DEPARTMENT ON INFORMATION TECHNOLOGY
CS6701-CRYPTOGRAPHY AND NETWORK SECURITY
UNIT-I INTRODUCTION & NUMBER THEORY

1. Define security attack, security mechanism and security services.

Security attack: any action that compromises the security of information owned by an organization.

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

Security services: a service that enhances the security of the data processing systems and the information transfers of an organization

2.Mention the different types of security services.

Authentication

Confidentiality

Data integrity

Non repudiation

Access control

Availability

3.Specify the categories of security threads?

Interruption

Interception

Modification

Fabrication

4.What are the essential ingredients of a symmetric cipher?

A symmetric cipher encryption has five ingredients. They are:

Plaintext

Encryption algorithm

Secret key

Cipher text

Decryption algorithm

5.What are the two basic functions used in encryption algorithms?

The two basic functions used in encryption algorithms are

Substitution

Transposition

6. How many keys are required for two people to communicate via a cipher?

If both sender and receiver se the same key, the system is referred to as symmetric, single key, secret key, or conventional encryption. If the sender and receiver e ch use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.

7.What is the difference between a block cipher and a stream cipher?

A block cipher processes the input one block of elements at a time, producing an output block for each input block.

A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

8.What are the two approaches to attacking a cipher?

The two approaches to attack a cipher are:

- Cryptanalysis
- Brute-force attack

9.Briefly define the Caesar cipher.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example:

Plain: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

10.Briefly define the monoalphabetic cipher, playfair cipher and transposition cipher

MonoalphabeticCipher:Its maps from a plain alphabet to cipher alphabet. Here a single cipher alphabet is used per message.

PlayfairCipher:The best-known multiple-letter encryption cipher is the playfair, which treats diagrams in the plain text as single units and translates these units into cipher text diagrams.

Transposition cipher:It is a cipher, which is achieved by performing some sort of permutation on the plaintext letters.

11.What are the two problems with one-time pad?

It makes the problem of making large quantities of random keys.

It also makes the problem of key distribution and protection.

12. What is Steganography?Mention few techniques init.

It is the art of hiding the information. This conceals the existence of the message.Techniques are:

Character marking

Invisible ink

Pin punctures

Typewriter correction ribbon

13.Why is it not practical to use an arbitrary reversible substitution cipher?

An arbitrary reversible cipher for a large block size is not practical, however, from an implementation and performance point of view. Here the mapping itself is the key.

14.What is the difference between diffusion and confusion?

Diffusion:

It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext.

Confusion:

It can be achieved by substitution algorithm. It is the relationship between ciphertext and key.

15.What is the difference between a mono alphabetic cipher and a poly alphabetic cipher?

Mono alphabetic cipher: Here a single cipher alphabet is used.

Poly alphabetic cipher: Here a set of related mono alphabetic substitution rules is used.

16.List the types of cryptanalytic attacks.

 Cipher text only Known plaintext Chosen plaintext Chosen cipher text Chosen text

17. Differentiate symmetric and asymmetric encryption?

Symmetric: A single key is used for both the encryption and decryption

Asymmetric: More than one keys are used for both the encryption and decryption

18. Define integrity and nonrepudiation?

Integrity:Service that ensures that only authorized person able to modify the message.

Non-repudiation:This service helps to prove that the person who denies the transaction is true or false.

19. Explain active and passive attack with example.

Passive attack: Monitoring the message during transmission. Eg: Interception

Active attack:It involves the modification of data stream or creation of false data stream.E.g.: Fabrication, Modification, and Interruption

20.Definecryptanalysis,cryptology and cryptography?

Cryptanalysis: techniques used for deciphering or decrypting a message without the knowledge of the enciphering or encrypting details is said to be cryptanalysis.

Cryptology: the study of cryptography and cryptanalysis together is called cryptology.

Cryptography:It is a science of writing Secret code using mathematical techniques. The many schemes used for enciphering constitute the area of study known as cryptography.

21. Specify the components of encryption algorithm.

1. Plaintext
2. Encryption algorithm
3. secret key
4. ciphertext
5. Decryption algorithm

22.Define confidentiality and authentication.

Confidentiality:

It means how to maintain the secrecy of me age It ensures that the information in a computer system and tran mitted information are accessible only for reading by autherised person.

Authentication:

It helps to prove that the source entity only has involved the Transaction.

23. Compare Substitution and Transposition techniques.

Substitution Technique	Transposition Technique
Substitution Technique is one in which the letters of the in text are replaced by other letter or by number or symbols Ceaser Cipher	It means different kind of mapping is achieved by performin some sort of permutation on the plaintext letters DES,AES

24. Differentiate unconditionally secure and computationally secure?

An encryption scheme is unconditionally secure if the cipher text generated by the encryption scheme doesn't contain enough information to determine corresponding plaintext.

An encryption scheme is computationally secure means,

1.The cost of breaking the cipher exceeds the value of the encrypted information.

2.The time required to break the cipher exceeds the useful lifetime of the information.

25.Give the relation between security services and security mechanisms

rity Service	**rity Mechanism**
confidentiality	pherment and routing control

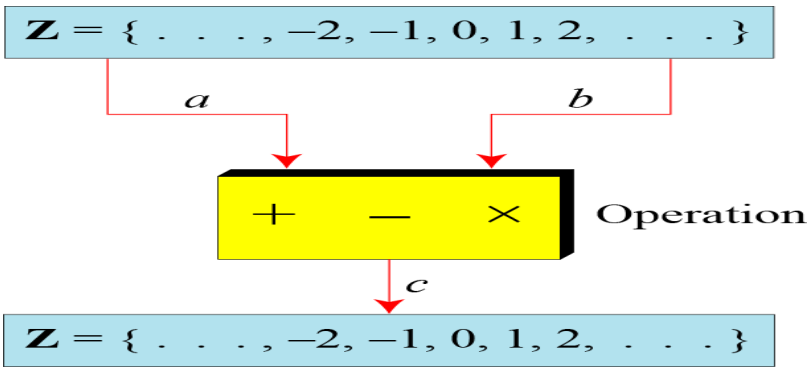
integrity	pherment, digital signature,data integrity
ıentication	pherment, digital signature, authentication ges
repudiation	tal signature, dataintegrity, Notarization
ess Control	ess Control mechanism

26.Define set of integers

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity.

