:-

- In cryptography, modular arithmetic directly underpins public key systems such as RSA and Diffie–Hellman, and provides finite fields which underlie elliptic curves, and is used in a variety of symmetric key

algorithms including Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and RC4.

- In modular arithmetic, we select an integer, n, to be our “modulus”.

Then our system of numbers only includes the numbers 0, 1, 2, 3, ..., n-1. In order to have arithmetic make sense, we have the numbers “wrap around” once they reach n.

Example: If we pick the modulus 5, then our solutions are required to be in the set {0, 1, 2, 3, 4}. We have 2+1=3 and 2+2=4 as usual. Then 2+3=5, which is not in our set, so it wraps around giving 2+3=0. Then 2+4=6, which wraps around to be 1.

This may seem strange, but in fact we use it everyday! Consider a clock, we go from 1 o’clock to 2 o’clock, ..., 11 o’clock, 12 o’clock, then back to 1 o’clock, and so on. This is an example of when the modulus is 12 and for clocks we use {1, 2, ..., 12} instead of {0,1, ..., 11}, but these are the same because we consider 0 and 12 to be the same in terms of wrapping around.

How do we write modular arithmetic?

Continuing the example above with modulus 5, we write:

2+1 = 3 (mod 5) = 3

2+2 = 4 (mod 5) = 4

2+3 = 5 (mod 5) = 0

2+4 = 6 (mod 5) = 1

Challenge question! What is 134 (mod 5)?

It might help us to think about modular arithmetic as the remainder when we divide by the modulus. For example 214 (mod 5) = 4 since 214 5 = 42 with remainder 4 (because 214 5 = 42*5 +4).

primary and factorization:

Primes are building blocks of whole numbers.

- A prime number is a number that is only divisible by one and itself, taken the even numbers out except two. There re infinite number of primes, and you can keep finding more by only using primes. Combining prime numbers can be multiplied to produce any number at all. prime can be explained as a basic-level number, when you look at it primes are the total set of numbers which are left over when the numbers are rewritten to their lowest possible level of integers. It is called factoring, and the numbers that are left over are primes. it is however hard to factor large prime numbers. it is just mathematically impossible or longer to factor a large number efficiently. Prime factorization is a mathematical problem commonly use to secure public key encryption systems, making it very important in cryptography. It is very common to use very large semi-primes which is the product of multiplying two prime numbers as the number which secures the encryption. To break it, they would have to find the prime factorization of the large semi-prime number which is two or more prime number that are multiplied together and result in the original number. The large number used to encrypt a file can be publicly known, due to the fact that encryption works so only the prime factors of the large number can be used in the decryption. It however takes a long time to find those factors and it is rather impossible even computationally.

Discrete Algorithms:

- Definition: If b is a unit modulo m and a is another unit with a ≡ b d (mod m), we say that d is the discrete logarithm of a modulo m to the base b, and write d = logb (a). ◦
- Note: Implicitly, we consider the discrete logarithm to be defined only modulo the order of b. Some authors instead define the discrete logarithm to be the smallest positive integer such that a ≡ b d (mod m) provided one exists, but (like with the definition of modular congruence) this definition is somewhat too restrictive.
- ◦ The reason this map is called the discrete logarithm is because its definition is analogous to that of the usual logarithm: logb (a) = d (mod k) is equivalent to a ≡ b d (mod m), where k is the order of b modulo m.

(Compare to the denition of the real-valued logarithm: logb (y) = x is equivalent to y = b x .)

- ◦ Example: Modulo 14, we have log3 11 = 4 since 3 4 ≡ 11 (mod 14). It is better to write log3 11 ≡ 4 (mod 6), since the order of 3 modulo 14 is 6.
- • As we would expect, it is easy to see that the discrete logarithm obeys the standard rules of logarithms.
- ◦ Specically, suppose that k is the order of b modulo m.
- ◦ Then logb (ac) ≡ logb (a) + logb (c) (mod k) and logb (a r) ≡ r logb (a) (mod k) for any integer r and any residue classes a and c whose discrete logarithms to the base b are defined.
- • Example: Find the discrete logarithms of each unit modulo 11 to the base 2.
- ◦ Since 2 is a primitive root modulo 11, we can write each unit as a power of 2.

The simplest way to do this is simply to compute each of the values 2 0 , 2 1 , ... ,

2 10 modulo 11; here is a table

of the results n 1 2 3 4 5

6 7 8 9 10 log2 n 0 1
8 2 4 9 7 3 6 5

◦ Observe, for example, that $3 \cdot 6 \equiv 7 \pmod{11}$, and log2 (3) + log2 (6) ≡ log2 (7) (mod 10), since 10 is the order of 2 modulo 11.

◦ Likewise, 3 3 ≡ 5 (mod 11), and 3 log2 (3) ≡ log2 (5) (mod 10).

- Having a table of discrete logarithms relative to a primitive root modulo m is very useful for computations.

◦ For example, it allows for very rapid multiplication and exponentiation, in the same manner as usual logarithms do. This is not terrically helpful because there already exist fast algorithms for these procedures.

