Unit - 1

Security Trends - Legal, Ethical and Professional aspects of security, Need for Security at multiple levels, Security policies - Model of Network Security, Security attacks, services and mechanisms - OSI Security Architecture - classical encryption techniques: substitution techniques, transposition techniques, steganography - Foundations of Modern cryptography, perfect security, Information theory, product cryptosystem - Cryptanalysis.

Security Trends - Legal & Ethical Aspects of Security.

Information security trends are as follows

1. Smart Attackers
2. Spreading of mobile malwares
3. Shortage of skill
4. Internet of Things drawback
5. Social networking attacks and phishing
6. Priority for Information Security
7. Use of AI and machine learning in cyber defenses.
8. Complex infrastructure for cyber Security

Smart Attackers :- Attackers capability of writing customized code will continue grow faster.

Spreading of mobile Malwares: Day by Day, use of mobile phones is increases, so mobile hardware has mainly targeted Android OS.

* Attacker key form in

Shortage of skill:- Required numbers of skill information security professional are not available with organization.

Internet of Things Drawback: Most of the organizations are using internet connected devices several devices lack.

Social Networking attacks and Phishing:-

Social Networks are becoming a very popular source of information for these phis

They can easily use all of the info which is contained in your social networking account to steal your identity.

Priority for Information Security:- Providing Importance to information security, we can expect the more use of it in organization with high capabilities.

Use of AI and machine Learning in cyber defenses:- Advances in machine Learning and automation are set to bring continued benefits to businesses and consumers alike.

complex infrastructure for cyber security: Large investment is required from Government and private sector for providing security of digital business.

pRofessional Aspect of Security :-

* Professional aspect of security are good security management practices.

* The security-management domain also introduces some critical documents such as policies, procedures, and guidelines.

* Defining security policy is one of the good security management practices. The key element in policy is that it should state management's intention towards security

* Following are the parameters, consider while deciding security policies:

1. Affordability
2. Functionality
3. Legality
4. cultural issue

Need for Security at Multiple levels :-

Bank robbery is the crime of stealing from a bank during opening hours. Protecting assets was difficult and not always effective.

Protection is easier because many factors working against the potential criminal. Very sophisticated alarm and camera systems silently protect secure places like banks.

Traditionaly information security provided by physical i.e. rugged filing cabinets with locks and administrative mechanisms i.e. personnel screening procedures during hiring process.

⇒ Data Security is the Science and Study of mett of protecting data from unauthorized disclosure and modification.

⇒ Computer Security: Generic name for the colle of tools designed to protect data and to thra hackers

⇒ Network security: Measures to protect data during transmission.

⇒ Internet security: Measures to protect data during transmission over a collection of interconnected networks.

Protecting Valuables:-

1. Increasing threat of attacks.
2. Fast growth of Computer Networking
3. Availability of number of tools and resources on Internet.

Need of Security:-

* User A transmits a sensitive information file to User B. The unauthorised user C is able to monitor the transmission and capture a copy of the file during its transmission.

* A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

* While transmitting the message between two users, the unauthorised user intercepts the message, alters its contents to add or delete entries, and then forwards the

the message to destination user.

Terminologies used in computer and Network Security

(a) cryptography - The art (or) Science encompassing the principles and method transforming an plaintext message into one that is unintelligible and then retransforming.

(b) plaintext - The original message

(c) ciphertext - The transformed message produced as output

(d) cipher - Cryptographic system is called as cipher.

(e) key - Some critical Information used by the cipher, known only to the Sender and receiver.

(f)) Encryption - The process of converting plaintext to ciphertext using a cipher and a key.

(g) Decryption - The process of converting ciphertext back into plaintext using cipher and a key.

(h) Cryptology - Both cryptography and Cryptanalysis.

(i) code - An Algorithm for transforming an plaintext message into an unintelligible one using a code-book.

Security Goals :-

security goals are as follows :-

(1) confidentially (2) Integrity (3) Availability.

1. Confidentiality:-

*Confidentiality ensures that no one can the message except intended receiver.

* Confidentiality refers to limiting inform access and disclosure to authorized user preventing access by (or) disclosure to unauthorized ones.

* Sensitive information should be k secret from individuals who are not auth to see the information.

*Confidentiality is not only applied to the storaag of data but also applies to the transmission of information.

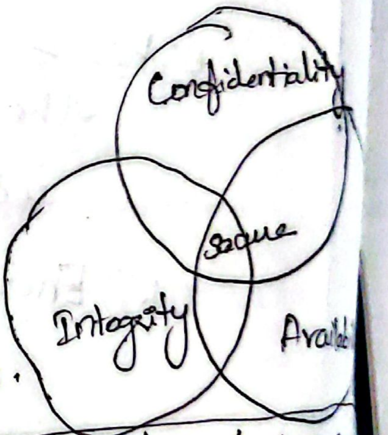


fig. Relationship between Confidentiality Integ and Availability.

2. Integrity:-

* Integrity ensures that received message has not been altered in any way from origin.

*Integrity refers to the trustworthiness of information resources.

*Integrity should not be altered without detection.

* It includes the concept of "data Integrity" namely, that data have not been changed inappropriately, whether by accident (or) deliberately malign activity.

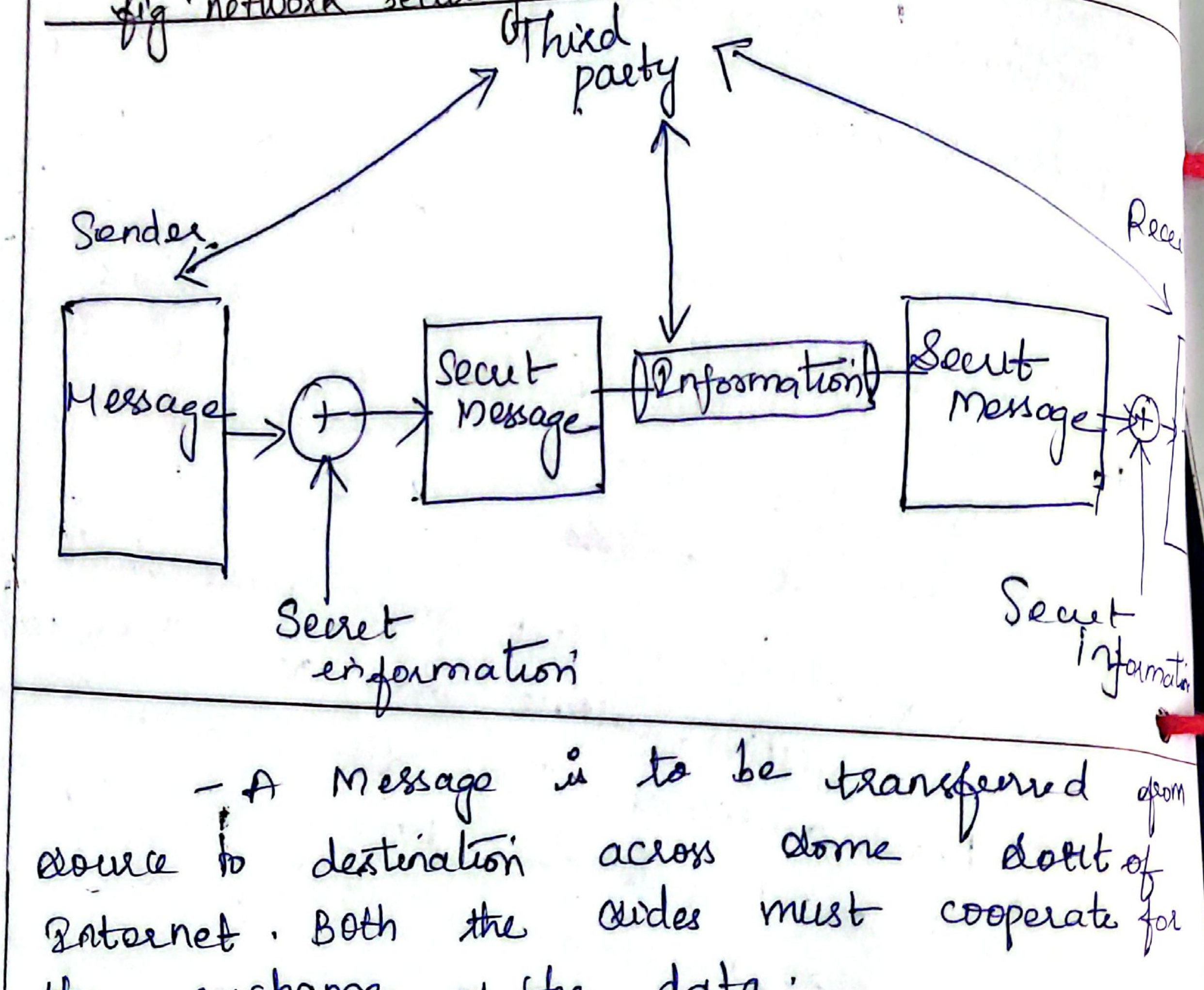
The security can be provided by using following approaches.

1. External approach - Security from external attackers

2. Internal approach - Security from internal attackers

Model of Network Security:-

fig: network security modal



- A Message is to be transferred from source to destination across some sort of Internet. Both the sides must cooperate for the exchange of the data.

- A logical information channel is established by defining a route through the Internet from source to destination

- All the techniques for providing security have two components

1. The security related transformation on the information to be sent.

2. Some secret information shared by the two principles, it is hoped, unknown to the opponent

— Trusted third party is needed to achieve secure transmission.

Security Attacks:-

-Computer based systems have 3 valuable components

- Hardware
- Software, and
- data

-Securities of these components are evaluated in terms of

- vulnerability
- Threats
- attacks
- control.

Asset

— Asset means people, property and information.

— people may include employees and customers along with other invited persons such as contractors or guests.

Vulnerability:-

Vulnerability refers to the security in a system that allows an attack be successful.

Threat:-

Threat refers to the source and me of a particular type of attack.

A threat assessment is performed t determine the best approaches to securin a system against a particular threat, or class threat.

Threats come in many forms, dependi on their mode of attack.

Risk:-

$$Risk = Asset + Threat + Vulnerability$$

$$R = A + T + V$$

Risk is a function of threats exploiting Vulnerabilities to obtain damage or dest assets. Thus, threats may exist, but if there are no vulnerabilities, there is little/no risk.

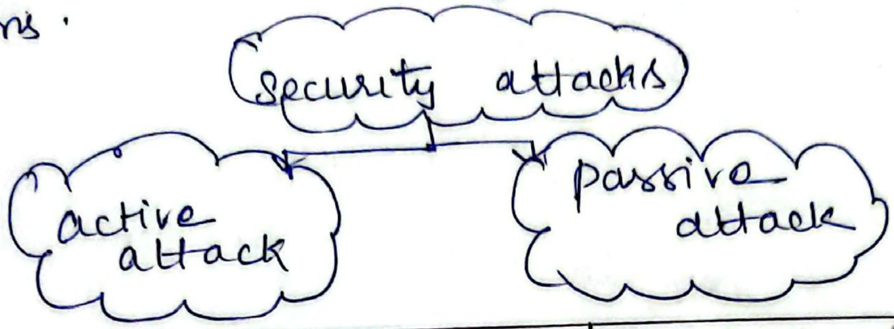
Control:-

-Control is used as proactive measure. Control is a action, device, procedure, or technique that removes (or) reduces a vulnerability.

- A threat is blocked by control of vulnerability

Types of Security Attacks:-

An attempt to gain unauthorized access to information resource (or) services, or to cause harm (or) damage to information systems.



passive attack	Active Attack.
passive attack are in the nature of eavesdropping on, or monitoring of, transmissions	Active attacks involve some modification the data stream or the creation of a fake stream
very difficult to detect	Easy to detect
does not affect the system	It affects the system
Types: Release of message contents and traffic analysis	Types:- Masquerade, replay, modification of message and denial of service

passive Attack:-

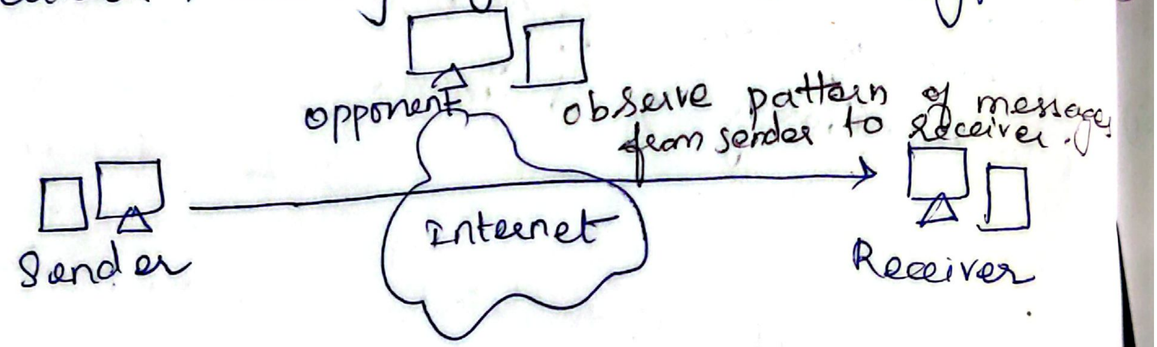
— passive attacks are those, wherein the attacker indulges in eavesdropping on, (or) monitoring of data transmission.