$$Z=\{\ldots\ldots\ldots,-2,-1,0,1,2,\ldots\ldots\}$$

27.Draw the three binary operations for the set of integers

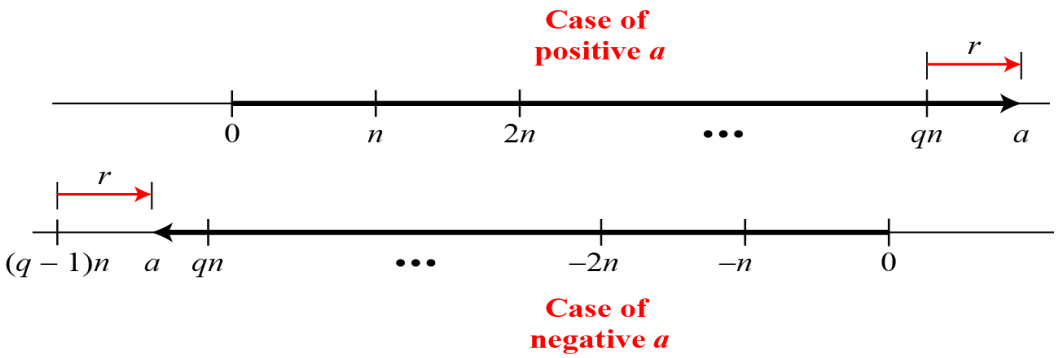


28.Define integer division

In integer arithmetic, if we divide a by n, we can get qAndr . The relationship between these four integers can be shown as

a=qxn+r

29.Draw the graph of division algorithm



30.Define divisibility

If a is not zero and we let r = 0 in the division relation, we get

a=qxn

- If the remainder is not zero,
- If the remainder is zero, a/n

31.Write the properties of divisibility

Property 1: if a|1, then a = ±1.

Property 2: if a|b and b|a, then a = ±b.

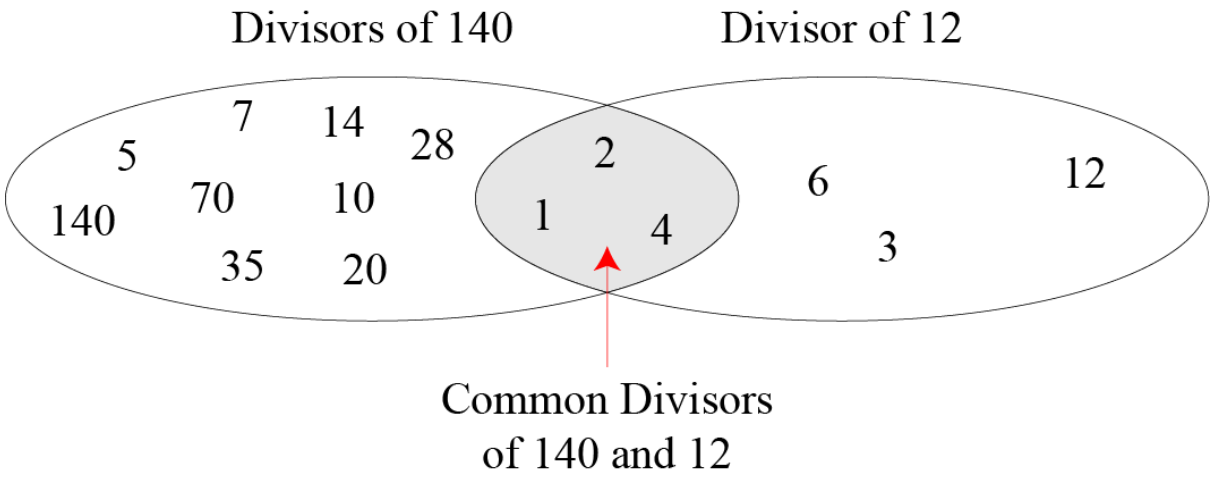
Property 3: if a|b and b|c, then a|c.

Property 4: if a|b and a|c, then

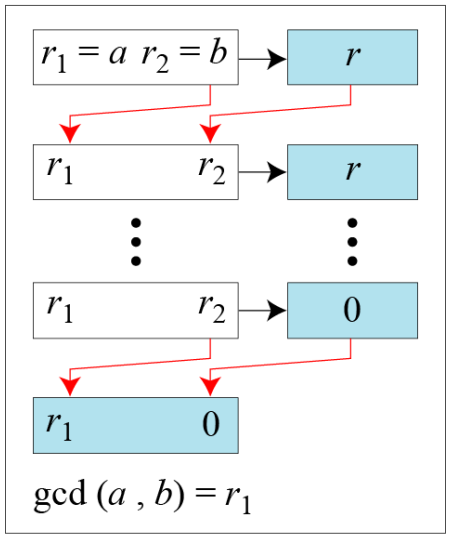
a|(m × b + n × c), where m

and n are arbitrary integers

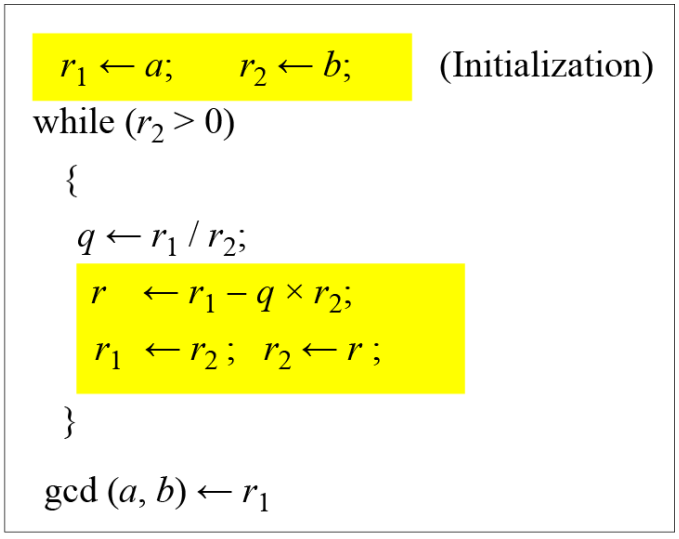
32.Find the GCD of 140 and 12



33.Draw the Euclidean algorithm and also write the steps



a. Process



b. Algorithm

Fact 1:gcd (a, 0) = a

Fact 2:gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

34. Define Extended Euclidean algorithm

Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

$$s \times a + t \times b = \gcd(a, b)$$

The extended Euclidean algorithm can calculate the gcd (*a*, *b*) and at the same time calculate the value of *s* and *t*.