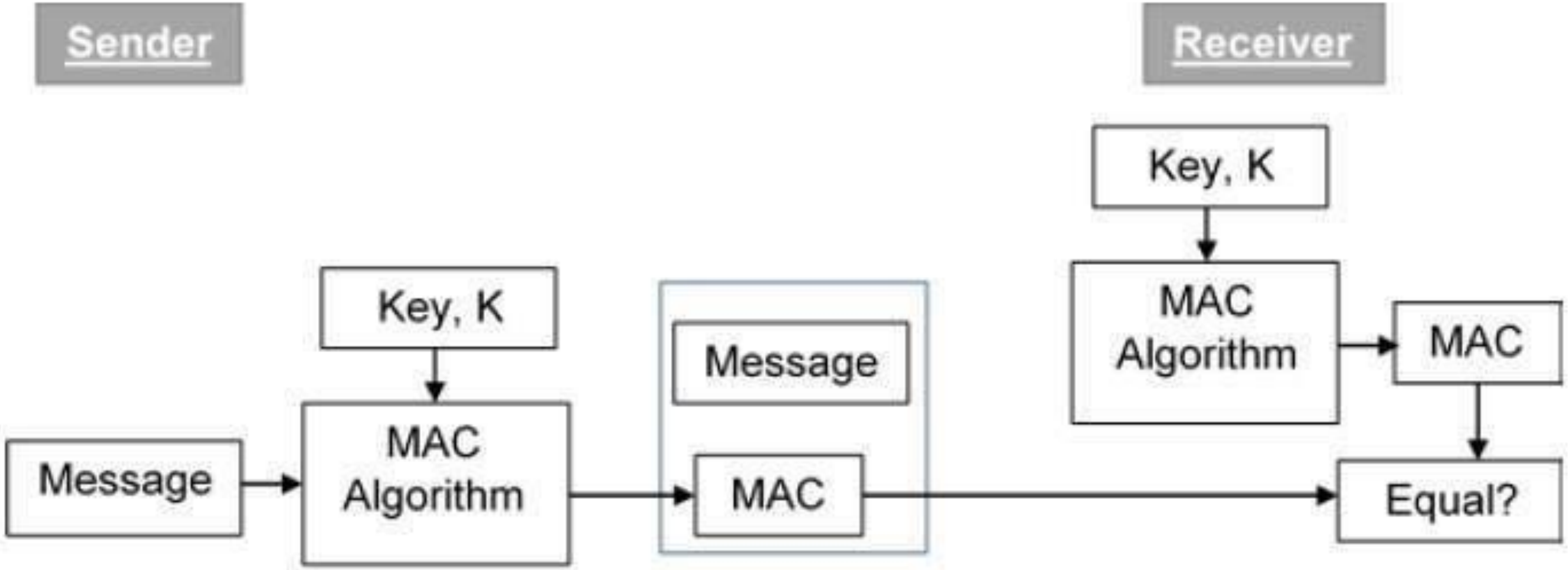
◦ More usefully, having a table of discrete logarithms also allows us to compute nth roots, if they exist.

Message Authentication:

- Alternative type of threat that happens for data is the lack of message authentication. In this threat, the user is not certain about the originator of the message.
- Message authentication can be delivered using the cryptographic methods that use secret keys as done in case of encryption.

Message Authentication Code:

- MAC algorithm is a symmetric key cryptographic method to offer message authentication. For starting MAC process, the sender and receiver share a symmetric key K.
- Basically, a MAC is an encrypted checksum produced on the underlying message that is sent along with a message to ensure message authentication.



- Let us now try to understand the entire process in detail −
- The sender uses some openly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.

- Alike 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. Now, we adopt that the message is sent in the clear, as we are worried of providing message origin authentication, not privacy. If confidentiality is essential then the message needs encryption.

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

- The receiver now checks equivalence of newly computed MAC with the MAC received from the sender. If they match, then the receiver receives the message and promises himself that the message has been sent by the proposed sender.

- If the calculated MAC does not match the MAC sent by the sender, the receiver cannot conclude whether it is the message that has been changed or it is the origin that has been falsified. As a bottom-line, a receiver securely assumes that the message is not the genuine.

Limitations of MAC

- There are two main boundaries 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 guarantee that a message inventor cannot deny any formerly sent messages and promises or actions.
- MAC method does not offer a non-repudiation service. If the sender and receiver get complicated in an argument over message origination, MACs cannot offer a proof that a message was certainly sent by the sender.

- However no third party can calculate the MAC, still sender could reject 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.
- Both these limits can be overcome by by means of the public key based digital names debated in resulting section.

Hash Function:

- Hashing is a cryptographic method that transforms any data type into a single text sequence. Any relational database, regardless of the size or form, can be hacked.
- The hash generated by any data has always been the same length irrespective of the size, form or complexity of the data.
- A hash is intended to be a one-way feature — you can accumulate information into a hacker algorithm and get a

single string, but you can't decode the data it contains until you get the current hash.

- In a more scientific context, it's a method that uses a statistical procedure to transform a different percentage of the input data into a remedied bitstring.
- The idea of a Hash function will take input data and use it to generate a single, nearly immutable, fixed-length output value.

How does Hash Function Work?

- Hash functions are widely used to monitor the credibility of the message and authenticating knowledge in the programming administrative controls.