- The attacker aims to obtain informati
that is in transit.

- passive attacks are of two types
  1. Release of message contents.
  2. Traffic analysis

- passive attaks are very difficult to de
because they do not involve any alternat
of data.

- It is fasible to prevent the success
attack, usually by means of encryption.



Active Attack:-

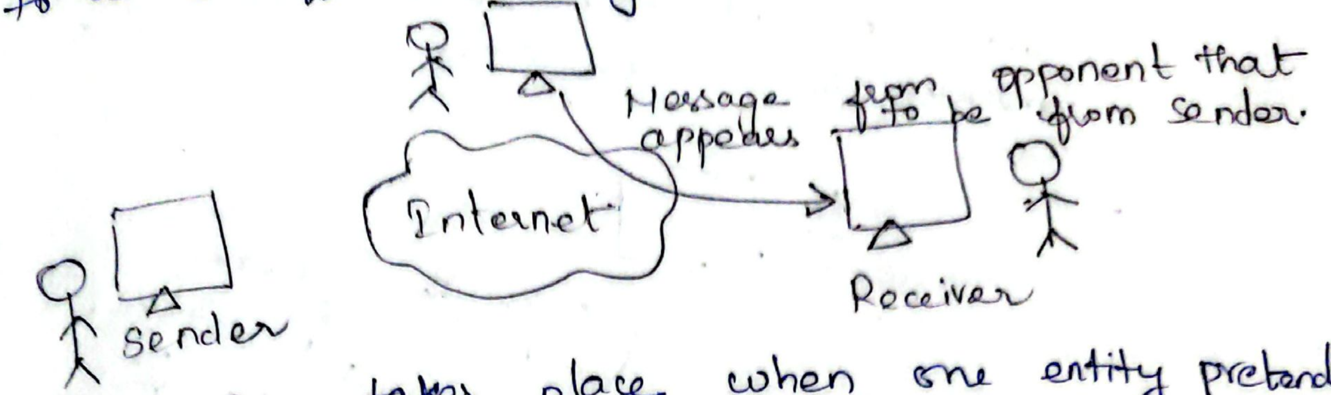
Active Attacks involve some modifications of the data stream (or) the creation of a false stream. These attacks can not be prevented easily.

Active attacks can be subdivided into four types.

1. Masquerade 2. Replay
3. Modification of Message.
4. Denial of Service.

1. Masquerade

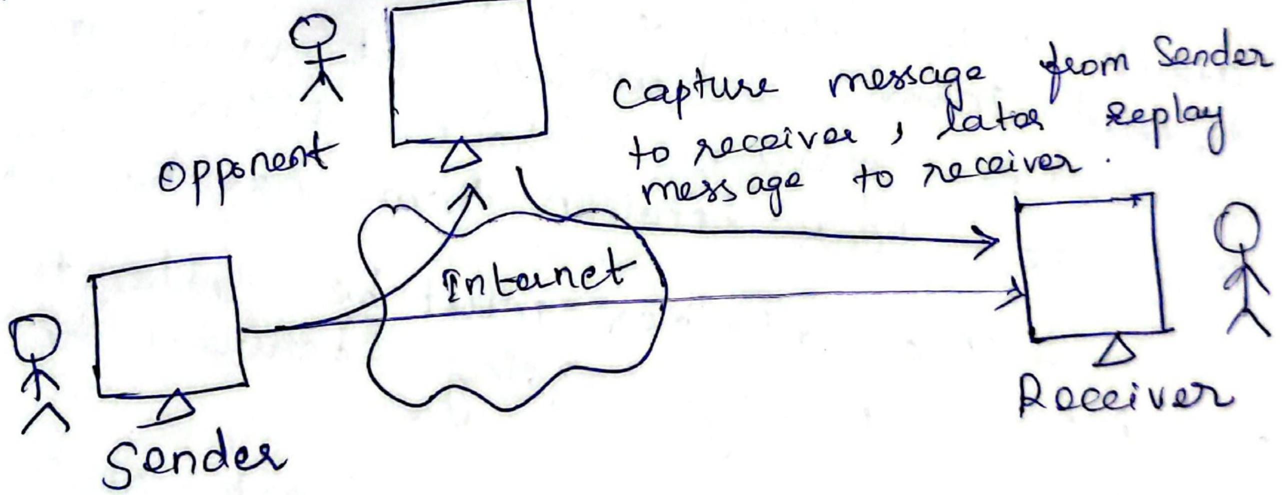
It take place when one entity pretends to be a different entity.



It takes place when one entity pretends to be different entity.

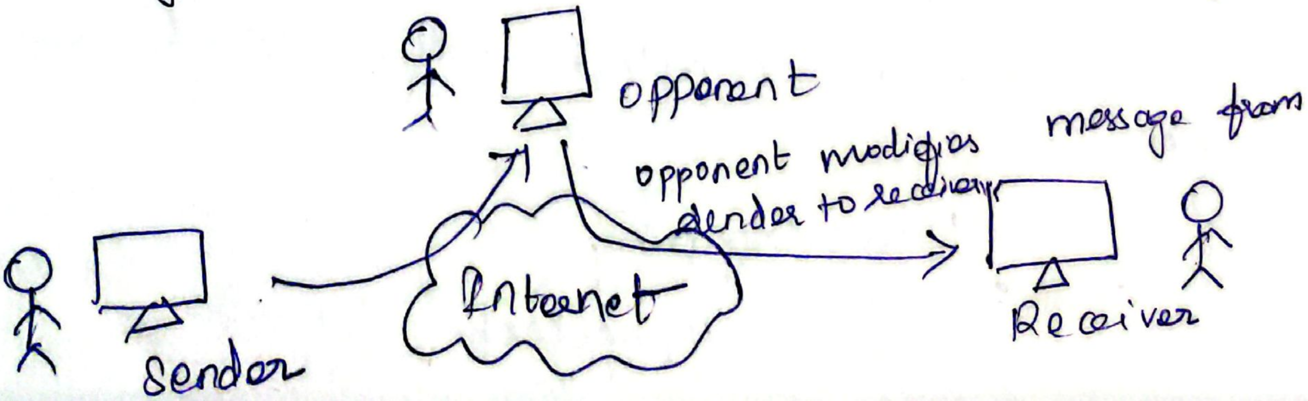
2. Replay.

It involves the passive capture of a data unit and its subsequent retransmission produce an unauthorized affect.



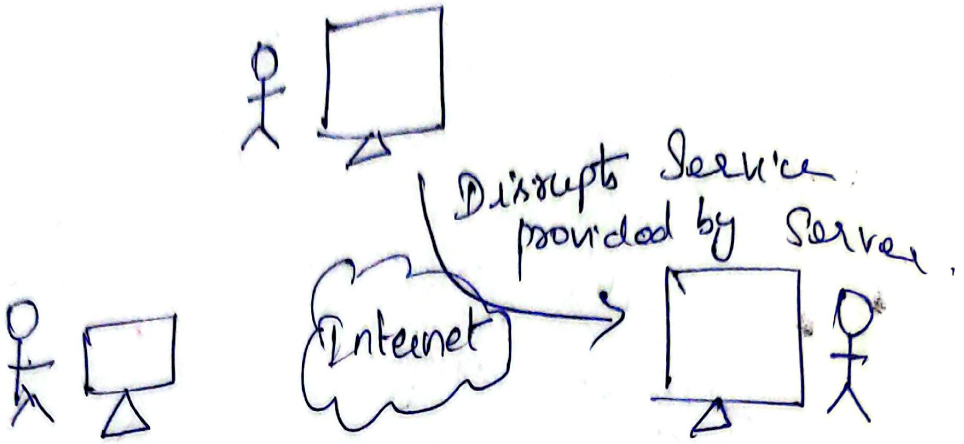
3. Modification of Message.

It involves some change to the original message. It produces an unauthorized effect.



4. Denial of Service:

- Fabrication causes Denial of Service (Dos)
- Dos prevents the normal use (or) mana of communication facilities.



Man-In-the Middle Attack

- In cryptography, a Man-In-The-Midde (MI attack is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party know that the link between them has be compromi

- The attacker must be able to observe and intercept messages going between the two victims.

- The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol when used without authenticat

- The MITM attack may include one (or) more of

1. Eavesdropping
2. Chosen Ciphertext attack
3. Substitution attack
4. Replay attacks.

Defenses against the attack:

Various Defenses agaist MITM attacks use authentication techniques that are based on :

1. Public keys
2. Stronger mutual authentication
3. Secret keys (high information entropy secrets)
4. Passwords (low information entropy secrets)
5. Other Criteria (such as voice recognition or other biometrics)

Security Services :—

X.800 defines a security services as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems. (or) of data transfers.

X.800 divides security services into 5 categories.

1. Authentication
2. Access control.
3. Data confidentiality
4. Data integrity
5. Non repudiation

1. Authentication

- Authentication is the process of determining whether someone (or) something is, in fact, who or what it is declared to be.

- In private & private computer network, authentication is commonly done through the use of logen passwords.

- Two specific authentication services defined in X.800

(a) Peer entity authentication

- used in association a logical connection to provide confidence identity of the entities connected

(B) Data origin authentication:

- Does not provide prot against the duplication (or) modificat of data units

2. Access control :-

It is the ability to limit and co the access to host systems and applications via communications links

This service control who can have access to a resource.

3. Data confidentiality

Confidentiality is the concealment of information (or) resources. It is the protection of transmitted data from passive attacks.

Confidentiality is classified into

1. Connection Confidentiality
2. Connectionless confidentiality
3. Selective field confidentiality
4. Traffic flow Confidentiality

Data Integrity :-

Integrity can apply to a stream of messages (or) selected fields within a message.

Modification causes loss of message Integrity.

Nonrepudiation :-

Non repudiation prevents either sender (or) receiver from denying a transmitted message.

Security Mechanism :-

- Security Mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.

- security mechanisms defined by X.800 are given below.

* Encipherment
* Data Integrity
* Digital signature
* Authentication exchange
* Traffic padding
* Routing control.

* Notarization

* Access control

X.800 defined security mechanisms as fo

1. Specific Security mechanisms:- May be inc into the appropriate protocol layer in order provide some of the OSI security ser

(a) Encipherment :-

(b) Digital signature

(c) Access control

(d) Data Integrity

(e) Authentication exchange

(f) Traffic padding

(g) Notarization

2. Pervasive Security mechanisms :-

Mechanisms that are not specific to any particular OSI Security Service (or) protocol layer.

(a) Trusted functionality

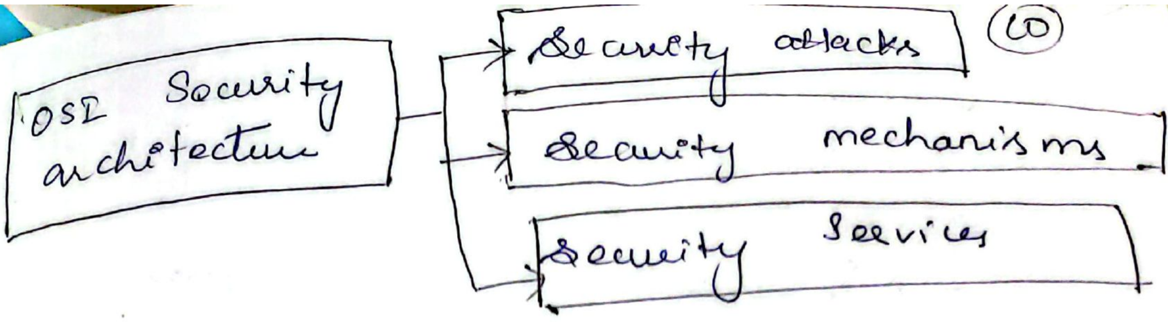
(b) Event detection

(c) Security label

(d) Security recovery

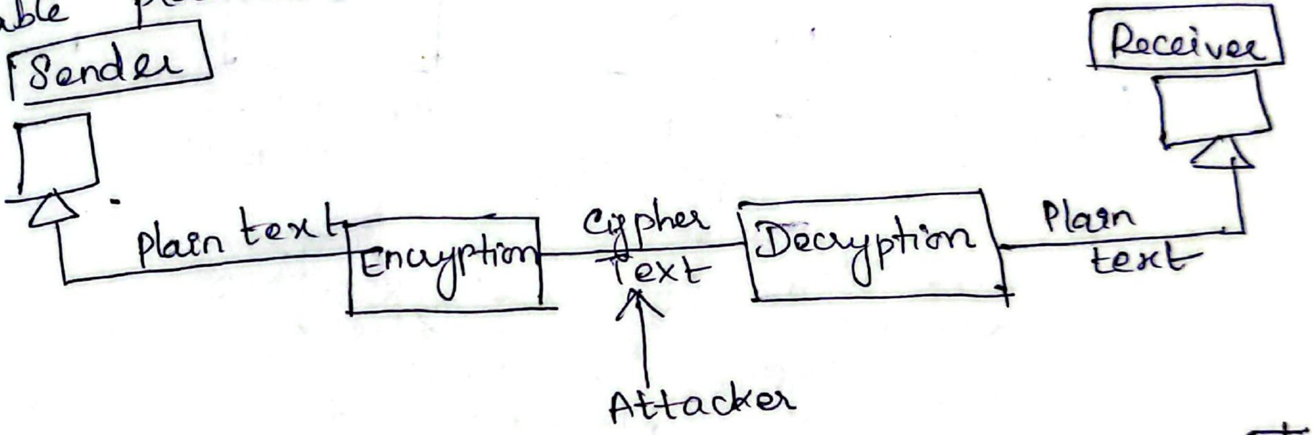
OSI Security Architecture

The OSI Security Architecture is useful to managers as a way of organizing the task of providing



Cryptography :-

- In cryptography, we start with the unencrypted data, referred to as plaintext. plaintext is encrypted into ciphertext, which will in turn (usually) be decrypted back into usable plaintext.