35. Write the particular solution and general solution of linear Diophantine equation?

Particular solution:

$x_0 = (c/d)s$ and $y_0 = (c/d)t$

General solutions:

$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$ where k is an integer

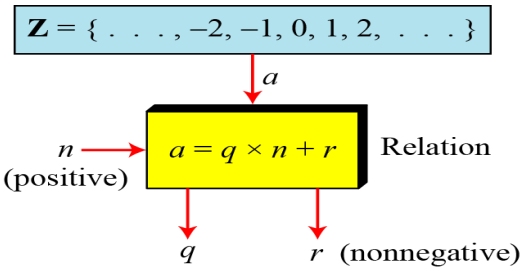
36. Find the particular and general solutions to the equation ?

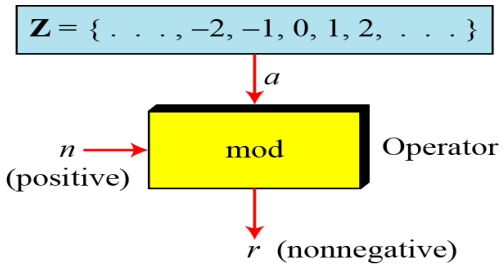
21x + 14y = 35.

$$\text{Particular: } x_0 = 5 \times 1 = 5 \quad \text{and} \quad y_0 = 5 \times (-1) = -5$$
$$\text{General: } x = 5 + k \times 2 \quad \text{and} \quad y = -5 - k \times 3$$

37. What is modulo operator?

The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.





38. Define set of residues?

The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$\mathbf{Z}_2 = \{ 0, 1 \}$ $\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$ $\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$

39. Perform the following operations(the inputs come from Zn):

a.Add to 14 in Z15.

b.Subtract 11 from 7 in Z13.

c.Multiply 11 by 7 in Z20.

$$(14+7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7-11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

40. Define additive inverse and multiple inverse

Additive inverse:In Z_n, two numbers *a* and *b* are additive inverses of each other if

a+b≡0(mod n)

Multiple inverse:In Z_n, two numbers *a* and *b* are the multiplicative inverse of each other if

a+b≡1(mod n)

41. Find all additive inverse pairs in Z10.

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

42. Say about Euler's phi function

It is sometimes called as Euler's totientfunction.The function finds the number of integers that are both smaller than n and relatively prime to n.The function φ(n) calculates the number of elements in this set.The following helps to find the value of φ(n).

1.φ(1)=0

2.φ(p)=p-1 if p is prime

3.φ(m*n)= φ(m)* φ(n) if m and n are relatively prime

4.$\varphi(p^e) = p^e - p^{e-1}$ if p is a prime.

43. Tell about Fermat's little theorem

Fermat's little theorem plays a very important role in cryptography.The two versions of this theorem are

First version: It says that p is a prime and a is an integer such that p does not divide a then $a^{p-1} \equiv a \bmod p$

Second version: It removes the condition on a.It says that if p is a prime and a is an integer,then$a^p \equiv a \bmod p$

44. Tell about Euler's theorem?

Euler's theorem can be thought of as a generalization of Fermat's little theorem. The modulus Fermat's little theorem is a prime, the modulus in Euler's theorems an integer

First version: The First version of Euler's theorem is similar to the First version of the Fermat's little theorem.If a and n are coprime,then$a^{\varphi(n)} \equiv 1 \pmod n$

Second version: The Second version of Euler's theorem is similar to the Secondversion of the Fermat's little theorem;it removes the condition that a and n should be coprime.If n-=p*q,a<n,and k an integer, then $a^{k* \varphi(n)+1} \equiv a \pmod n$

45. Give the formula for Mersenne primes and fermat primes

Mersenne defined the formula called Mersenne numbers that are used to enumerate all primes.

$M_p=2^p-1$

Fermat tries to find a formula to generate primes.

$F_n=2^{2n}+1$

46. Properties of congruence theorem

Let m be a positive integer and let a, b, c, d be integers. Then

1. $a \equiv a \bmod m$
2. If $a \equiv b \bmod m$, then $b \equiv a \bmod m$.
3. If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$.
4. (a) If $a \equiv qm + r \bmod m$, then $a \equiv r \bmod m$.

   (b) Every integer a is congruent mod m to exactly one of $0, 1, \ldots, m - 1$.
5. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then

$a \pm c \equiv b \pm d \bmod m$ and $ac \equiv bd \bmod m$.

5'. If $a \equiv b \bmod m$, then$a \pm c \equiv b \pm c \bmod m$ and $ac \equiv bc \bmod m$.

5''. If $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$ for any $n \in Z+$.

6. If $(c, m) = 1$ and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m$.

47. Find all solutions to each of the following congruences:

1.$2x \equiv 1 \bmod 3$.

2.$3x \equiv 4 \bmod 8$.

3.$6x \equiv 3 \bmod 15$.

4.$8x \equiv 7 \bmod 18$.

5.$9x + 23 \equiv 28 \bmod 25$.

Solution:(i) We first note that $(2, 3) = 1$. Therefore we can apply the theorem above. Since $2 \cdot 2 \equiv 1 \bmod 3$, we get $x \equiv 1 \cdot 2 \equiv 2 \bmod 3$.

(ii) We first note that $(3, 8) = 1$. Therefore we can apply the theorem above. Since $3 \cdot 3 \equiv 1 \bmod 8$, we get $x \equiv 4 \cdot 3 \equiv 12 \equiv 4 \bmod 8$.

(iii) Since (6, 15) = 3, we can't apply the theorem above directly again. However, canceling out 3, we obtain $2x \equiv 1 \bmod 5$. Note that (2, 5) = 1. Therefore we can apply the theorem above to the new equation. Since $2 \cdot 3 \equiv 1 \bmod 5$, we get $x \equiv 1 \cdot 3 \equiv 3 \bmod 5$.

(iv) Since (8, 18) = 2, we can't apply the theorem above directly. We now note that $8x \equiv 7 \bmod 18$ is equivalent to $8x - 18y = 7$, which is impossible, since the left-hand side is divisible by 2,whereas the right-hand side is not. So, this equation has no solutions.

(v) We first rewrite this congruence as $9x \equiv 5 \bmod 25$. Note that (9, 25) = 1. Therefore wecan apply the theorem above. Since $9 \cdot 14 \equiv 1 \bmod 25$, we get $x \equiv 5 \cdot 14 \equiv 70 \equiv 20 \bmod 25$.

48. What is the last digit of 4321^{4321}?

Solution: It is obvious that $4321 \equiv 1 \bmod 10$, therefore by property 5" we have $4321^{4321} \equiv 1^{4321} \equiv 1 \bmod 10$. This means that the last digit is 1.