- They are called cryptographically "weak," but cannot easily be deposited since they can be solved in polynomial times.
- Cryptographic hash capabilities apply authentication features to traditional hash functions, making it impossible to identify message content or receiver and sender information.

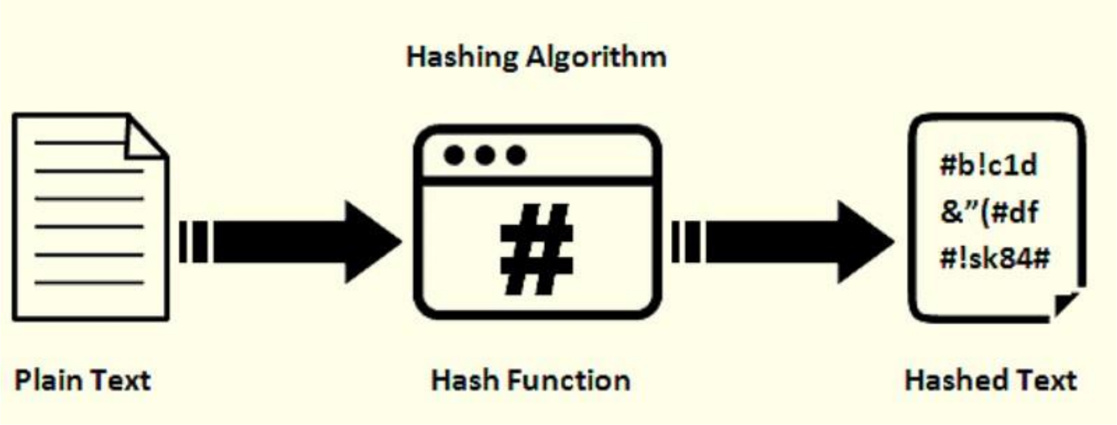
Characteristics Of Hash Function In Cryptography

1. Hashing is also regarded as a one-way function. That's due to the time and computing capital involved with that

since it's extremely unfeasible. This means without an unsustainable amount of money, you would not be able to work out the specific results gathered on the hash value.

2. There should not be two separate input data that produce the same hash value. It creates a so-called collision if they fit, implying that the formula is not safe to use. Further, Collision protection affects the durability of the hash and helps to preserve the data. That's perhaps because an intruder can not only break the hash value, but also the salt value.

Properties Of Hash Function In Cryptography



1.This phenomenon means it is difficult to modify a hash function algorithmically. This asset safeguards against an antagonist who only has a hash value and tries to locate the data.

2.This definition states that it is difficult to find another input with the same key given input and its hash. It defends against an offender with input and its hash value and tries to overwrite a numerical significance with a valid value instead of the original value.

Applications Of Hash Function In Cryptography

1. Password security defense is provided by hash functions. In place of saving passwords in plain, the hash values for passwords in the file are generally stored in all user account operations. And if you have entered the password, an outsider will be only the one to see the password hashing. You cannot either log in with hash or extract the hash value password as the hash feature has pre-image resistance characteristics.
2. Data integrity monitoring hash functions are the most general feature. It is used to generate data file compiled code. This program ensures the customer that the data is right. The honesty search lets the user spot modifications

to the original file. Nevertheless, it provides a little guarantee of originality. The intruder will update the whole file and together measure a new hash and send it to the recipient instead of changing file data. Only when the user knows what file originality is, is this integrity check program usable.

Hash and MAC algorithms

Hash algorithms are used to take a large message and produce a unique short digest o With a cryptographically strong hash function:

- Different data (usually) maps into different digest values.

•It is hard to find two different data sets that will produce the same hash value.
•It is hard to modify the data without changing the hash.
•It is hard to find data that will produce a given hash except by brute force.
Hashing provides a way to make sure that two messages are equal with a high level of confidence without the need to read the entire message. Only the digest of a message is signed for efficiency. It also allows ensuring that a received message was not changed after it was transmitted by the sender. Only the digest of a message is signed for efficiency.

Intel® DAL supports the one-way hashes:
•SHA-1
•SHA-256

•SHA-512

Message Authentication Code(MAC)

Message Authentication Code (MAC) algorithms are a sort of keyed hash. They take a message and a secret shared key and provide an output that can be authenticated by the other party to the key.
The advantage of MAC algorithms is that they are very very fast and can usually be easily offloaded to the hardware.
The disadvantages are that the hashed data cannot be retrieved and there is still a requirement for symmetric keys.

Intel DAL supports the symmetric signature algorithms (keyed hashes):
•HMAC-SHA1
•HMAC-SHA256

- HMAC-SHA512

LONG ANSWER QUESTIONS

1.Write in detail about Public-Key Cryptography?

2.Explain Euler’s Theorem.

3.Describe about D-H Key sharing technique.

4.Definr briefly about Hash and MAC algorithm.

5.Explain about RSA and its variants-Homomorphic Encryption Technique.

SHORT ANSWER QUESTIONS

1.Define Discrete logarithm.

2.Explain about message authentication.

3.Explain about Hash functions.

4.Describe Number Theory.

5.Explain about Primary and Factorization.