- cryptography provides secure communication in the presence of malicious third parties.

- Encryption is the process of encoding a plain text message into non-readable form.

_Decryption is a process of transferring an encrypted message back into its normal form

Advantages of cryptography:

* provides Security to online network Communication
* provides security to email, credit / debit card information etc...

classical encryp...

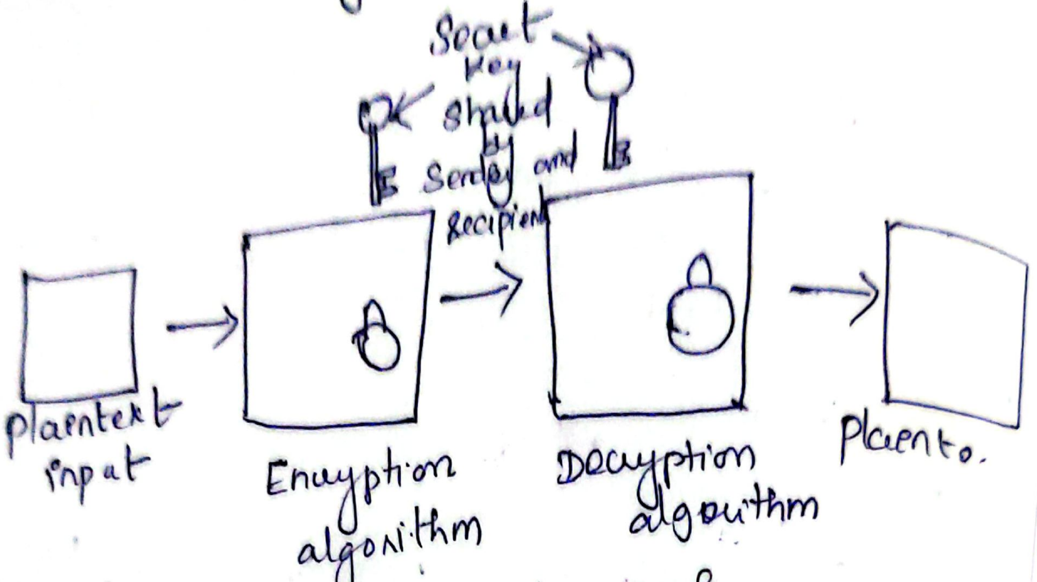
A symmetric encryption model h

ingredients

1. plaintext 2. Encryption algorithm

3. Secret key 4. ciphertext

5. Decryption algorithm.



Characteristics of cryptography

1. The type of operations used for transforming plaintext to ciphertext

2. The number of keys used.

3. The way in which the plaintext is processed

Cryptanalysis:-

*) The process of trying break any cipher text message to obtain the original plain text message itself is called as Cryptanalysis.

*) Cryptanalysis is the breaking of codes. The person attempting a cryptanalysis is called as a cryptanalyst.

Advantages of Symmetric Cryptography

1. High rates of data throughput
2. Keys for symmetric-key ciphers are relatively short.

Disadvantages of symmetric-key Cryptography

1. Key must remain secret at both ends.
2. In large networks, there are many key pairs to be managed.

Substitution Techniques

- A substitution cipher changes characters in the plaintext to produce ciphertext.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Ceaser Cipher

Ceaser cipher is a special case of substitution techniques wherein each alphabet in a message is replaced by an alphabet three places down the line

plain text	hello
ciphertext	KHOOR

The algorithm can be expressed as fo

Encryption	Decryption:
p+SK=C	C-SK = P.

Playfair cipher:-

Playfair algorithm is based on th use of a 5x5 matrix of letters cons using keyword.

Key word = Monarchy

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

balloon ⇒ ba/lx/lo/on

I/J B/SU/MP/NA

IB/JB SU MB NA.

Monoalphabetic cipher:-

Monoalphabetic cipher substitutes one letter of the alphabet with another letter of the alphabet.

Hill cipher:-

The encryption algorithm takes m successi-ve plaintext letters and substitutes for them m cipher text letters.

encryption : $C = KP \bmod 26$.

Decryption : $P = K^{-1}C \bmod 26$ when $K^{-1} = 1/|K| \text{ adj}K$

$P = ACT$, $K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

p	q	r	s	t	u	v	w	x	y	z
15	16	17	18	19	20	21	22	23	24	25

$\boxed{C = KP \bmod 26}$

$$= \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} P \\ O \\ H \end{bmatrix}$$

$\boxed{P = K^{-1}C \bmod 26}$

$$K^{-1} = 1/|K| \text{ adj}(K)$$

$$|K| = 6(16 \times 15 - 10 \times 17) - 24(13 \times 15 - 10 \times 20) + 1(13 \times 17 - 16 \times 20)$$

$$= 6(40) - 24(-5) + 1(-99)$$

$$= 6(70) - 24(-5) + 1(-99)$$

$$= 420 + 120 - 99$$

$$= 441$$

$$\text{adj}(K) = K^T = \begin{bmatrix} 6 & 13 & 20 \\ 24 & 16 & 17 \\ 1 & 10 & 15 \end{bmatrix}$$

$$= \begin{bmatrix} 16 \times 15 - 17 \times 10 & 24 \times 15 - 17 \times 1 & 24 \times 10 - 16 \times 1 \\ 13 \times 15 - 10 \times 2 & 6 \times 115 - 20 \times 1 & 6 \times 10 - 13 \times 1 \\ 20 \times 16 & 17 \times 16 - 24 \times 20 & 6 \times 16 - 13 \times 24 \end{bmatrix}$$

$$= \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$$

$$= \frac{1}{441} \begin{bmatrix} 70 & -342 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \bmod 2$$

$$= \frac{1}{441} \begin{bmatrix} -2184 \\ 726 \\ 2295 \end{bmatrix} \bmod 26$$

$$= 25 \begin{bmatrix} -2184 \\ 726 \\ 2295 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 54600 \\ 18150 \\ 57375 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \cdot$$

polyalphabetic substitution :-

In polyalphabetic substitution, each occurence of a character can have a different substitute. The relationship between a character in the plaintext to a character the ciphertext is one to many.

eg: Vignere cipher:-

plain Text : BE ACTIVE

key : MAN

~~M~~A NMANMA		12	0	13	12	0	13	12	0
BE ACTIVE	+	1	4	0	2	19	8	21	4
		13	4 ~~5~~	13	14	19	21	33	4

Cipher Text = N E N O T V H E

Decryption Process

MANMANMA
NENOTVHE

$$\begin{array}{rrrrrrrr} & 12 & 0 & 13 & 12 & 0 & 13 & 12 & 0 \\ - & 13 & 4 & 13 & 14 & 19 & 21 & 7 & 4 \\ \hline & 1 & 4 & 0 & 2 & 19 & 8 & -5 & 4 \end{array}$$

plaintext: BE ACTIVE

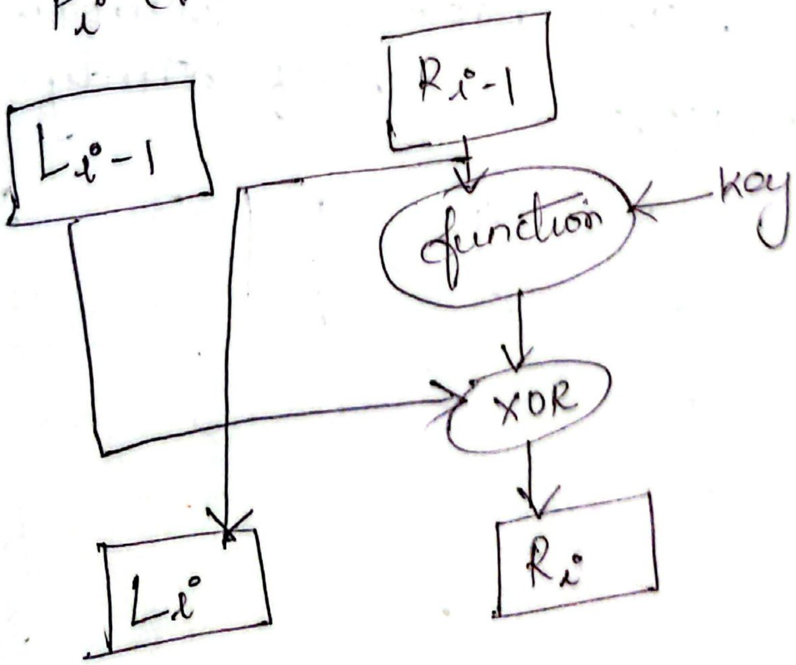
One Time Pad:-

The key string is chosen at random and at least as long as the message, so it does not repeat.

Vernam cipher uses a one time pad, which is discarded after a single use, therefore is suitable only for short messages.

Feistal cipher:

P_i (plaintext)



$L_i = R_i - 1$
$R_i = L_{i-1}$ XOR
(function(R_{i-1}, key))

Parameters:

1. No. of rounds 16 bytes 16 bytes
2. Blocksize 128 bits
3. Key size

$a * a^{-1} = a^{-1} * a = e$

Transposition Techniques:-

The transposition cipher rearranges Characters in the plain text to form ciphertext. The letters are not changed

The rail fence cipher is composed writing the plaintext in two rows, proceeds down, then across and reading the ciphertext across, then down

for example, to encipher the message "me me after this party" with a rail fence of depth 2,

m e m a t r h s a t
e t e f e t i p r y

ciphertext = MEMATRHSATETEFETI PRY

(2)

plaintext = The book is suitable for self study

key = 564132

Key :	5	6	4	1	3	2
Plaintext :	t	h	e	b	o	o
	k	i	s	s	u	i
	t	a	b	l	e	f
	o	r	s	e	l	f
	s	t	u	d	y	

Ciphertext : BSLED OIFFOUELYESBSU TKTOS HIART

Rail Fence Cipher:-

- The Rail Fence Cipher is a transposition cipher. It rearranges letters by drawing them in a way that they form a shapo of the rails of an imaginary fenc.

To encrypt the message, the letters should be written in a zigzag pattern, going downwards and upwards between the levels of the top row down to the bottom one.

eg: plaint text = buy your book in August

b				o				o				n				u		
	u		y		u		b		o		i		A		g		s	
		y				r				k				u				t

ciphertext: BOONUUYUBOIAGSYRKUT

Cryptanalysis:-

- The process of attempting to discover X (or) K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

- The various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Ciphertext Only - A copy of cipher text alone is known to the cryptanalyst

Known plaintext - The cryptanalyst has a cop the cipher text and the correspond plaintext.

Chosen plaintext - The cryptanalyst gains tempo access to the encryption machine. They cannot open it to find the key, howe they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text - The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

Steganography:-

-A plaintext message may be hidden in any one of the two ways. The methods of steganography hide the existence of the message, whereas the methods of cryptography make the message unintelligble to outsiders by various transformations of the text.

-A simple form of steganography is time consuming to contruct an arrangement in which of words or lett an apparently protected text spells out the real message.

(or) the sequence of first letter of each word of the overall message spells out the real (hidden) message.

various other techniques have been used historically, some of them are:

<u>character marking</u> - second letters of printed (or) typewritten are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

<u>Invisible Ink</u> - a number of substances can be use for writing but not visible trace until heat (or) some chemical is applied to the paper.

<u>Pen punctures</u> - small pen punctures on selected letters are ordinary not visible unles the paper is held on light

<u>Typewritten correction ribbon</u> - used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Drawbacks of steganography

* Requires a lot of overhead to hide relatively few bits of information.