49. Prove that there is no perfect square a2which is congruent to 2 mod 4.

By the property 4(a) each integer number is congruent to 0, 1, 2, or 3 mod 4. Consider all these cases and use property 5":If $a \equiv 0 \bmod 4$,

then $a^2 \equiv 0^2 \equiv 0 \bmod 4$.

If $a \equiv 1 \bmod 4$, then $a^2 \equiv 1^2 \equiv 1 \bmod 4$.

If $a \equiv 2 \bmod 4$, then $a^2 \equiv 2^2 \equiv 0 \bmod 4$.

If $a \equiv 3 \bmod 4$, then $a^2 \equiv 3^2 \equiv 1 \bmod 4$.

So, $a^2 \equiv 0$ or $1 \bmod 4$. Therefore a^{26}not congruent to 2 mod 4

50. Prove that the following equations have no solutions in integer numbers:

$x^2 - 3y = 5$

Solution: Rewrite this equation as $x^2 = 3y + 5$, which means that $x^2 \equiv 5 \equiv 2 \bmod 3$. By theproperty 4(a) each integer number is congruent to 0, 1, or 2 mod 3. Consider all these cases and useproperty 5":

If $a \equiv 0 \bmod 3$, then $a^2 \equiv 0^2 \equiv 0 \bmod 3$.

If $a \equiv 1 \bmod 3$, then $a^2 \equiv 1^2 \equiv 1 \bmod 3$.

If $a \equiv 2 \bmod 4$, then $a^2 \equiv 2^2 \equiv 1 \bmod 3$.

So, $a^2 \equiv 0$ or $1 \bmod 3$. Therefore a^{26} not congruent to 2 mod 3

51.What is the remainder after dividing $3^{50}$by 7?

By Fermat's Little theorem we have $3^6 \equiv 1 \bmod 7$, therefore by property 5" we get $3^{6 \cdot 8} \equiv 1^{48} \equiv 1 \bmod 7$, therefore $3^{50} \equiv 9 \equiv 2 \bmod 7$.6

52. Find all solutions of the following congruence $2x \equiv 5 \bmod 8$.

Solution: Since (2, 8) = 2, we can't apply the theorem above directly. We now note that $2x \equiv 5 \mod 8$is equivalent to $2x - 8y = 5$, which is impossible, since the left-hand side is divisible by 2, whereas theright-hand side is not. So, this equation has no solutions.

53. Write about Miller rabin test and pollard rho method?

The miller Rabin algorithm is used for testing whether a given number is prime. In fact we shall consider the decisional problem, ***IsComposite***, to decide whether a given number is composite.

IsComposite

Input: A positive integer n>=2

Yes-No problem: Is n composite?

pollard rho method: Pollard developed second method for factorization. The pollard rho is based on the following points. Assume that there are two integers x_1 and x_2 such that p divides x_1-x_2, but n does not.It can be proven that p=gcd(x_1-x_2, n) because p divides x_1-x_2, it can be written as x_1-x_2 =q*p but because n does not divide x_1-x_2, it is obvious that q does not divide n. This means that gcd(x_1-x_2, n) is either 1 or a facyor of n.

54. What is Fermat method?

The fermat factorization method divides a number into two positive integers a and b so that n=a*b.

55. What are the two efficient methods devised for factorization methods?

Quadratic sieve. Its complexity is $O(e^C)$, where $C=(\ln n \ln\ln n)^{1/2}$

Number field sieve. Its complexity is $O(e^C)$, where $C=2(\ln n)^{1/3}(\ln\ln n)^{2/3}$

56.Define Chinese remainder theorem and its applications

The CRT is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime as given below

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

....

$x \equiv a_k \pmod{m_k}$

Applications: It has several applications in cryptography. One is to solve quadratic congruence the other is to represent very large integer interms of a list of small integers.

PART B

1.Briefly discuss about Substitution and transposition techniques

2.Briefly explain about group,ring and field

3.Determine gcd(1970,1066)

4.Explain Fermat's Theorm and also about Euler totient function

5.Describe and illustrate Chinese Remainder Theorem

6.Find all the primitive roots of 25

UNIT-II: BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

1. Define Product cipher.

It means two or more basic cipher are combined and it produce the

resultant cipher is called the product cipher.

2. Explain Avalanche effect.

A desirable property of any encryption algorithm is that a s all change in either the plaintext or the key produces a significant change in the ciphertext. In particular, a change in one bit of the plaintext r ne bit of the key should produce a change in many bits of the iphertext.

3. Give the five modes of operation of Block cipher

1. Electronic Codebook(ECB)
2. Cipher Block Chaining(CBC)
3. Cipher Feedback(CFB)
4. Output Feedback(OFB)
5. Counter(CTR)

4. State advantages of counter mode.

*Hardware Efficiency *Software Efficiency *Preprocessing

*Random Access

* Provable Security *Simplicity

5. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times. Eg: Double DES, Triple DES

6. Specify the design criteria of block cipher.

Number of rounds

Design of the function F

Key scheduling

7. Define Reversible mapping.

Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.

8. Specify the basic task for defining a security service

A service that enhances the security of the data processing systems and the information transfer of an organization.The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.

9. What is the difference between link and end to end encryption?

Link Encryption

1. With link encryption, each vulnerable the Communications link is equipped on encryption.
2. Transperant to ser
3. Provides host authentication
4. Can be done in hardware
5. One facility for ll users

End to End Encryption

1. With end to end encryption, the encryption process is carried out at the t o end system.
2. User applies encryption
3. Provides user authentication
4. Software implementations
5. Users selects encryption scheme

10. What is traffic Padding? What is its purpose?

Traffic padding produces ciphertext output continuously, even in the absence of the plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible to for an attacker to distinguish between true dataflow and padding and therefore impossible to deduce the amount of traffic.

11. List the evaluation criteria defined by NIST for AES?

The evaluation criteria for AES is as follows: 1.Security

2. Cost

3. Algorithm and implementation characteristics

12. What is Triple Encryption? How many keys are used in triple encryption?

Triple Encryption is a technique in which encryption algorithm is performed three times sing three keys.

13. What is the purpose of the State array?

A single 128-bit block is depicted as a square matrix of bytes. This block is copied into the St terr y, which is modified at each stage of encryption or decryption After the final stage, State is copied to an output matrix.

14. How is the S-box constructed?

The S-box is constructed in the following fashion: Initialize the S-box ith the byte values in ascending sequence row by row. The first row contains {00}, {01}, {02}, ……., {0F}; the second row contains{10},{11},etc; and so on. Thus, the value of the byte at row x, column y is {x y}. Map each byte in the S-box to its multiplicative inverse in the finite field GF (28); the value {00} is mapped to itself. Consider that each byte in the S-box consists of 8 bits labeled (b7,b6,b5,b4,b3,b2,b1,b0).Apply the following transformation to each bit of each byte in the S-box.