UNIT-4

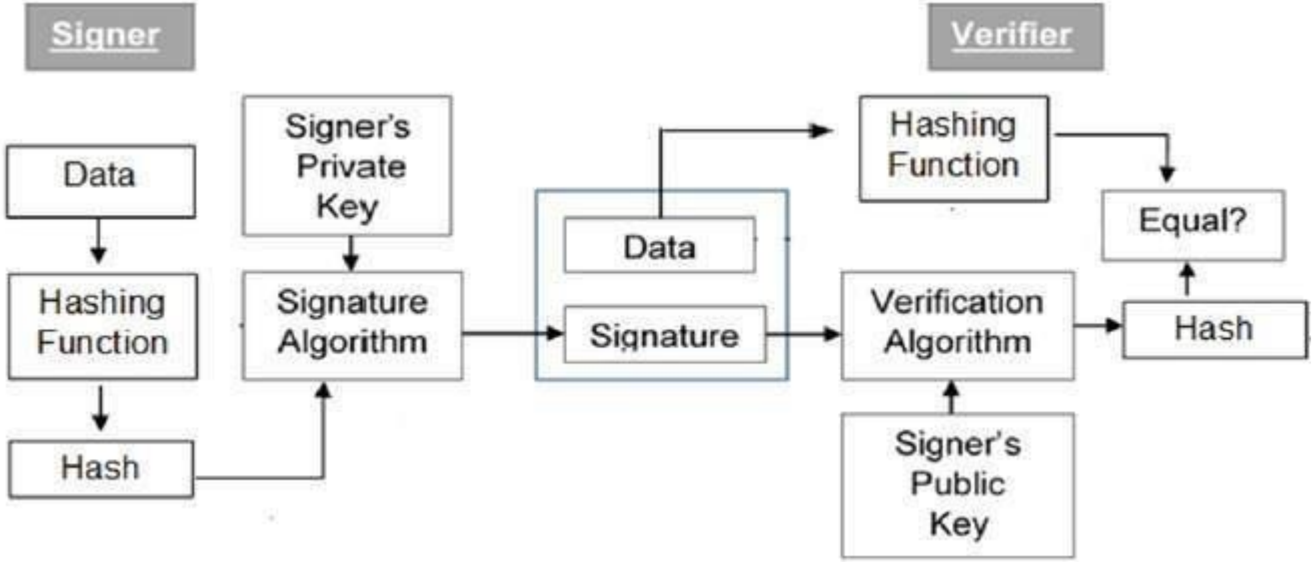
Digital Signatures:

- 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. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature:

- As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.

- Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

Importance of Digital Signature

- Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.
- Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the 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.

Authentication Protocols

- an authentication protocol is a communication protocol. It can be encrypted or designed to ensure the **safe transfer of authenticated data** between two or more different parties.
- In order to make it easier to understand, we can try employing an analogy: Let’s say that you want to transfer some money from one bank to another. In order to do this, you first need to complete the necessary documentation to prove that you are the rightful owner of that money.
- Then, you would need to find secure vehicles for the transportation process since you cannot put bankrolls on a handcart and merrily roll along.
- In addition, you would also need to ensure that the secure vehicles are not identifiable for the safety of your money. All in all, it is not a wise idea to carry large

sums of money out in the open or tell people the license plate number of your money loaded vehicles.

- Now, **cryptography and authentication processes** work very similarly: The necessary documentation you submit to the bank is user verification and authentication, secure vehicles are the authentication protocol and making sure that your money filled vehicles are unidentifiable is the encryption of data.

What are the types of authentication protocols?

- There are **various types of authentication protocols** that aim to answer different needs. Below you can find some of the most common authentication protocols and how they can be used.
- **Password authentication protocol:** Also known as the **PAP**, it is one of the most straightforward authentication protocols. The simplicity of this protocol stems from the fact that it transmits the

data in plain text. As a result, PAP is not a very durable against attacks.

- It is often used during testing processes of system simulations. Moreover, PAP can be employed when the software on the systems is incompatible with **various standard protocols** like **CHAP**.
- **Shiva password authentication protocol:** Also known as **SPAP**, this protocol is a more **primitive version of PAP**. SPAP processes the password through a **reversible encryption system**, that is why it is more secure than PAP.

- SPAP is used in certain situations when the sender party uses a Windows 2000 server or a Windows XP 2000 system

Digital signature Standard:

- As we have studied, signature is a way of authenticating the data coming from a trusted individual. Similarly, digital signature is a way of authenticating a digital data coming from a trusted source.
- **Digital Signature Standard (DSS)** is a Federal Information Processing Standard(FIPS) which defines

algorithms that are used to generate digital signatures with the help of Secure Hash Algorithm(SHA) for the authentication of electronic documents. DSS only provides us with the digital signature function and not with any encryption or key exchanging strategies.

Sender Side :

In DSS Approach, a hash code is generated out of the message and following inputs are given to the signature function – 1.The hash code.

2.The random number ‘k’ generated for that particular signature.

3.The private key of the sender i.e., PR(a).

4.A global public key(which is a set of parameters for the communicating principles) i.e., PU(g).

- These input to the function will provide us with the output signature containing two components – ‘s’ and ‘r’. Therefore, the original message concatenated with the signature is sent to the receiver.