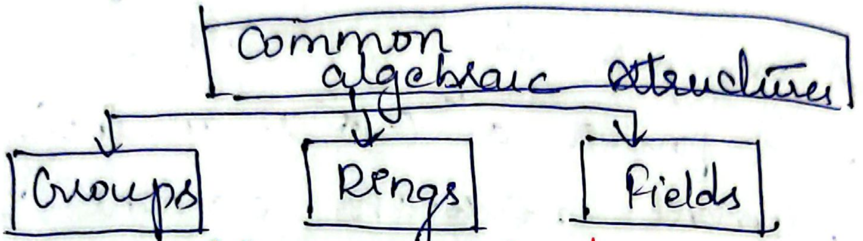
* Once the system is discovered, it becomes virtually worthless.

—— x ——

Unit - II Symmetric key Cryptography

1. Algebraic Structures :-

combination of the set and the operations that are defined for those sets, applied to the elements of the set is called an algebraic structure.



Groups, Rings and Fields :

Groups :-

A group G, sometimes denoted by {G, *}, is set of elements with a binary operation by * that associates to each ordered pair (a,b) of elements in G an element (a*b) in such that the following axioms are obeyed.

(A1) Closure : If a & b belong to G, then a*b is also in G.

(A2) Associative : $a*(b*c) = (a*b)*c$ for all a, b, c in G

(A3) Identity element : There is an element e, in G such that $a*e = e*a$ for all a in G.

(A4) Inverse element : for each in G, there is an element a^{-1} in G such that $a*a^{-1} = a^{-1}*a = e$

(A5) Commutative : $a*b = b*a$ for all a, b in (

cyclic Group :-

- We define exponentiation within a group as a repeated application of the group operator, so that $a^3 = a \cdot a \cdot a$.

- We define $a^0 = e$ as the identity element

- A group G is cyclic if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to generate the group G or to be a generator of G. A cyclic group is always abelian and may be finite (or) infinite.

- The additive group of integers is an infinite cyclic group generated by the element 1.

Rings:-

A ring R, sometimes denoted by $\{R, +, *\}$, is a set of elements with two binary operations, called addition and Multiplication, such that for all a, b, c in R the following axioms are obeyed.

(M1) Closure under Multiplication : If a and b belong to R, then ab is also in R.

(M2) Associativity of Multiplication : $a(bc) = (ab)c$ for all a, b, c in R

(M3) Distributive laws : $a(b+c)=ab+ac$ for all a,b,c in R

$(a+b)c=ac+bc$ for all a,b,c in R

(M4) commutativity of Multiplication: $ab=ba$, for all a,b in R

(M5) Multiplicative identity :. There is an element 1 in R such that $a1=1a=a$ in R

(M6) No Zero Divisors :- if a,b in R and $ab=0$, then either $a=0$ (or) $b=0$.

Fields :-

A field F, denoted by {F, +, ×}, is a set of elements with two binary operations, called addition and Multiplication, such that for all a,b,c in F the following axioms are obeyed.

(A1-M6) F is an Integral domain ; that is, F satisfis axioms A1 through A5 and M1 through M6.

(M7) Multiplicative Inverse :- for each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1}=(a^{-1})a=1$

8. Modular Arithmetic

The modulus:-

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus.

$0 <= r < n; q = [a/n]$

$a = [a/n] * n + (a \bmod n)$

Two integers a and b are said to be congruent modulo n, if (a mod n) = (b mod n). This is written as $a \equiv b \pmod{n}$3.

Divisors:-

We say that a non zero b divides a if a=mb for some m, where a, b and m are integers. That is b divides a if there is no remainder on division.

If a|1, then a = ± 1

If a|b and b/a, then a = ± b,

Any b ≠ 0 divides 0.

If a/b and b/c, then a/c.

Properties of congruences:-

1. a=b (mod n) if n /(a-b).

2. a=b(mod n) implies b=a(mod n)

3. a=b(mod n) and b=c (mod n) imply a ≡ c (mod n).

Modular Arithmetic operations:-

By definition the (mod n) operator maps all integers {0, 1, ..., (n-1)}. We can perform arithmetic operations within the confines of this set, this is known as modular arithmetic tech.

1. $[(a \bmod n) \div (b \bmod n)] \bmod n = (a \div b) \bmod n$

2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

3. $[(a \bmod n) * (b \bmod n)] = (a * b) \bmod n$

4. The Euclidean Algorithm

one of the basic techniques of number theory is the Euclidean Algorithm, which is a simple procedure for determining the gretest common divisor of two positive integers.

Greatest Common Divisor

⇒ A nonzero b is defined to be a divisor of a if a=mb for some m, where a,b and m are integers. We use the notation gcd(a,b) to mean the greatest common divisor of a and b. The gcd(0,0)=0.

⇒ The positive integer c is said to be the greatest common divisor of a and b if:

1. c is a divisor of a and of b.
2. Any divisor of a and b is a divisor of c.

6. Block Cipher principles of DES:

A stream cipher is one that encrypts a digital data stream one bit or one byte of a time. Eg. Vigenere

7. Block Cipher Design Principles:-

The three critical aspects of b
cipher design: the number of rounds, d
of the function F, and key Schedulin

DES Design criteria

1. No output bit of any S-box should be too close a linear function of the input bits.

2. Each row of an S-box should include all 16 possible output bit combinations

3. If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits.

4. If two inputs to an S-box differ in exac the outputs must differ in at least two bits.

Number of Rounds:-

The cryptographic strength of a feistel cipher derives from three aspects of the design: the number of rounds, the function F, and the key schedule algori

Design of Function F:-

The function F provides the element of confusion in a feistel cipher. Thus, it must be difficult to "unscramble" the substitution performed by F.

- Several other criteria should be considered in designing F. The algorithm have good avalanche properties. In general, this means that change in one bit of the input should produce a change in many bits of the output.

S-box Design:-

- One of the most intense areas of reasearch in the field of symmetric block ciphers is that of S-box design.

- one obvious characteristic of the S-box is its size. An n*m S-box has n input bits and m output bits. DES has 6x4 S-boxes.

- Bent functions are a special case of Boolean functions that are highly nonlinear according to certain mathematical criteria.

- The authors define the guaranteed avanlanche (GA) criterion as follows. An S-box satisfies GA of order g, if for a 1 bit input change, at leas g output bits change

---

Key schedule Algorithm:-

- A final area of block cipher design, is the key schedule algorithm. With any Feistel block cipher, the key is used to generate one subkey for each round.

- In general, we would like to select subkey to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main k

8. Evaluation criteria of AES

The origins of AES:-

There is a high level of confidence that 3DES is very resistant to cryptanaly If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm.

The principal drawback of 3DES is that the algorithm is relatively slow in softwa

AES Evaluation

The three categories of criteria were as follows :

Security :- This refer to the effort requ to cryptanalyze algorithm.

Cost :- NIST propose AES to be practical in a wide range of applications

Algorithm and Implementation Characteristi This category includes a variety of considera -tion, including flexibility, suitability and software implementation

9. Block cipher modes of operation (9)

Block cipher algorithm is a basic building block for providing data Security

(a) electronic Code Book

(b) Cipher block chaining mode

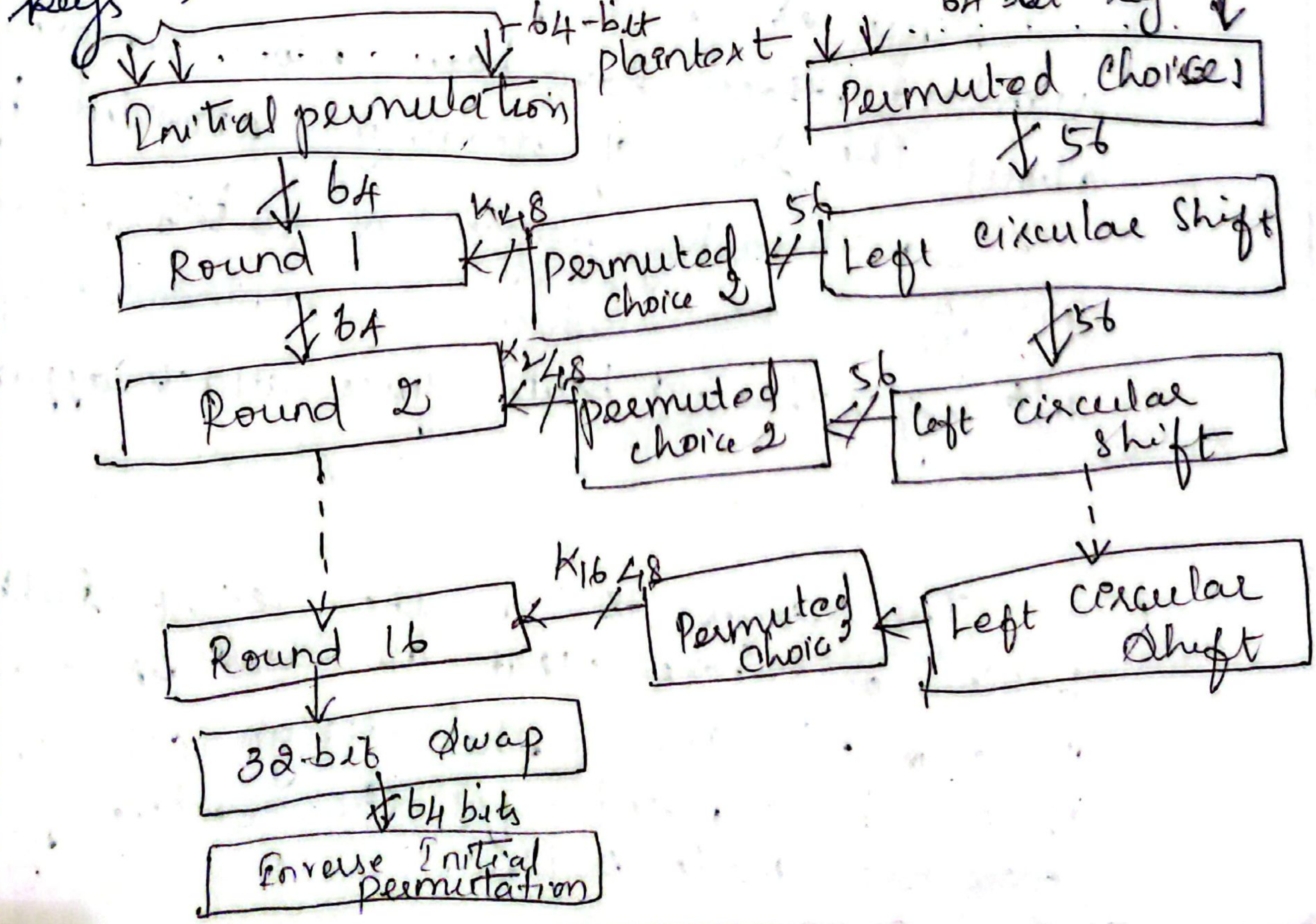
(c) Cipher feedback mode

(d) output feedback mode

(e) counter mode.

10. (S-DES) Simplified Data encryption standard

for DIS, data are encrypted in 64-bit blocks using 56 bit key. The algorithm transforms 64-bit input in a series of steps into 64-bit output. The same steps, with the same keys, are used to reverse the encryption.



Initial Permutation

The input to a table consists of 6. numbered from 1 to 64. The 64 entries in permutation table contain a permutation number from 1 to 64.

Each entry in the permutation indicates the position of a numbered input bit in the output.

The Avalanche Effect:-

A desirable property of any encrypti algorithm is that a small change in ei the plaintext or the key should produce significant change in the ciphertext.

11. The Strength of DES:-

→Since it is accepted as a centralized standard, there have been slow concerns about the level of security provided by DES.

- with a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} key. Thus, a brute force attack appears.

The Nature of the DES Algorithm:-

The focus is on the eight substitution tables, or S-boxes, that are used in each Iteration. Because the design criteria for these boxes, and for the entire algorithm were not made public.

13) Advanced Encryption Standard ·

AES structure

The AES specification uses the same three key size alternatives but limits the block length to 128 bits. A number of AES parameters depend on the key length,

Key Expansion Algorithm :

The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176bytes)

14: RC4

- RC4 is a stream cipher designed In 1987 by Ron Rivest for RSA Security. It is a variable key size stream cipher with byte-oriented operations.

- The algorithm is based on the use of random permutation. Eight to sixteen machine operations are require per output byte, and the cipher can be expected to run very quickly in software

- RC4 is used in the Secure Sockets Layer / Transport layer Security (SSL/TLS) standards that have been defined for communication between web browsers and servers.

Strength of RC4 :

- The author demonstrate that the WE protocol, intended to provide confidential on 802.11 wireless LAN network, is vulnerabl to a particular attack approach.

- In essence, the problem is not with RC4 itself but the way in which keys are generated for use as input to RC4.

- This particular problems does not appear to be relevant to other applicatio using RC4 and can be remediated in WEP by changing the way in which keys are generated.

15. Key distribution

- for symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protect from access by others.

- for two parties A and B, key distribu can be achieved in a number of ways.

1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.

previously and recently used a key, one party can transmit the new key to the other, encrypted link using the old key. 1

4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

options 1 and 2 call for manual delivery of a key.