15. Briefly describe Sub Bytes.

Sub byte uses an S-box to perform a byte-by-byte substitution f the block. The left most 4 bits of the byte are used as row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8- bit value.

16. Briefly describe Shift Rows .

In shift row, a row shift moves an individual by e from one column to another, which is a linear distance of a multiple of 4 bytes. In Forward Shift Row, each row perform circular left shift. Second Row a 1-byte circular left shift is performed. Third Row a 2-byte circular left shift is performed. For the Fourth Row a 3-byte circular left shift is performed. In Inverse Shift Row, each row perform circular right shift.

17. How many bytes in State are affected by Shift Rows?

Totally 6-bytes in state are affected by Shift Rows.

18. Briefly describe Mix Columns.

Mix Column is substitution that makes use of arithmetic over GF(28).Mix Column operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The Mix Column Transformation combined with the shift row transformation ensures that after a few rounds, all output bits depend on all input bits.

19. Briefly describe Add Round Key.

In Add Round Key, the 128 bits of State are bit wise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation. The Add Round Key transformation is as simple as possible and affects every bit f State.

20. Briefly describe the Key Expansion Algorithm

The AES key expansion algorithm takes as input a 4-word(16-byte) key and produces a linear array of 44 words(156 byt). This is ufficient to provide a 4-word round key for the initial Add Round K y stage and each of the 10 rounds of the cipher.

21. What is the difference between Sub Bytes and Sub Word? Sub Bytes:

Sub Bytes uses an S-box toperform a byte-by-byte substitution of the
block.

Sub Word:

Sub Word performs byte substitution on each byte of its input word,using the Sbox

22. What is the difference between Shift Rows and Rot Word? Shift Rows:

Shift Row is simple permutation. It shifts the rows circularly left or

right.

Rot Word:

Rot word performs a one-byte circular left shift on a word. This means that an input word [b0,b1,b2,b3] is transformed into [b1,b2,b3,b0].

23 . Why do some block cipher modes of operation only use

encryption while others use both encryption and decryption?

Some block cipher modes of operation only use encryption because the input is set to some initialization vector and the leftmost bits of the output of the encryption function are XORed with the first segment of plain text p1 to produce the first unit of cipher text C1 and it is transmitted. While in decryption, the cipher text is XORed with the output of the en rypti n function to produce the plain text.

24. What is triple encryption?

Tuchman proposed a triple encryption m hod hat uses only two keys [TUCH79]. The function follows an encrypt – decrypt – encrypt (EDE) sequence. C=E [D [E [P]]]

k1 k2 k1

There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES:

C=E [D [E [P]]] = E [P] k1 k2 k1 k1

25. What is a meet-in-the-middle attack?

If we have

C=E [E [P]] k2 k1 Then

X=E [P]=D [C]

Given a known pair, (P,C), the attack proceeds as follows. First, encrypt P for all 2 possible values of K . Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 2 possible values of K. As each decryption is produced, check the result against the table for a match.If a match occurs, then test the two resulting keys against a new known plaintext-ciphertext pair.

27. List important design considerations for a stream cipher.

The encyption sequence should have a large period. The keystream should approximate the properties of a true random number stream as close as possible. Theoutput of the pseudorandom number generator is nditined on the value of the input key.

28. Why is it not desirable to reuse a stream cipher key?

If two plaintexts are encrypted with the ame key using a stream cipher then cryptanalysis is often quite simple. If he two ciphertext streams are XORed together the result is the XOR of he original plaintexts. So it is not desirable to reuse a stream cipher key.

29. What is the difference between Rijn ael and AES?

AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.

30. Why is the middle portion of 3DES a decryption rather than an encryption?

Decryption requires that the keys be applied in reverse order: This results in a dramatic increase in cryptographic strength.

The use of DES results in a mapping that is not equivalent to a single DES encryption.

31. What is the difference between the AES decryption algorithm and the equivalent inverse cipher?

In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes.

PART-B

1.What are the criteria used while designing the DES algorithm?

2.Describe the block modes of operations of DES with their advantages.

3.Explain simplified DES with example.

4.Explain RSA algorithm with an example.

5.Give brief note on Elliptic curve cryptosystem.

6.Explain briefly about Diffie Hellman Key Exchange.

UNIT-III:HASH FUNCTIONS AND DIGITAL SIGNATURES

1. What is message authentication?

It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

2. Define the classes of message authentication function.

Message encryption: The entire cipher text would be used for authentication.

Message Authentication Code: It is a function of message and secret key produce a fixed length value.

Hash function: Some function that map a message of any length to fixed length which serves as authentication.

3. What are the requirements for message authentication?

The requirements for message authentication are

Disclosure: Release of message contents to any person or process not processing the appropriate cryptographic key

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.

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 acknowledgements of message receipt or no receipt 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 modification.

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 connectionless application, an individual message could be delayed or replayed.

Source repudiation: Denial of transmission of message by source.

Destination repudiation: Denial of receipt of message by destination.

4.What you meant by hash function?

Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

5. Differentiate MAC and Hash function?

MAC: In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the sourceat a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. Thehash function itself not considered to be secret.

6. Any three hash algorithm.

MD5 (Message Digest version 5) algorithm.

SHA_1 (Secure Hash Algorithm).

RIPEMD_160 algorithm.

7. What are the requirements of the hash function?

H can be applied to a block of data of any size.

H produces a fixed length output.

H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

8. What you meant by MAC?

MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC.

MAC = CK(M)

Where M = variable length message

K = secret key shared by sender and receiver.

CK(M)= fixed length authenticator.

Where M= variable length message

K = secret key shared by sender and receiver.

CK(M)= fixed length authenticator.

9. Differentiate internal and external error control.

Internal error control: An error detecting code also known as frame check sequence or checksum.

External error control: Anerror detecting codes are appended after encryption.

10. What is the meet in the middle attack?

This is the cryptanalytic attack that attempts to find the value in each ofthe range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.

11. What is the role of compression function in hash function?

The hash algorithm involves repeated use of a compression function f, thattakes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value usually b>n; hence the term compression.