Receiver Side :

At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs –

1. The hash code generated by the receiver.
2. Signature components ‘s’ and ‘r’.
3. Public key of the sender.
4. Global public key.

- The output of the verification function is compared with the signature component ‘r’. Both the values will match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.

Network Security Practice:

The International Standards Organization (ISO) developed the Open Systems Interconnect (OSI) model in 1981. It consists of seven functional layers that provide the basis for communication among computers over networks, as described in the table below. You can easily remember them using the mnemonic phrase “All people seem to need data processing.”
Understanding this model will help you build a strong network, troubleshoot problems, develop effective applications and evaluate third-party products.

Layer 7: Application	Provides services such as e-mail, file transfers and file servers	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, RLogin, BootP, MIME
Layer 6: Presentation	Provides encryption, code conversion and data formatting	MPEG, JPEG, TIFF
Layer 5: Session	Negotiates and establishes a connection with another computer	SQL, X- Window, ASP, DNA, SCP, NFS, RPC
Layer 4: Transport	Supports end-to-end delivery of data	TCP, UDP, SPX
Layer 3: Network	Performs packet routing	IP, OSPF, ICMP, RIP, ARP, RARP

Layer 2: Data link	Provides error checking and transfer of message frames	Ethernet, Token Ring, 802.11
Layer 1: Physical	Physically interfaces with transmission medium and sends data over the network	EIA RS-232, EIA RS-449, IEEE, 802

Understand Types of Network Devices

- To build a strong network and defend it, you need to understand the devices that comprise it. Here are the main types of network devices:
- Hubs connect multiple local area network (LAN) devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. Hubs do not perform packet filtering or addressing functions. Hubs operate at the Physical layer.
- Switches generally have a more intelligent role than hubs. Strands of LANs, are usually connected using switches. Mainly working at the Data Link layer, they read the packet

headers and process the packets appropriately. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

- Routers help transmit packets to their destinations by charting a path through the sea of interconnected network devices. They remove the packets from the incoming frames, analyze them individually and assign IP addresses. Routers normally work at the Network layer of the OSI model.
- Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. Bridges work only at the Physical and Data Link layers of the OSI model.
- Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous

protocols and standards from different vendors; gateways are used to deal with them.

Authentication Application:

- Authentication is the act of establishing identity via the presentation of information that allows the verifier to know the presenter is who or what it claims. This identity could be any number of things, including:

- People
- Systems

- Applications
- Messages

Types of Authentication

- There are many different types of authentication that can be used in an application. The selection of the most appropriate type of authentication will depend on the needs of the application; use this guide to determine which makes the most sense for your application.

- Basic, single-factor authentication
- Multi-factor authentication
- Cryptographic authentication

Basic Authentication

- Basic authentication is a commonly used term that most people probably understand already. It refers to password-based authentication. A password can be any information that is used to verify the identity of a presenter. Common examples that fall into this category are:
- The common password
- Host or system names
- Application names
- Numerical IDs

There are some important caveats when using basic authentication of which every developer should be aware:

- Passwords are commonly weakly specified
- Identities can be spoofed and impersonated
- Passwords can be susceptible to theft
- Requires considerable effort to provide strong security
- Can be difficult to scale across distributed and large environments

Multi-Factor Authentication:

Multi-factor authentication is the use of a combination of authentication methods to validate identity. The most commonly used description of multi-factor authentication is the use of information that is known only by the person, combined with something in his or her possession. These are typically

- The name and password
- Some form of token

A token is a hardware component that is used during the authentication process; it typically provides another piece of information that cannot be ascertained without physical control of the token. Different types of tokens used in multi-factor authentication are:

- Smart cards
- One-time password/phrases
- Single-use PINs or pseudo-random numbers
- Biometric information

Cryptographic Authentication:

The final form of authentication outlined here is that which utilizes cryptography. This includes the following forms:

- Public Key Authentication
- Digital Signatures

- Message Authentication Code
- Password permutation

Public key Authentication:

Public key authentication occurs when the owner of a key pair (private and public) communicates the public key, in some form, to the authenticating party, at which point it is verified to be true. There are a couple of methods for public key authentication worth discussing:

- The use of the public key itself
- Public key certificates

Electronic Mail:

Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as Email address. Different users can send and receive messages according to the e-mail address. E-mail is generally of the form username@domainname. For example,
webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by @ **(at)** symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

Advantages:

- E-mail has prooved to be powerful and reliable medium of commmunication. Here are the benefits of **E-mail:**
- Reliable
- Convenience
- Speed
- Inexpensive
- Printable
- Global
- Generality

Disadvantages:

- Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:
- Forgery
- Overload
- Misdirection
- Junk

- No response

Pretty Good Privacy (PGP):

- PGP stands for which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.

- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

IP Security:

- The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.
- **Uses of IP Security –**

-

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –

It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**

It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data’s confidentiality.

3. **Internet Key Exchange (IKE) –**

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.

5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

Web security:

- In general, web security refers to the protective measures and protocols that organizations adopt to protect the organization from, cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk

- Web security must be a critical priority for every organization. Along with email, the web is one of the top vectors for cyberattacks. The web and the use of DNS services specifically are part of 91% of all malware attacks, and email and web together are a key part for 99% of successful breaches.
- While the importance of web security is undisputed, protecting against web security threats grows more challenging each day. From thwarting attacks to dealing with limits in skills and resources, IT security departments face serious challenges when trying to secure the web.