- If end-to-end encryption is done at a network (or) IP level, then a key is needed for each pair of hosts on the network that wish to communicate.

- Thus, if there are N hosts, the number of required key is [N(N-1)]/2.

- for end-to-end encryption, dome Variation on option 4 has been widely adopted

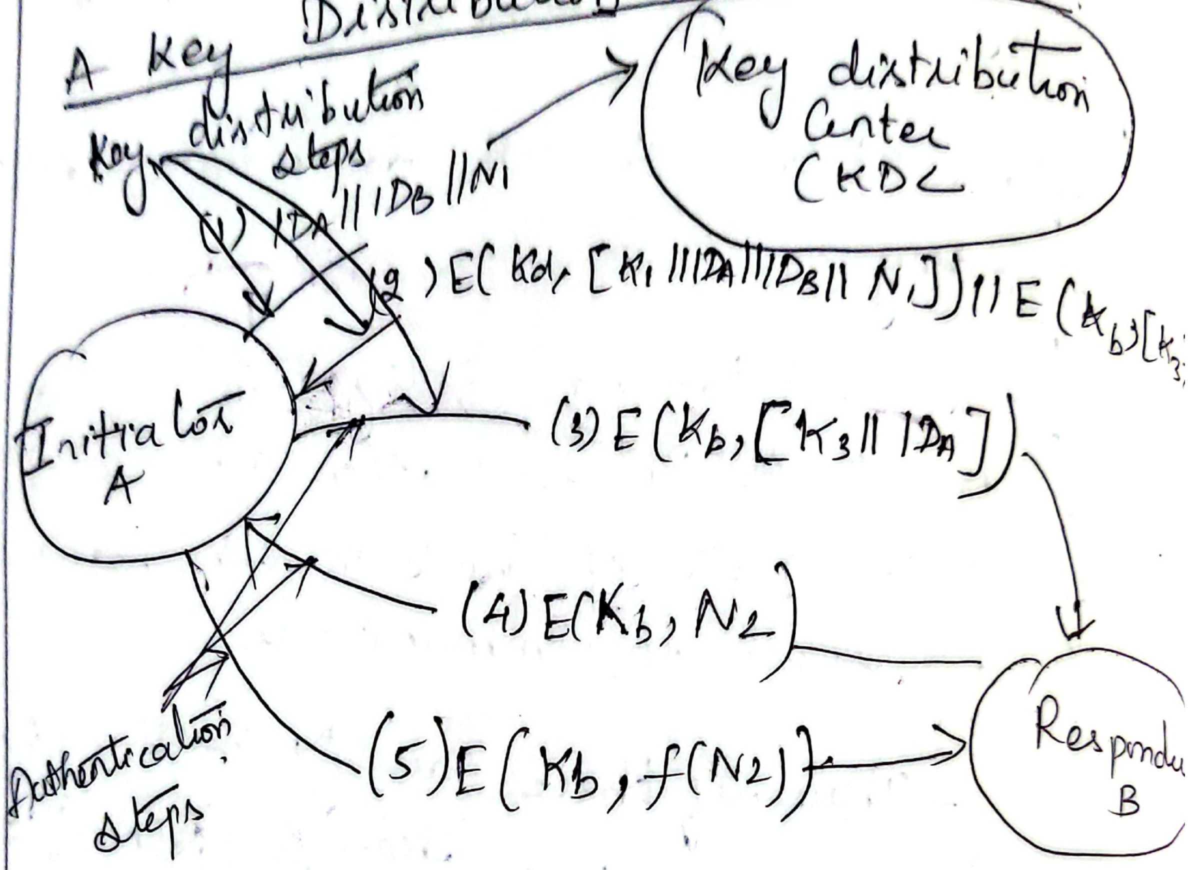
- Each user must share a unique key with the key distribution center for purposes of key distribution.

- At a minimum, two levels keys are used communication between end systems is encrypted using a temporary key.

often

Session keys are transmitted in encrypted form, using a master ke that is shared by the key distribut center and an end system (ES) user.

A Key Distribution Scenario:-



Hierarchical Key Control

- It is not necessary to limit the key distribution function to a single KDC.

- As an Alternative, a hierarchy of KDC's can be established. for communication among entities within the local domain, the local KDC is reponsible for key distribution.

- Any one of the three KDCs involved can actually select the key

Session key lifetime

* The more frequently session keys ar exchanged, the more secure they are, becau the opponent has less ciphertext to work with for any given session key.

* A security manager must try to balance these competing considerations in determining the lifetime of a particular session key

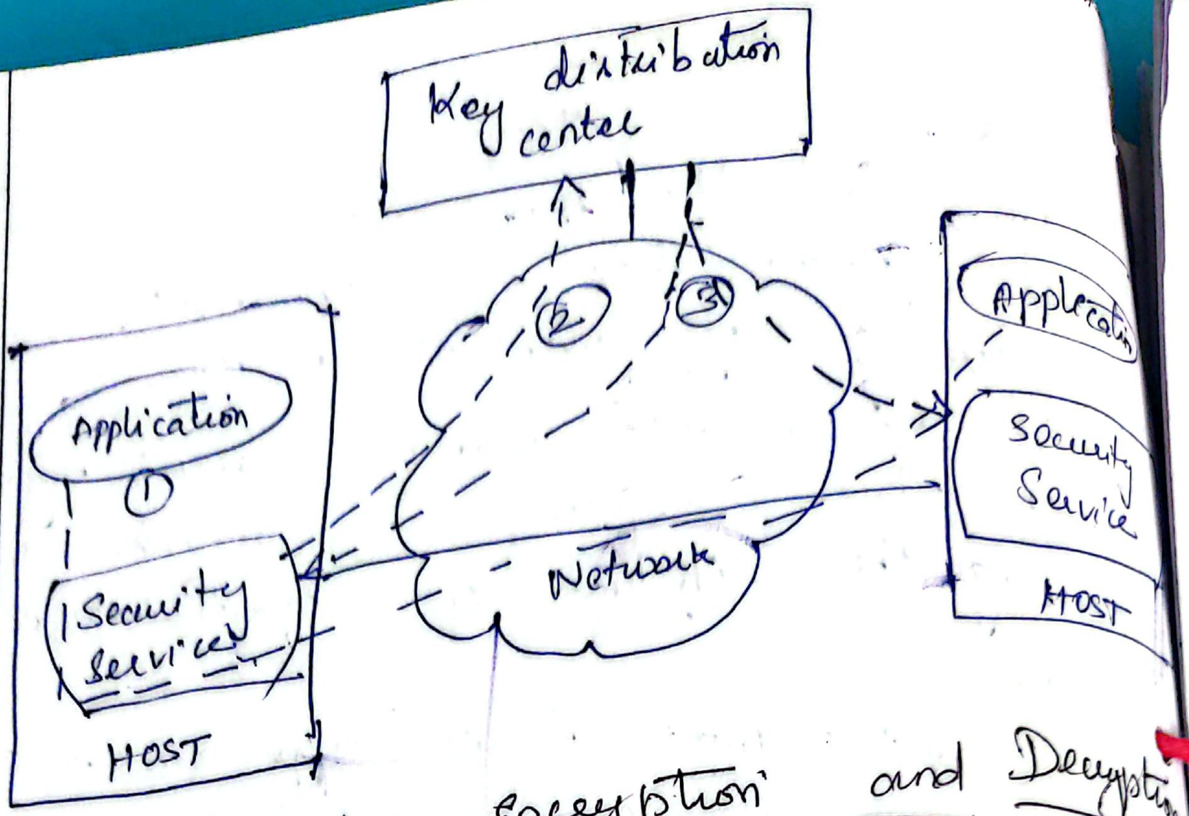
* The most secure approach is to use a new session key for each exchange.

A Transparent key control Scheme:

* The approach assumes that communication makes use of a connection-oriented end-to end protocol, such as TCP.

* The noteworthy element of this approach is a session security module (SSM), that performs end-to-end encryption and obtains session keys on behalf of its host (or) terminal.

* When one host wishes to set up a connection to another host, it transmits a connection-request packet (step 1)



Control Vector Encryption and Decryption

Hash value = $H = h(CV)$

Key input = K_m H

cipher text = $E([K_m H], K_s]$

* Where Km is the master key and Ks is the session key. The session key is recovered in plaintext by the reverse operation'

$D([K_m H], E([K_m H], K_s))$

* The session key can be recovered only by using both the master key that the user shares with the KDC and the control vector.

Unit-3 Public Key Cryptography: ①

1. Prime Numbers:-

~~The~~ Any Integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t} \text{ —— ①}$$

where $p_1 < p_2 < \cdots < p_t$ are prime numbers and where each a_i is a positive integer. This is known as the fundamental theorem of arithmetic.

$91 = 7 \times 13$

$3600 = 2^4 \times 3^2 \times 5^2$.

$$a = \prod_{p \in P} p^{a_p} \text{ where each } a_p \geq 0.$$

2. Fermat's and Euler's Theorems:-

Two fermat's states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a \times 2a \times \cdots \times (p-1)a \equiv [(1 \times 2 \times \cdots \times (p-1)] \pmod{p}$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Euler's Totient function

An importan [illegible] in number theo refered to as Euler's totient function, wr $\varphi(n)$, and defined as the number of posi integer less than n and relatively preime to, By convention, $\varphi(1) = 1$ $\boxed{\varphi(p) = p-1}$

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$$

$$\phi(n) = (pq-1) - [(q-1) + (p-1)]$$
$$= pq - (p+q) + 1$$
$$= (p-1) \times (q-1)$$
$$= \phi(p) \times \phi(q)$$

3. Chinese Remainder Theorem :-

One of the most useful results of number theory is the Chinese remainder theorem. In essence, the CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

$$M = \prod_{i=1}^{k} m_i \qquad \boxed{A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) (\text{mod } M)}$$

1. Key Mangement :-

One of the major roles of public-key encryption has been to address the problem of key distribution.

- The distribution of public keys
- The use of public-key encryption to distribute secret keys

distribution of Public keys.

- * public announcement
- * publicly available directory.
- * public-key authority
- * Public-key certificates.

2. RSA algorithm

The block size must be less than or equal to $\log 2(n)$; in practice, the block size is k bits, where $2k < n < 2k+1$

Encryption and Decryption are of the following form, for some plaintext block M and ciphertext block C.

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e \bmod n) \bmod n$$

$$= (M^e)^d \bmod n.$$

$$M^{ed} = M \bmod n$$

Key Generation

Select p, q . p, q both prime $p \neq q$

calculate $n = p \times q$

calculate $\phi(n) = (p-1)(q-1)$

select integer e $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$

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

public key $KU = \{e, n\}$

private key $KR = \{d, n\}$

Encryption:-

plaintext $M < n$

ciphertext $c = M^e \pmod{n}$

Decryption:-

ciphertext c

plaintext $M = c^d \pmod{n}$

Security of RSA

There are three approaches to attack the RSA

- * brute force key Search
- * mathematical attacks.
- * timing attacks
- * Chosen ciphertext attacks

3. Diffie - Hellman key Exchange

The purpose of the algorithm is to enable two users to exchange a key securel that can then be used for subsequent encryption of messages.

For any integer, "b" and a primitive root, "a" of a prime number, "p", we c find a unique exponent, "i" such that

$$\boxed{b \equiv a^i \bmod p, \text{ where } 0 \le P \le (p-1)}$$

* User A computes the Key as $k = (YB)^{XA} \bmod q$ and User B computes the key as $K = (YA)^{XB} \bmod q$

$$
\begin{aligned}
k &= (YB)^{XA} \bmod q \\
&= (\alpha^{XB} \bmod q)^{XA} \bmod q \\
&= (\alpha^{XB})^{XA} \bmod q \\
&= (\alpha^{XA})^{XB} \bmod q \\
&= (\alpha^{XA} \bmod q)^{XB} \bmod q \\
&= (YA)^{XB} \bmod q.
\end{aligned}
$$

Global Pulic Elements

q	prime numbe
α	$\alpha < q$ and α a primitive root of q

User A key Genration

select private X_A $\quad X_A < q$

calculate public Y_A $\quad Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

select private X_B $\quad X_B < q$

calculate public Y_B $\quad Y_B = \alpha^{X_B} \bmod q$

~~UserB~~ **Calculation of Secret key by User A**

$k = (YB)^{XA} \bmod q$

Calculati of Secret key by User B

$k = (YA)^{XB} \bmod q$

8.2 Elliptic curve cyptography.

The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple addition is the counterpa of modular exponentiation.

Consider the equation $Q = kP$ where $Q, P \in Ep(a,b)$ and $k < p$. It is relatively easy to calculate Q given k and P, but it relatively hard to determine k given and P.

ECC Duffie-Hellman key Exchange

Global public Elements

$E_q(a,b)$ - elliptic curve with parameters a, and q, when q is a prime or an integer of the form 2^m

G - point on elliptic curve whose order is large value n.