12. What is the difference between weak and strong collision resistance?

k collision resistance	**ng collision resistance**

ny given block x, it is computationally infeasible y = x with/H(y)=H(x)	computationally infeasible to find any pair (x,y) that H(x)=H(y)
proportional to 2n	proportional to 2 n/2

13. Compare MD5, SHA1 and RIPEMD-160 algorithm.

	MD5	**SHA-1**	**RIPEMD160**
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
No of steps	64(4 rounds of 16)	(4 rounds of 20)	(5 paired rounds of 16)
Maximum message size		-1 bits	^64-1 bits
Primitive logical function			
Additive constants used			
Endianess	Little Endian	Big Endian	Little Endian

14.Write Short notes on MD5.

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

15. Write Short notes on SHA(Secure Hash Algorithm).

The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

16. Distinguish between direct and arbitrated digital signature?

ct Digital Signature	**itrated Digital Signature**
direct digital signature involves only the municating parties.	arbiter plays a sensitive and crucial role in this al signature
may be formed by encrypting the entire message the sender's private key	y signed message from a sender x to a receiver y first to an arbiter A, who subjects the message an gnature to a number of tests to check its origin an ent.

17. What are the properties a digital signature should have?

It must verify the author and the data and time of signature.

It must authenticate the contents at the time of signature.

It must be verifiable by third parties to resolve disputes.

18. What requirements should a digital signature scheme should satisfy?

The signature must be bit pattern that depends on themessage being signed.

The signature must use some information unique to the sender, to prevent both forgery and denial.

It must be relatively easy to produce the digital signature.

It must be relatively easy to recognize and verify the digital signature.

It must be computationally infeasible to forge a digitalsignature, either by constructing a new message for an existing digital signature or by constructing a fraudulentdigital signature for a given message.

It must be practical to retain a copy of the digital signaturein storage.

19.What is Digital Signature?

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

20.List the Digital Signature Algorithms.

RSA

ElGamal

DSA

21.What is Birthday attack ?

This cryptanalytic attack attempts to find two values in the domain of a function that map to the same value in its range

22.DefineElGamal Public Key Cryptosystem.

ElGamal Public Key Cryptosystem is an asymmetric key encryption for public key cryptography based on Diffie-Hellman Key Exchange

23. What is one way function?

One way function is one that map the domain into a range such that every function value has a unique inverse with a condition that the calculation of the function is easy where as the calculations of the inverse is infeasible.

24.DefineSchnorr?

Schnorr Digital Signatures also uses exponentiation in a finite (Galois)security based on discrete logarithms, as in D-H.Minimizes message dependent computation : multiplying a 2n-bit integer with an n-bit integer.Main work can be done in idle time using a prime modulus p – p–1 has a prime factor q of

appropriate size – typically p 1024-bit and q 160-bit numbers

25.What are the attacks in DSS?

Key-only attack: Adversary knows only the verification function (which is supposed to be public).

Known message attack: Adversary knows a list of messages previously signed by Alice.

Chosen message attack: Adversary can choose what messages wants Alice to sign, and he knows both the messages and the corresponding signatures.

PART-B

1.Explain about Elgamal cryptosystem.

2.llustrate with appropriate diagrams the basic uses of Hash Function.

3.Describe briefly about MD5.

4.Explain in brief about digital signature.

5.Explain Authentication protocols.

UNIT-IV SECURITY PRACTICE & SYSTEM SECURITY

1. In the content of Kerberos, what is realm?

A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

The Kerberos server must have user ID and hashed password of all participating users in its database.

The Kerberos server must share a secret key with each server.Such an environment is referred to as "Realm".

2. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?

Dialogue between client „C" , server „S" and authentication erver(AS) are given below

a) C AS: [IDc|| Pc || IDs]

b) AS C: Ticket

c) C S: [IDc || ADc || IDs]

Ticket = EKs [IDc ||ADc ||IDs]

3. What is the purpose of X.509 standard?

X.509 defines framework for authentication services by the X.500 directory to its users X.509 defines authentication protocols based on public key certificates

4.Define X.509 Authentication Service.

X.509 is part of the X.500 series. X.509 define a directory service. X.509 is based on the use of public-key cryptography and digital signatures. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. For example, the X.509 certificate format is used in S/MIME, IP Security , and SSL/TLS and SET .

5.Define Kerberos.

Kerberos is an authentication service developed as part of project Athena at MIT.The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

6.List out the requirements for Kerberos.

Secure

Reliable

Transparent

Scalable

7.Mention the limitations of version 4 of Kerberos.

a. Environmental shortcomings

Encryption system dependence

Internet protocol dependence

Message byte ordering

Ticket lifetime

Inter realm authentication

b. Technical deficiencies

double encryption

propagating block chaining encryption

session keys

password attacks

8.Write short notes on Secure Electronic Transaction .What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet.

Confidentiality of information

Integrity of data

Cardholder account authentication

Merchant authentication

9. What are the steps involved in SET Transaction?

The customer opens an account

The customer receives a certificate

Merchants have their own certificate

The customer places an order.

The merchant is verified.

The order and payment are sent.

The merchant requests payment authorization.

The merchant confirm the order.

The merchant provides the goods or services.

The merchant requests payment.

10.Define Intruder

An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

11.List Classes of Intruders.

Masquerader

Misfeasor

Clandestine user

12.Write short notes on Intrusion detection system

A set of automated tools designed to detect unauthorized access to a host system.

13.Write short notes on Malicious software.

Malicious software is software that is intentionally included or inserted in a system for a harmful purpose.

14.Write short notes on Virus and its types.

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.

Types:

1) Parasitic virus

2) Memory-resident virus

3) Boot sector virus

4) Stealth virus

5) Polymorphic virus

15.Write short notes on Worm.

A worm is a program that can replicate itself and send copies from computer to computer across network connections.

16.Define 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

17.Define Threshold detection.

This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

18.Define Profile based.

A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

19.Define 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.

20.Define Anomaly detection.

Rules are developed to detect deviation from previous usage patterns.

21.Define Penetration identification.

An expert system approach that searches for suspicious behavior.

22.Define Honeypot .

A decoy system designed to lure a potential attacker away from critical systems. A form of intrusion detection.

23.What is Zombie?

A program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.

24.What is Denial of Service?

A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service.

25.Define Firewall.

A firewall is a device or set of devices designed to permit or deny network transmissions based

upon a set of rules and is frequently used to protect networks from unauthorized access.

26.List the types of Firewall:

1.Packet Filtering Router

2.Application-Level Gateway

3.Circuit-Level Gateway

27.List the Firewall Configuration.

1. Screened host Firewall System(single homed bastion system)
2. Screened host Firewall System(Dual homed bastion system)
3. Screened Subnet Firewall System

28.What is Trusted System?