Web security Threats:

- Web security threats are vulnerabilities within websites and applications, or attacks launched by malicious actors.
- Web security threats are designed to breach an organizations security defenses, enabling hackers and cyber criminals to control systems, access data and steal valuable resources.
- Common web security threats include malware, ransomware, cross-site scripting (XSS), SQL injection, phishing, denial of service and many others.

Intruders:

- Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access. Intruders are of three types, namely, masquerader, misfeasor and clandestine user.

- Masquerader is an external user who is not authorized to use a computer, and yet tries to gain privileges to access a legitimate user's account. Masquerading is generally done either using stolen IDs and passwords, or through bypassing authentication mechanisms.
- An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management

(SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Classification of Intrusion Detection System: IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS)**
2. **Host Intrusion Detection System (HIDS)**
3. **Protocol-based Intrusion Detection System (PIDS)**
4. **Application Protocol-based Intrusion Detection System (APIDS)**
5. **Hybrid Intrusion Detection System**

Viruses , Worms and Firewalls:

Virus:

- A Virus is a malicious software program that exists on local disk drives and spreads from one computer to another through sharing of "infected" files. Once installed on a computer, a virus may modify or remove applications and systems files.

Worm:

Acronym for a WORM - Write Once, Read Many times

- A worm is a computer virus capable of disrupting a computer program. It is a self-contained program that can propagate itself through systems or networks. Worms are often designed to use up available resources such as storage or processing time.

Firewall:

- A firewall is a type of protective layer between your computer(s) and the Internet. When used correctly, a firewall prevents unauthorized use of and access to your network.
- It analyzes the data that comes into and goes out of your computer. Based on the rules in the firewall, specific data may be blocked or discarded.
- Firewalls can be either hardware (a device) or software (a program). Your computer setup should include both. You may think of a firewall as something that only businesses need, but **if your computer can get to the Internet, you need a firewall!**
- Hardware firewalls are separate devices from your individual computer(s). They are often built into broadband modems and routers. If you have a broadband connection, check your documentation or contact your ISP to find out about your hardware firewall.
- Software firewalls are installed directly on each computer connected to the

Internet. Computers with Windows XP or higher can use the built-in Windows Firewall; Mac computers also come with a built-in firewall. Other firewall programs are available for most types of computers. Some firewalls are included with anti-virus or anti-spyware software.

LONG ANSWER QUESTIONS

1.Explain about Digital, Signatures and Authentication Protocols?

2.Describe about Network Security Practice?

3.Explain Authentication Applications.

4.Briefly Explain Electronic Mail Security.

5.Explain about Web Security.

SHORT ANSWER QUESTIONS

1.Define Intruders.

2.Explain about viruses and Worms.

3.What are the differences between Signatures and Authentication.

4.What is Network Security Practice.

5.What is Web Security.

UNIT-5

Mobile Security:

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

What is Mobile Device Security ?

- With more than half of business PCs are now mobile, portable devices present distinct challenges to network security,   which must account for all of the locations and uses that employees require of the company network. Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen. To avoid a security breach, companies should take clear, preventative steps to reduce the risk.

benefits of mobile device security

- Mobile device security, or mobile device management, provides the following:
- Regulatory compliance
- Security policy enforcement
- Support of “bring your own device” (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup

- Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.

How does mobile device security work?

- Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

To get started, here are some mobile security best practices:

1. Establish, share, and enforce clear policies and processes
2. Password protection
3. Leverage biometrics
4. Avoid public Wi-Fi
5. Beware of apps
6. Mobile device encryption:

Risk model

- **Cyber security risk modeling is the task of creating a variety of risk scenarios, assessing the severity of each, and quantifying the potential outcome if any scenario is realized – in a language that makes sense to your business.**

- Cyber risk modeling should not be confused with threat modeling. Threat model frameworks help identify cyber threats and vulnerabilities and inform and prioritize mitigation efforts. On the other hand, cyber risk modeling is an efficient and repeatable means of quantifying the likelihood of a cyber-attack. With this insight, your business can make robust decisions about where to focus investment for the greatest ROI.

Example of cyber security risk modeling

- One of the most impactful examples of cyber security risk modeling is the quantification of cyber risk in financial terms as opposed to business terms. By establishing a universal understanding of cyber risk across your organization you can develop a more mature cybersecurity program and lead meaningful conversations on the business impact of different cyber scenarios and cybersecurity investments.
- This analysis is not too different from the process of quantifying risk in a financial portfolio. For example, traders

and portfolio managers use risk models to analyze and anticipate the impact of future events on performance so they can make preemptive decisions about where to invest funds.

Ecosystem

- Since the world operates as a huge machine, cybersecurity ecosystem or security ecosystem are extremely invested in protecting users' benefit against cyberattacks. The consideration of cybersecurity and cyber threats are taken into account when severe malware attacks targeted company systems these days.