User A key Generation

Select private n_A. $n_A < n$

calculate public P_A $P_A = n_A \times G$

User B key Generation

Select private n_B $n_A < n$

calculate public P_B $P_B = n_B \times G$

calculation of Secret key by user A

$K = n_A \times P_B$

calculation of Secret key by user B.

$K = n_B \times P_A$

10. Elgamal Cryptographic System

we can restate the Elgamal process as follows:

1. Bob generates a random integer k

2. Bob generates a one-time key K using Alice's public key components YA, q and k

2. Bob encrypts k using the public-key component α, yielding C1. C1 provides different information for Alice to recover K.

4. Bob encrypts the plaintext message M using K.

5. Alice recovers K from C1 using her private key.

6. Alice uses K-1 to recover the plaintext message from C2.

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice

Select private X_A	$X_A < q-1$
calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
public key	$PU = \{q, \alpha, Y_A\}$
private key	X_A

R.a ll 1-

Encryption by bob with Alice's Public

plaintext: $M < q$

delect random integer k $k < q$

calculate K $K = (Y_A)^k \bmod q$

Calculate C_1 $C_1 = \alpha^k \bmod q$

Calculate C_2 $C_2 = KM \bmod q$

ciphertext: (C_1, C_2)

Decryption by Alice with Alice's Private k

Cipher text: (C_1, C_2)

Calculate K: $K = (C_1)^{XA} \bmod q$

plaintext: $M = (C_2 K^{-1}) \bmod q$

11. Differential Cryptanalysis:-

The prime concern with DES has been its vulnerability to brute-force attack because of its relatively short (56 bits) key length.

The two most powerful and promising approaches are differential cryptanalysis and linear cryptanalysis.

Differential cryptanalysis

one of the mast significant advances in cryptaralysis is differential cryptanalysis.

Differential cryptanalysis is the first published attack that is capable of breaking DES in less than 2^{55} encryptions. The scheme com successfully cryptanalyze DES with an effort on the order of 2^{55} encryptions, requiring 2^{47} Chosen plaintext.

Although differential cryptanalysi is a powerful tool, it does not do very well against DES. The need to strengthen DES against attacks using differential cryptanalysis played a large part in the design of the S-boxes and the permulation - P.

Differential cryptandysis attack:- The differenlial cryptanalysis attack is complex.

Consider the original plaintext block m to consist of two halves m0, m1. Each round of DES maps the right-hand input into the left - hand output and sets the right hand output to be the function of the hand input and the subkey for thi round.

If we label each new block m_i (2....i.. than the intermediate message halves are related as follows:-

$$m_{i+1} = m_{i-1} \oplus f(m_i, k_i), \quad i = 1, 2, \ldots, 16.$$

In differential cryptanalysis, we start wi two messeyes , m and m', with a known xo diffeance XOR diffeence $\Delta m = m \oplus m'$, and cons the difference between the intermediate m halves $\Delta m = m_i \oplus m'_i$. Then we have

$$\Delta m_{i+1} = m_{i+1} \oplus m'_{i+1}$$

$$= [m_{i-1} \oplus f(m_i, k_i)] \oplus [m'_{i-1} \oplus f(m'_i$$

$$= \Delta m_{i-1} \oplus [f(m_i, k_i) \oplus f(m'_i, k_i)]$$

Now, suppose that many pairs of inputs to f with the same diffeence yield the same output difference if the same subkey is used. To put this more precisely, let us say that X may cause Y with probability p, if for the fraction p of the pairs in which the input XOR is X, The output XOR equals Y.

Therefore, if we Know Δ input XOR is X, the output XOR equals Y. furthermore if a number of such differences are determined, it is feasible to determine the subkey used in the function f. The overall strategy of differential cryptanalysis is based on these considerations for a single round. The procedure is to begin with two plaintext messages m and m_i with a given difference and trace through a probable pattern of differences after each round to yield a probable difference for the Ciphertext.

$$\boxed{E(K,m) \oplus E(K,m') = (\Delta m_{17} \| \Delta m_{16})}$$

then we suspect that all the intermediate probable patterns at all the rounds are correct. With that assumption, we can make some deductions about the key bits. This procedure must be repeated many times to determine all the key bits.

The probabilities shown on the right refer to the probability that a given set of intermediate differences will appear as a function.

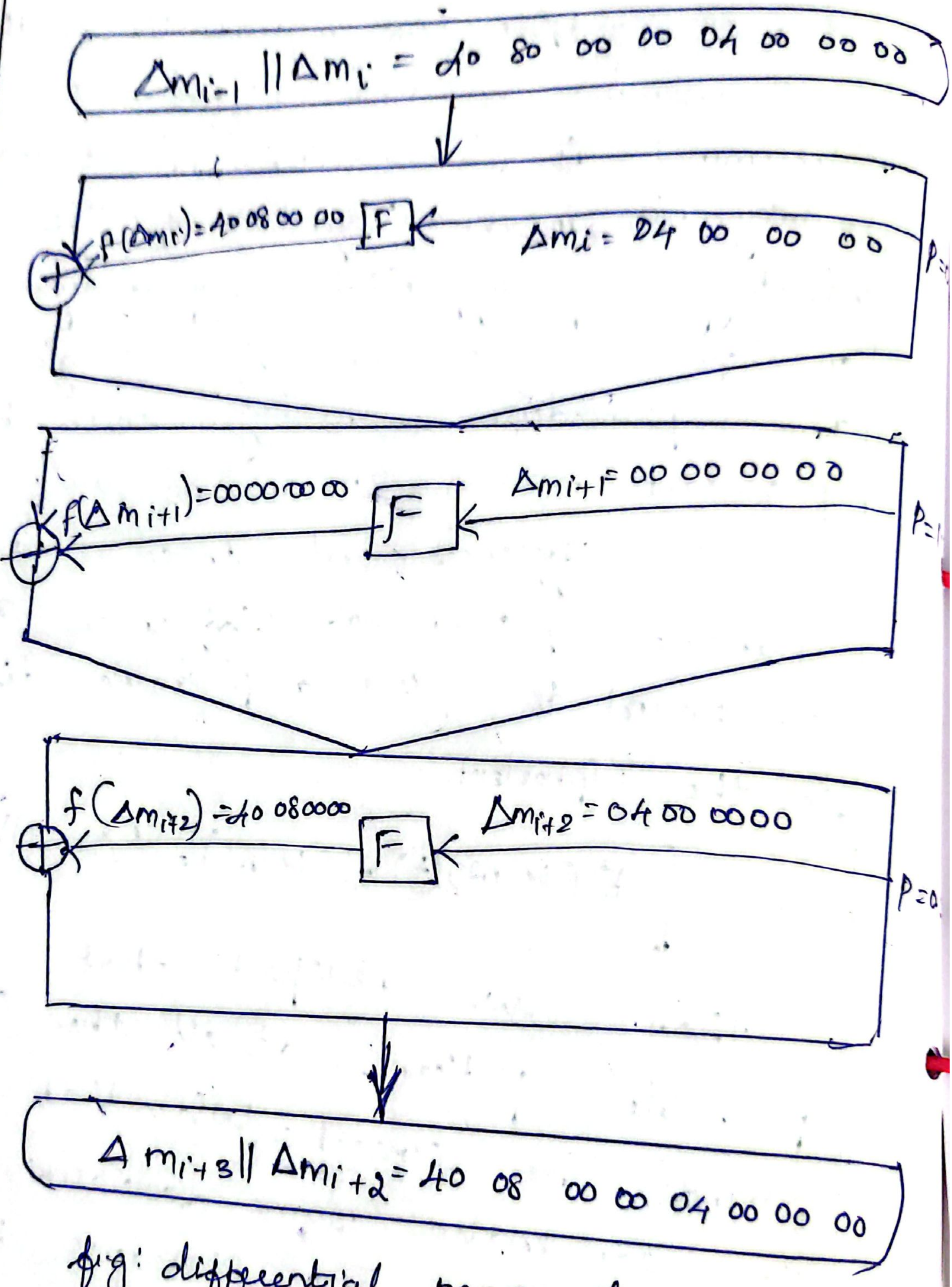

$\Delta m_{i-1} || \Delta m_i$ = 40 80 00 00 04 00 00 00
$f(\Delta m_i)$= 40 08 00 00
F
Δm_i = 04 00 00 00
P=
$f(\Delta m_{i+1})$=00000000
F
Δm_{i+1}= 00 00 00 00
P=1
$f(\Delta m_{i+2})$ =40 080000
F
Δm_{i+2} = 04 00 0000
P=0.
$\Delta m_{i+3} || \Delta m_{i+2}$= 40 08 00 00 04 00 00 00

fig: differential propagation through the Rounds of DES.

Overall, after three rounds, the probability that the output difference is as shown is equal to 0.25 × 1 × 0.25 = 0.0625.

Linear Cryptanalysis:

A more recent development is linear cryptanalysis. This attack is based on finding linear approximations to describe the transformations performed in DES. This method can find a DES key known plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis.

We now give a brief summary of the principle on which linear cryptanalysis is based. For a cipher with n-bit plaintext and ciphertext blocks and an m-bit key. Let the plaintext block be labeled P[1]... P[n], the cipher text block C[1],... C[n], and the key K[1]....K[m]. Then define.

$$A[i, j, \ldots, k] = A[i] \oplus A[j] \oplus \cdots \oplus A[k]$$

The objective of linear cryptanalysis is to find an effective linear equation of the form:

$$P[\alpha_1, \alpha_2, \ldots \alpha_a] \oplus C[\beta_1, \beta_2, \ldots \beta_b] = K[\gamma_1, \gamma_2, \ldots \gamma_c]$$

(where $x = 0$ or 1; $1 <= a$; $b <= n$; $c <= m$; and where the a, b and g terms represent fixed, unique bit locations) that holds with probability $p != 0.5$. the further p is from 0.5, the more effective the equation. Once a proposed relation is determined, the procedure is to compute the results of the left-hand side of the preceding equation for a large number of plaintext-ciphertext pairs.

If the result is 0 more than half the time, assume $k[1,2,\ldots,c]=0$, If it is 1 most of the time $k[1,2,\ldots,c]=1$. This gives us a linear equation on the key bits. Try to get more such relations so that we can solve for the key bits. Because we are dealing with linear equations, the problem corn be approached on round of the cipher at a time, with the results combined.

—— X ——

Chinese Remainder Theorem :

$A \leftrightarrow (a_1, a_2, \cdots a_k) \rightarrow \circledast$

where $A \in Z_m$, $a_i \in Z_{m_i}$ and $a_i = A \bmod m_i$ for $1 \leq i \leq k$. The CRT makes two assertion :

(1) The mapping of equation $\circledast$ is a one-to-one correspondence (called a bijection) between Z_m and the Cartesian product $Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_k}$. That is, for every integer A such that $0 \leq A \leq M$, there is a unique k-tuple $(a_1, a_2, \cdots a_k)$ with $0 \leq a_i < m_i$ that represents it, and for every such k-tuple $(a_1, a_2, \cdots a_k)$, there is a unique integer A in Z_m.

(2) Operations performed on the elements of Z_m can be equivalently performed on the corresponding k-tuples by performing the operations independently in each coordinate position in the appropriate system.

Let us demonstrate the first assertion. The transformation from A to $(a_1, a_2, \cdots a_k)$ is obviously unique; that is each a_i is uniquely calculated as $a_i = A \bmod m_i$

Computing A from $(a_1, a_2, \cdots a_k)$ com be done as follows. Let $M_i = M[m_i$ for $1 \le i \le k$. Note that $M_i = m_1 \times m_2 \times \cdots \times m_{i-1} \times M_{i+1} \cdots m$ Also that $M_i = 0 (\bmod m_i)$ for all $j \neq i$. Then let.

$$c_i = M_i \times (M_i^{-1} \bmod m) \text{ for } 1 \le i \le k.$$

$$A = \left(\sum_{i-1}^{k} a_i c_i\right) (\bmod M) \longrightarrow ①$$

To show that the value of A produced by equation ① is correct, we must show that $a_i = A \bmod m_i$, for $1 \le i \le k$.

Note that $c_j \equiv M_j \equiv 0 \ (\bmod m_i)$ if $j \neq i$, and that $c_i \equiv 1 (\bmod m_i)$. It follows that $a_i = A \bmod m_i$.

The second assertion of the CRT, concerning arithmetic operations, follows from the rules for modular arithmetic. That is, the second assertion com be stated as follows. If

$$A \leftrightarrow (a_1, a_2, \cdots a_k)$$

$$B \leftrightarrow (b_1, b_2 \cdots, b_k)$$

then $(A+B) \bmod M \longleftrightarrow ((a_1+b_1) \bmod m_1, \ldots (a_k+b_k) \bmod m_k)$

$(A-B) \bmod M \longleftrightarrow ((a_1-b_1) \bmod m_1, \ldots (a_k-b_k) \bmod m_k)$

$(A \times B) \bmod M \longleftrightarrow ((a_1 \times b_1) \bmod m_1, \cdots (a_k \times b_k) \bmod m_k)$

one of the useful featur of the chinease remaindu theorem is that it provides a way to manipulate (potentialy very large) numbers mod M in tams of tuples of smaller numbers. This can be useful when M is 150 digits (or) more. However, note that it is necessary to know beforehand the factorization of M.