A trusted system is a computer and operating system that can be verified to implement a given security policy. Typically, the focus of a trusted system is access control.

29.List the types of Viruses:

parasitic virus

memory-resident virus

boot sector virus

stealth virus

polymorphic virus

metamorphic virus.

30.Classify the intruders.

Masquerader

Misfeasor

Clandestine user

31.How the password files be protected?

The password files can be protected in one of the two ways:

one way encryption

access control

32. What are the design goals of the firewall.

a. All traffic from inside to outside, and vice versa, must pass through the firewall.

b. Only authorized traffic, as defined by the local security policy, will be allowed to pass.

c. It is immune to penetration.

33. List out the limitations of the firewall.

a. It cannot protect against attacks that bypass the firewall.

b. The firewall does not protect against internal threats.

c. It cannot protect against the transfer of virus infected programs or files.

34. Define Basiton host.

A Basiton host is a system identified by the firewall administrator as a critical strong point in the network security.

PART-B

1.Explain X.509 Authentication Services.

2.Discuss in detail Kerberos 4 message Exchanges for providing authentication.

3.Explain the Firewall Design Principles

4.List out the limitations of Kerberos 4 and give a short note on Kerberos 5.

5.What are types of firewalls?Discuss.

6.Write short notes on viruses and related threats.

UNIT-V E-MAIL, IP & WEB SECURITY

1.What are the services provided by PGP services?

- Digital signature
- Message encryption
- Compression
- E-mail compatibility
- Segmentation

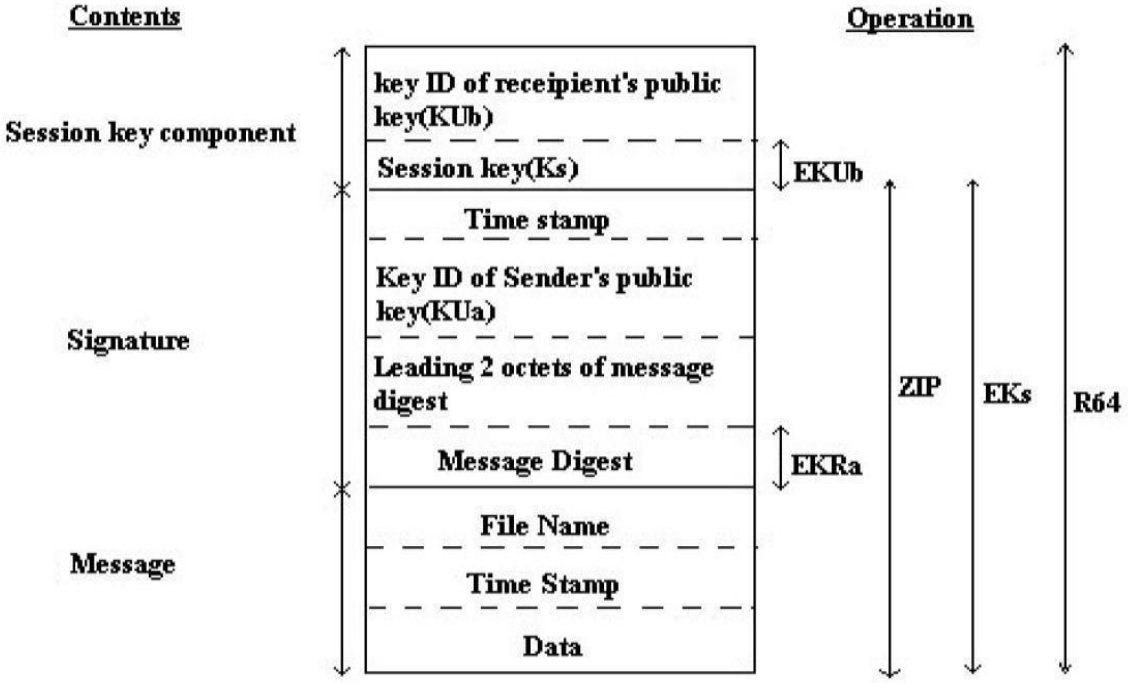
2.Signature is generated before compression in PGP. Why?

There are two reasons behind it.

It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.

Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty. Thealgorithm is not deterministic.

3.What is the general format for PGP message?



4.Why E-mail compatibility function in PGP needed?

E-Mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this urpose is Radix-64 conversion.

5. Explain the reasons for using PGP?

It is available free worldwide in versions that run on a variety of platforms, incl ding DOS/windows, UNIX, Macintosh and many more.

It is based on algorithms that have survived extensive public review and are considered extremely secure.

E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128,IDEA, 3DES for conventional encryption, SHA-1for hash coding.

It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.

It was not developed by nor is it controlled by any governmental or standards organization.

6. Name any cryptographic keys used in PGP?

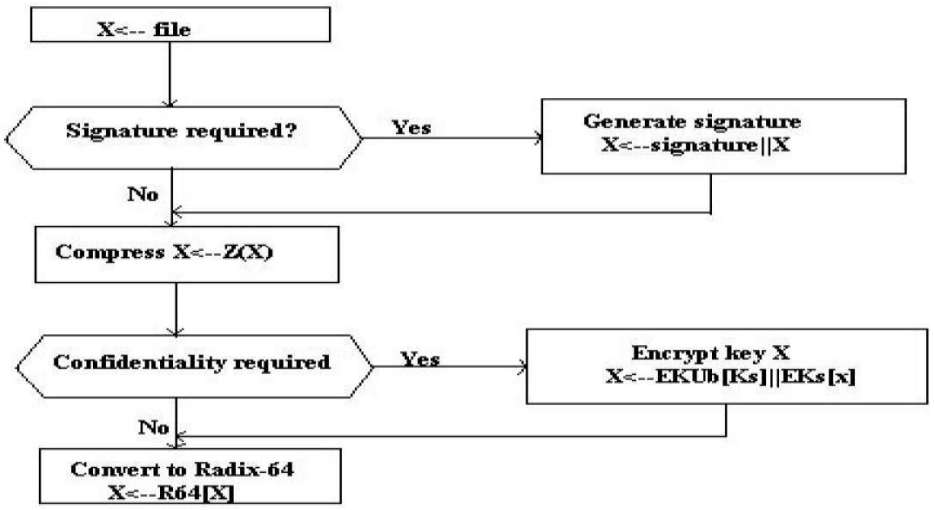
a) One-time session conventional keys.

b) Public keys.