Cyber ecosystem

The cyber ecosystem is believed to adjust the relationship among participants within the cybersecurity infrastructure. In fact, you cannot ignore the interaction of linked entities in a cyber ecosystem that is remarkably similar to animals in the natural ecosystem. Accordingly, those individualities showed within the communication induce a vulnerable environment to unauthorized acts. Expressly, without a proper security level in the ecosystem, hackers could handily steal data, personal identities, and business secrets.

Service Risks

- The necessity for you to guard your business against cyber-attacks has never been more crucial as network security risks are continually on the rise. Regardless of whether your company's data and information are stored on a hard drive or sent through e-mails, being wary of network security risks, knowing how to prevent them, and hiring a managed IT security provider can help you alleviate any possible data breaches.

Most Common Network Security Risks

Here are some five most common network security threats you need to be vigilant about:

1. Phishing

- This type of online fraud is designed to steal sensitive information, such as credit card numbers and passwords. Phishing attacks impersonate reputable banking institutions, websites, and personal contacts, which come in the form of immediate phishing e-mails or messages designed to look legitimate.
- Once you click the URL or reply to the messages, you are prompted to enter your financial details or use your credentials, which then sends your data to the malicious source.

2. Computer Viruses

- These are pieces of software designed to spread from one computer device to another. Mostly they are downloaded from particular websites or sent as e-mail attachments with the intent of infecting your computer as well as other computers on your contact list through systems on your network. They can disable your security settings, send spam, steal and corrupt data from your computer, and even delete every single thing on your hard drive.
- 3. Malware/Ransomware

- Malware is a malicious software mostly used by criminals to hold your system, steal your confidential data, or install damaging programs in your device without your knowledge. It spreads spyware, Trojans, and worms through pop-up ads, infected files, bogus websites, or e-mail messages.
- On the other hand, ransomware is a type of malware where the cyber-criminals lock your device through a bad app or phishing emails then request a ransom to unlock the device. It can hinder you from running applications, encrypting your files, and even from completely using your device.

4. Rogue Security Software

- This is malicious software that deceives users by making them believe that their security measures are not up-to-the-minute or their computer has a virus. They then offer to help you install or update the user's security settings by asking you to pay for a tool or download their program to help do away with the alleged viruses. This can lead to the installation of actual malware in your device.
- 5. Denial-Of-Service Attack
- A denial-of-service attempts to hinder legitimate users from accessing services or information from a website. It happens when malicious attackers overload a website with traffic. It is carried out by one computer and its internet connection, which may enable the intruder to access your credentials. A distributed denial-of-service is similar to the denial-of-service but is harder to overcome. This is because it is launched from different computers that are distributed all over the globe. The network from these compromised computers is called a botnet.

How To Prevent Network Security Threats

- Never pay ransom to any individual
- Always identify any unusual traffic activity
- Reduce visits to unfamiliar websites
- Use authentication as well as strong passwords
- Be cautious of public Wi-Fi
- Keep your antivirus up-to-the-minute
- Employ the services of a managed IT security provider

A managed IT security provider can help you to remain ahead of the attackers by assisting you to:

- Identify the emerging trends in data sets
- Identify weaknesses in your network security infrastructure
- Provide cyber-security training to your team
- Help your business with compliance
- Carry out backups
- Update your cyber-security defences
- Enjoy 24 hours a day network monitoring to prevent any risks

App Risks

- Applications now play an integral role, with many businesses and users relying on a wide range of applications for work, education, entertainment, retail, and other uses.
- In this current reality, development teams play a key role in ensuring that applications can provide users great usability and performance as well as security from threat actors who are always on the lookout for weaknesses, vulnerabilities, misconfigurations, and other security gaps that they can abuse to conduct malicious activities.
- Security risks have become even more pronounced as organizations have had to rush applications to market in order to maintain business and revenue-generating processes.

Top security risks to applications:

- Using components with known vulnerabilities. ...
- Data leaks and exposure. ...
- Weak backend access controls. ...
- Injection. ...
- Security misconfiguration. ...
- Broken authentication and authorization. ...
- Cross-site scripting (XSS). ...
- Unsecure deserialization.

Counter measures:

- In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it
- Security countermeasures are **the controls used to protect the confidentiality, integrity, and availability of data and information systems**. ...
- These programs use a variety of techniques to scan and detect viruses, including signature scanning, heuristic scanning, integrity checks, and activity blocking.

Some Counter Measures:

Virus Scanners Antivirus programs can use one or more techniques to check files and applications for viruses. While virus programs didn’t exist as a concept until 1984, they are now a persistent and perennial problem, which makes maintaining antivirus software a requirement. These programs use a variety of techniques to scan and detect viruses, including signature scanning, heuristic scanning, integrity checks, and activity blocking.

Pretty Good Privacy (PGP) In 1991, Phil Zimmerman initially developed PGP as a free email security application, which also made it possible to encrypt files and folders. PGP works by using a public-private key system that uses the International Data Encryption Algorithm (IDEA) algorithm to encrypt files and email messages.

Secure Multipurpose Internet Mail Extensions (S/MIME) S/MME secures e-mail by using X.509 certificates for authentication. The Public Key Cryptographic Standard is used to provide encryption, and can work in one of two modes:

signed and *enveloped*. Signing provides integrity and authentication. Enveloped provides confidentiality, authentication, and integrity.