To represent 973 mod 1813 as a pair of numbers mod 37 and 49, define

$m_1 = 37$

$m_2 = 49$

$M = 1813$

$A = 973$

we also have $M_1 = 49$ and $M_2 = 37$. Using the extended Euclidean algorithm, we compute $M_1^{-1} = 34 \bmod m_1$ and $M_2^{-1} = 4 \bmod m_2$

Taking residues modulo 37 and 49,

Our representation of 973 is (11, 42).

because 973 mod 37 = 11 and 973 mod 49 =

Now suppose we want to add 678 to 973.

$(678) \leftrightarrow (678 \bmod 37,\ 678 \bmod 49) = (12, 41$

→ Then we add the tuples element wise and reduce $(11 + 12 \bmod 37,\ 42 + 41 \bmod 4$

$(23, 34)$.

To verify that this has the correct effect, we compute

$$(23, 34) \longleftrightarrow a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} \bmod M$$

$$= [(23)(49)(34) + (34)(37)(4)] \bmod 1813$$

$$= 43350 \bmod 1813$$

$$= 1651.$$

$(973 + 678) \bmod 1813 = 1651.$

We multiply (23, 34) by 73 and reduce get $(23 \times 73 \bmod 37,\ 34 \times 73 \bmod 49) = (14, 32)$

It is easily verified.

$$(14, 32) \longleftrightarrow [(14)(49)(34) + (32)(37)(\quad \bmod 1813$$

$$= 865$$

$$= 1651 \times 73 \bmod 1813.$$

Unit IV.

MESSAGE AUTHENTICATION AND INTEGRITY

Authentication requirement - Authentication function - MAC - Hash function - Security of hash function and MAC - SHA - Digital signature and authentication protocols - DSS - entity Authentication : Biometrics, passwords, Challenge Response protocols - Authentication ~~protocols~~ applications Authentication ~~ke~~ Beros, X 509.

1.1 Authentication Requirements.

communication across the network, these following attacks can be identified.

Disclosure :

release of message contents to any person or process not possessing the appropriate cryptographic key.

Traffic analysis :

discovery of the pattern of traffic between parties.

1) in a connection oriented application

2. In a eifher a connection oriented or connection less environment.

Masquerade.

Insertion of message into the network from fraudulent source.

content modification

change to the contents of the message including insertion deletion, transposition ,deletion and recording.

Sequence modification.

Any modification to a sequence of message between parties. including insertion, deletion and modification.

Timing modification:

delay or replay of message.

Source of repudiation

denial of transmission of message by Source

Destination repudiation

denial of receipt of message by destination

(ii) Authentication Function

Any message authenticator or degital signature mechanism can be viewed as two level.

Lower Level :-

There must be some sort of function that provides an authenticator, a value to be used to authenticate a message.

At the higher level.

Authentication protocols that enabled a receiver to verify the authenticity of message.

Message encryption

Ciphertext of entire message serves as its authenticator

Message authentication code:

A public function of the message and a secret key that produces a fixed length values that serves as the authenticator

Hash function:

A public function that maps a message

of any length into a fixed length hash value which serves as a authenticator.

Message encryption

message encription by itself can provide a measoore of authentication.

The anlysis differs from Symmetric and public key encryption schemes

(a) if symmetric encryption is used then

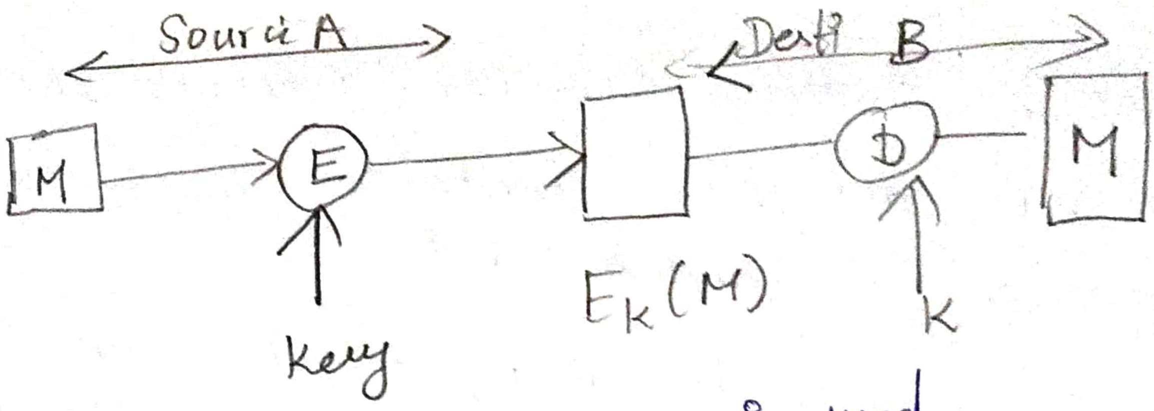
→ a message m transmitted from soure A to destination B is encrypted using a Secret key shared A and B.

→ Since only sender and receiver knowns key used

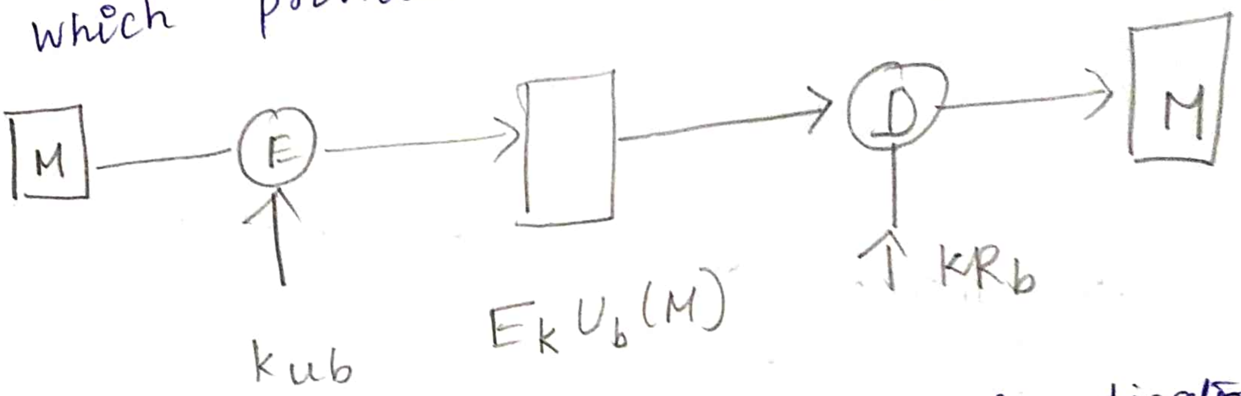
→ Receiver knows sender must have created it, Hence authentication is provided

→ if message has suitable structure redundancy or a checksum to detect any changes

→ therefore symmetric encryption provides authentication and confidentiality



(b) if public key encryption is used this method is use of public key cryptigraphy which provides confidentiality only.

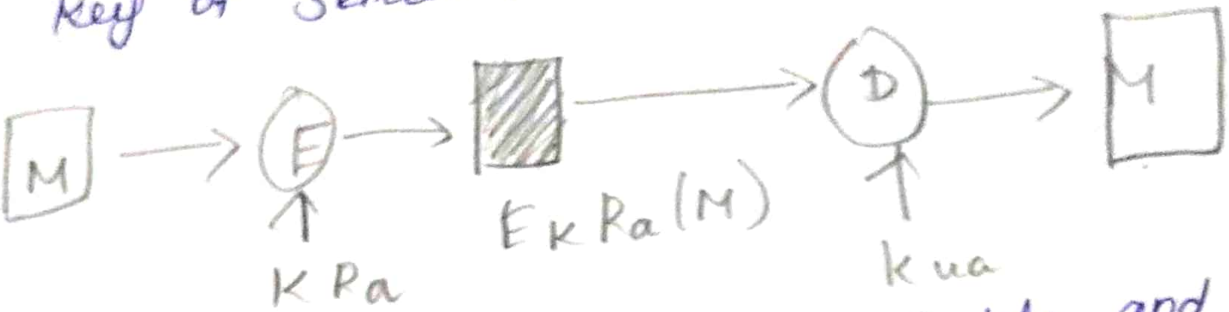


→ inthis method it have only authenticaton the message is encrypted with the sender'A is a private key. the receiver B uses the sender is A ^ is a public key decrypt the message. Now A cannot deny that it has not transmitted since it only knowns its private key.

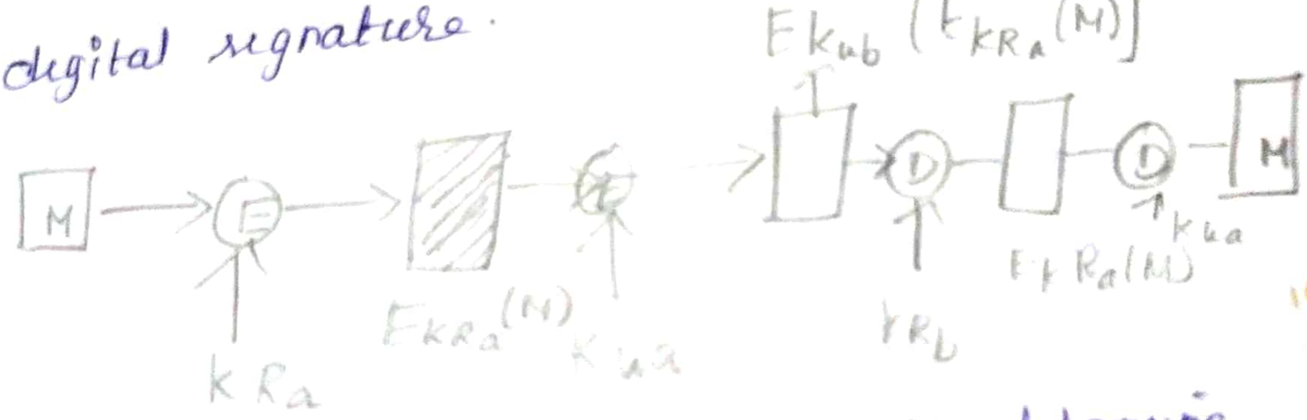
→ this is called as authenticaton or digital signature.

→ Receiver cannot determine whether the packet decrypted contains some useful message or random bits

→ The problem is that anyone can decrypt the message when they know the public key of Sender A.



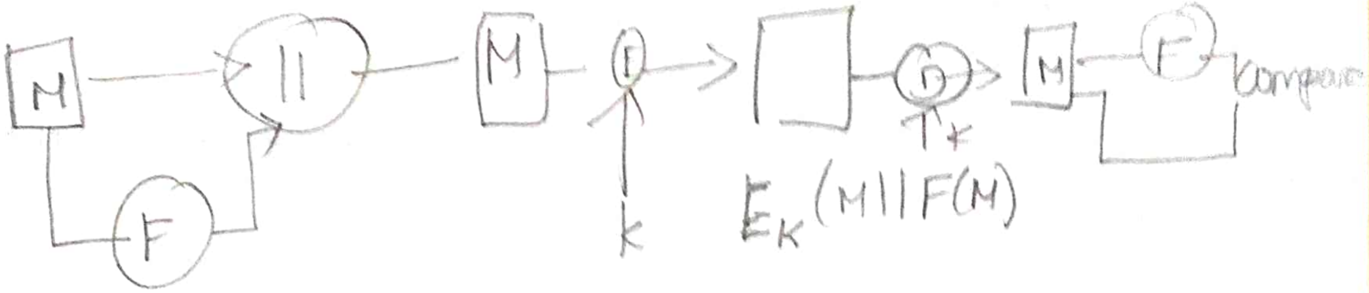
this method provides confidentialdy and digital signature.



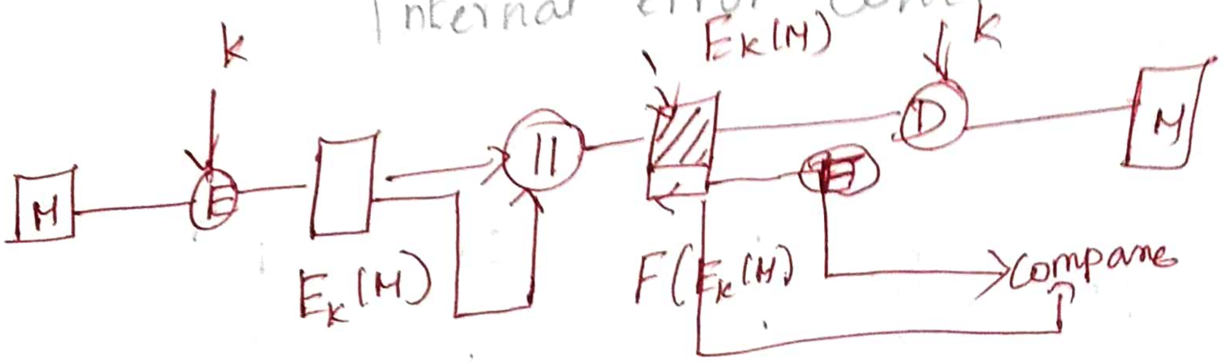
inthis case there is no way to determine automaticically, at the destination whether an incoming message is the ciphertext of a legitimate message.