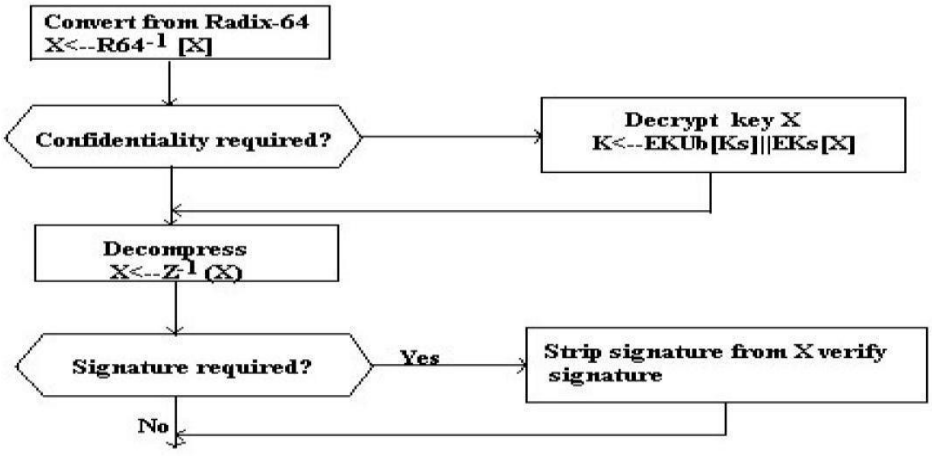
c) Private keys.

d)Pass phrase based conventional keys

7. Draw the diagram for PGP message transmission reception?



a)Transmission Diagram



b)Reception Diagram

8. Define key Identifier?

PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

9. Give the steps for preparing envelope data MIME?

Generate Ks.

Encrypt Ks using recipient' s public key. RSA algorithm used for encryption. Prepare the 'recipient info block' .

Encrypt the message using Ks.

10. What are the elements of MIME?

Five new message header fields are defined which may be included in an RFC 822 header.

A number of content formats are defined. 9_Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

11. Define S/MIME?

Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security

12.List the limitations of SMTP/RFC 822?

a) SMTP cannot transmit executable files or binary objects.

b) It cannot transmit text data containing naional language characters.

c) SMTP servers may reject mail mess ge over certain size.

d) SMTP gateways cause problems while transmitting ASCII andEBCDIC.

e) SMTP gateways to X.400 E-mail network cannot handle non textual data inclded in X.400 messages.

13.What are the headers fields define in MIME?

- MIME version.
- Content type.
- Content transfer encoding.
- Content id.
- Content description.

14.What is MIME content type and explain?

It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15subtypes. They are,

1. Text type
2. Multipart type
3. Message type
4. Image type
5. Video type.

6. Audio type.
7. Application type

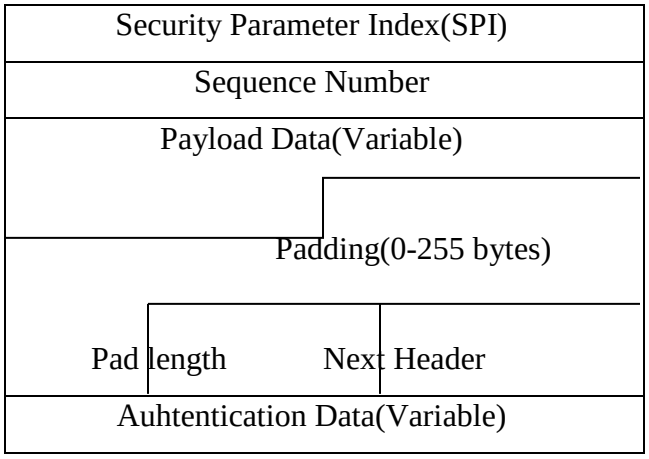
15.What are the key algorithms used in S/MIME?

DSS

DiffiHelman

RSA

16.General format of IPsec ESP Format?



18.List the Applications of IPSec.

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

19.What do you mean by Security Association?

An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on. A key concept that appears in both the authentication and confidentiality mechanism for IP is the security association (SA).

20. Specify the parameters that identifies the Security Association?

A security Association is uniquely identified by 3 parameters:

Security Parameter Index (SPI).

IP Destination Address.

Security Protocol Identifier

21.What is Authentication Header? Give the format of the IPsec Authentication Header?

It provides the authentication of IP Packet, so authentication is based on the use of MAC.

Format of IPsec Authentication Header:

Header(TCP)	oad Header	rved
Security Parameter Index(SPI)		
Sequence Number		
Integrity Check Value (HMAC of IP Header,AH,TCP payload)		

22. Mention the benefits of IPSec.

It provides strong security that can be applied to all traffic crossing the perimeter.

IPSec in a firewall is resistant to bypass.

IPSec is below the transport layer and so is transparent to applications.

IPSec is transparent to users.

23. List out the services provided by the IPSec.

a. Access control

b. Connectionless integrity

c. Data origin authentication

d. Rejection of replayed packets Confidentiality

f. Limited traffic flow confidentiality

24. What is the need of public key ring and private key ring?

Public key ring is one of the data structures which is used to store the public keys of the other participants

Private Key ring is a data structure which is used to store the public and the private keys of the owner alone.

25. Why do we need an anti replay service?

Anti replay service is required in order to avoid the duplicate packets (created by the opponent) which may cause disruption in the service.

26.What is the need padding in Encapsulating Security Payload (ESP)?

a. If an encryption algorithm requires the plaintext to be a multiple of some number of bytes, the padding field is used to expand the plaintext to the required length.

b. ESP format requires that the pad length and the next header fields be right aligned within a 32-bit word. The padding field is used to assure this alignment.

c. Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

28. List the steps involved in SSL record protocol?

1. SSL record protocol takes application data as input and fragments it.
2. Apply lossless Compression algorithm.
3. Compute MAC for compressed data.
4. MAC and compression message is encrypted using conventional alg.

29. Give SSL record format?

ent Type	r Version	r Version	pressed Length
Plain text(optionally Compressed)			
MAC(0,16or 20 bytes)			

30.Write short notes on Web Security:

Secure socket layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called transport layer service (TLS).

31.Write short notes on Transport Layer Security(TLS) ?

Transport Layer Security is defined as a Proposed Internet Standard in RFC 2246. RFC 2246 is very similar to SSLv3. The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version number.

PART-B

1.Describe briefly about PGP services.

2.Write brief note on S/MIME.

3.Explain briefly about IP Security.

4. Explain in detail the operation of Secure Socket Layer in detail

5.Explain about IKE and ISAKMP

6. Explain about TLS.

7.Describe how PGP provides confidentiality and authentication service for e-mail applications

8.Write short notes on authentication header and ESP