Privacy Enhanced Mail (PEM): PEM is an older e-mail security standard that provides encryption, authentication, and X.509 certificate-based key management.

Secure Shell (SSH): SSH is a secure application layer program with different security capabilities than FTP and Telnet. Like the two aforementioned programs, SSH allows users to remotely log into computers and access and move files. The design of SSH means that no cleartext usernames/passwords can be sent across the wire. All of the information flowing between the client and the server is encrypted, which means network security is greatly enhanced. Packets can still be sniffed but the information within the packets is encrypted.

Cloud computing Security:

- Cloud computing refers to the on demand delivery of computing services such as applications, computing resources, storage, database, networking resources etc. through internet and on a pay as per use basis. At the present time the demand for cloud computing services are increasing with respect to that demand for cloud computing skills is also increasing. It provides three main types of service models i.e. SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). With this as starting from small to large organizations have started using cloud services so depending upon their requirement they go for the different types of cloud like Public cloud, Private cloud, Hybrid cloud, Community cloud.

- Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks. Community Cloud : These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

Types of Cloud Computing Security Controls :

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of cloud computing:

- For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization’s infrastructure. Cloud security has a lot of benefits –
- **Centralized security :** Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- **Reduced costs :** Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration

- **Reduced Administration :** It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- **Reliability :** These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.
- Almost every organization has adopted cloud computing to varying degrees within their business. However, with this adoption of the cloud comes the need to ensure that the organization's cloud security strategy is capable of protecting against the top threats to cloud security.

- **Unauthorized Access**
- **Unauthorized Access**
- **Hijacking of Accounts**
- **Lack of Visibility**

- **External Sharing of Data**
- **Cyberattacks**

Denial of Service Attacks

- The cloud is essential to many organizations’ ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications.
- This means that a successful Denial of Service (DoS) attack against cloud infrastructure is likely to have a major impact on a number of different companies. As a result, DoS attacks

where the attacker demands a ransom to stop the attack a significant threat to an organization’s cloud-based resources.

LONG ANSWER QUESTIONS

1.Define briefly about service risks and app risks?

2.What are the importance of cloud computing.

3.What is block chain? Explain about working of Ethereum.

4.Describe Crypto Currency.

5.Write about Bit Coin Security?

SHORT ANSWER QUESTIONS

1.What is mobile device security.

2.What are the benefits of mobile device security.

3.What is risk model.

4.What is example of cyber security risk modeling?

5.Write about Threats in cloud computing.

INTERNAL EXAMINATIONS- I

SECTION- A

Answer any FIVE of the following **5*2=10M**

1.What is Cryptography?
2. Write a short note on Conventional Encryption Model.
3. Define Steganography?
4. What is DES?
5. Write a short note on Conventional Encryption Algorithms?
6. Describe IDE Algorithm.
7. What is Blowfish.

8. Define RC5

SECTION-B

Answer any one question from each unit 2*10=20M

UNIT-I

9.Explain in detail about Classical Encryption Techniques.

(OR)

10.Write the differences between Block Cipher Design Principles and Modes of Operation.

UNIT-II

11.Define Cryptography? Explain what is Confidentiality using Conventional Encryption.

(OR)

12.Explain the Characteristics of Advanced Symmetric Block Ciphers.

INTERNAL EXAMINATIONS- II

SECTION-A

Answer any FIVE of the following 5*2=10M

1.What is Public-Key Cryptography?
2. Define Introduction to Number Theory.
3. What is Modular Arithmetic?
4. Differentiate between Primary and Factorization Algorithms.
5. What is Authentication Protocol?
6. Define Digital Signature Standard.

7. Write a short note on Network Security Practice.
8. What are the applications of Authentication.

SECTION-B

Answer any one question from each unit 2*10=20M

UNIT-I

9. Explain about Euler's Theorem?

(OR)

10. Explain about Message Authentication and Hash Function.

UNIT-II

11. Define Signature. Write a detailed note on Protocols.

(OR)

12. what is MIME.

External Examination

SECTION- A

Answer any FIVE of the following 5*2=10M

1.What is Cryptography?
2. Write a short note on Conventional Encryption Model.
3. Write a short note on Conventional Encryption Algorithms?
4. Describe IDE Algorithm.
5. What is Modular Arithmetic?
6. Differentiate between Primary and Factorization.

7. Write a short note on Network Security Practice.
8. What are the applications of Authentication.

SECTION-B

Answer any one question from each unit. 1*12=12M

UNIT-I

9. Explain in detail about Classical Encryption Techniques.

(OR)

10.Write the differences between Block Cipher Design Principles and Modes of Operation.

UNIT-II

11. Define Cryptography? Explain what is Confidentiality using Conventional Encryption.

(OR)

12. Explain the Characteristics of Advanced Symmetric Block Ciphers.

UNIT-III

13. Explain about Euler's Theorem?

(OR)

14. Explain about Message Authentication and Hash Function.

UNIT-IV

15. Define Signature. Write a detailed note on Protocols.

(OR)

16. what is MIME.

UNIT-V

17. What is Risk Model. Define types of Risks.

(OR)

18. What is Block Chain. Explain about the working of Ethereum.