Append an error detecting code, also known as frame check srequence (or) "check sum"

Althe destinalion B decrypts the incoming block and treats the result as a message with appended FCS. B applies the same function F to attempt ti reprodcee the FCS.



internal error control



External error Control.

(iii) MAC.

An alternative authentication technique involves the use of secret key ti generate a small fixed size block of data. known as cryptographic Checksum or MAC is appended to the message.

This techniques assues that two communication parties say A and B share a common secret 'k' when A has to

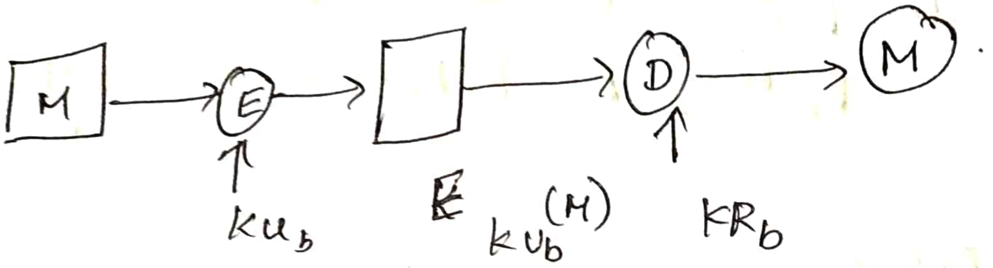
Sends a message B it calculates the MAC as a function of the message and the key.

$$MAC = C_K(M)$$

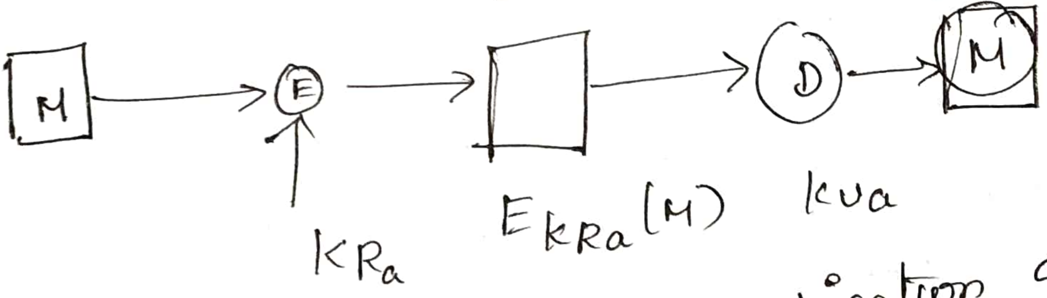
M → input message   K → Shared Secret key

C → MAC function

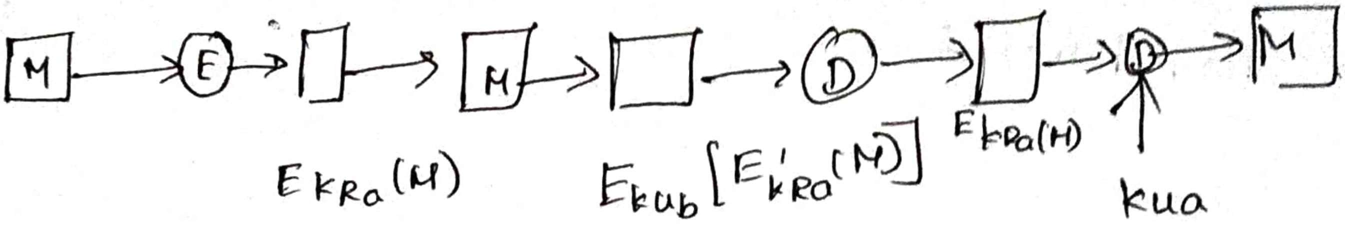
message plus MAC are transmitted to the intended recipient. the receiptent performs same calculation on received message. using some secret key generate a new MAC.



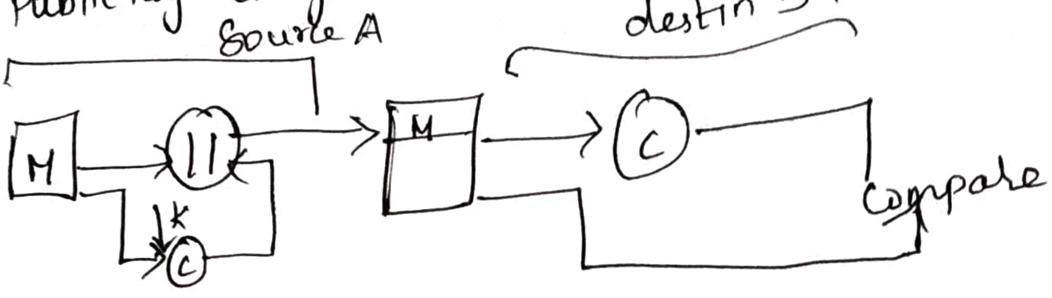
(a) Public key encryption Confidentiality



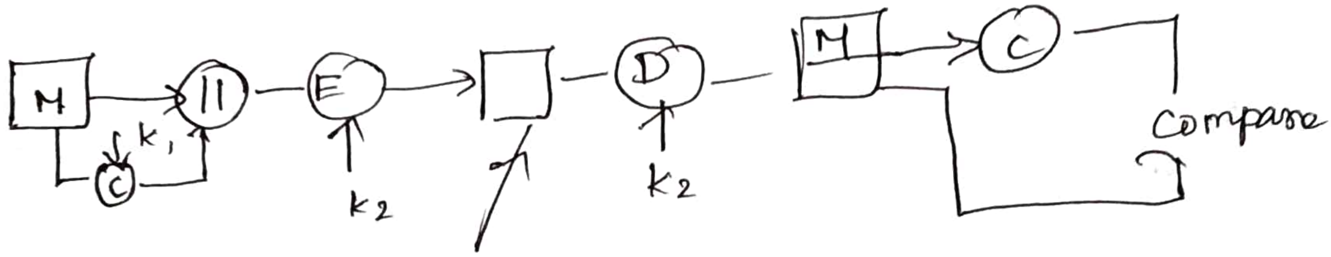
Public key encryption : Authentication and signature.



Public Key encryption : confi . Auth, Signature

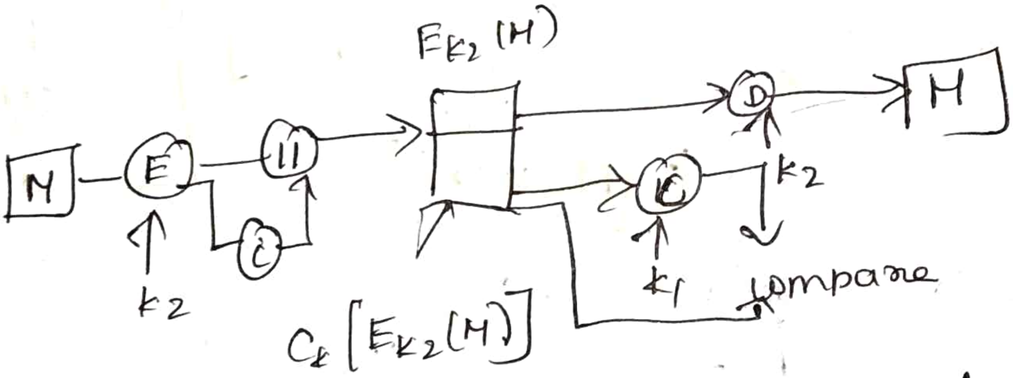


Message authentication



$E_{K2}[M || C_{K1}(M)]$

Mess authen & conf Authentication tied to plaintext



Message Authent and confi Authentication

to Plaintext

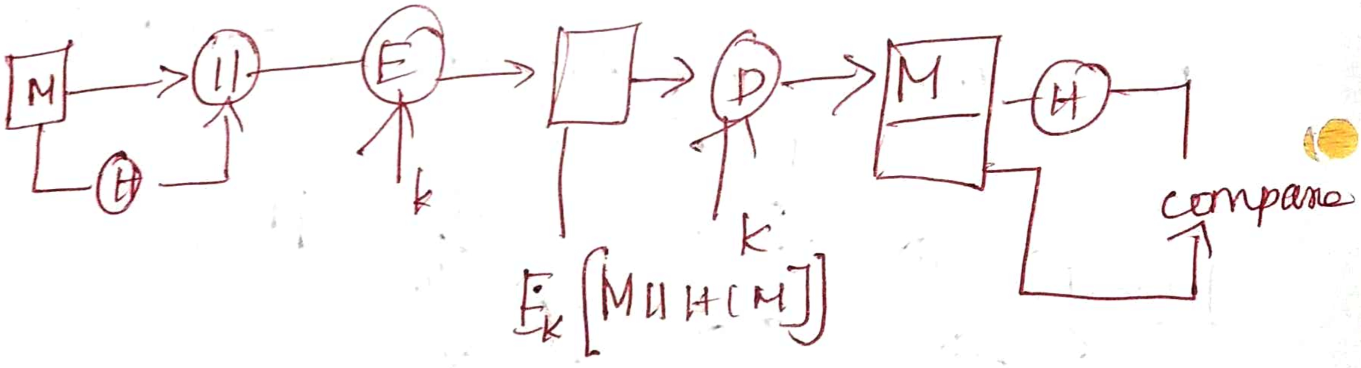
Authentication of computer program in plaintext is an alternative service.

Hash Function

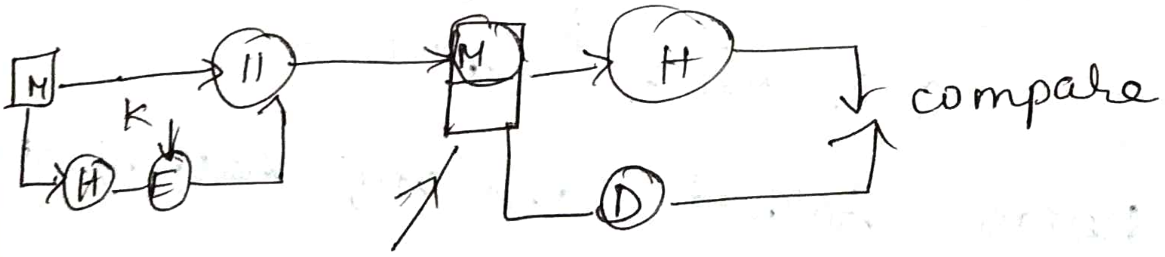
A variation of the message authentication code is one way hash function as with the message authentication code hash function that accepts a variable size message M as input and produces ~~a~~ fixed size output referred to hash code.

1) This hash code is also referred to as a message digest (MD) or hashcode.

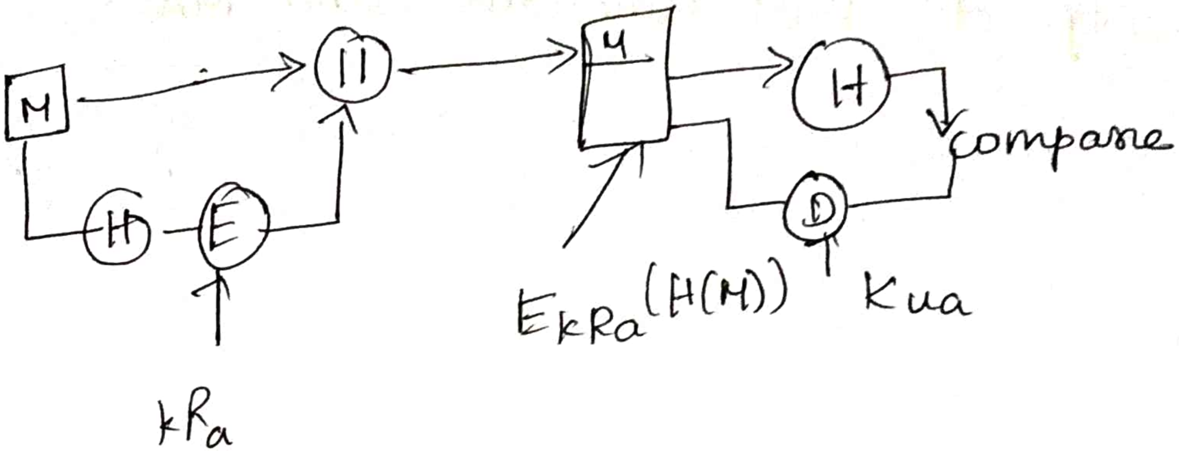
2) The hash code is a function of all the bits of all the bits of the message and provides an error detection techniques

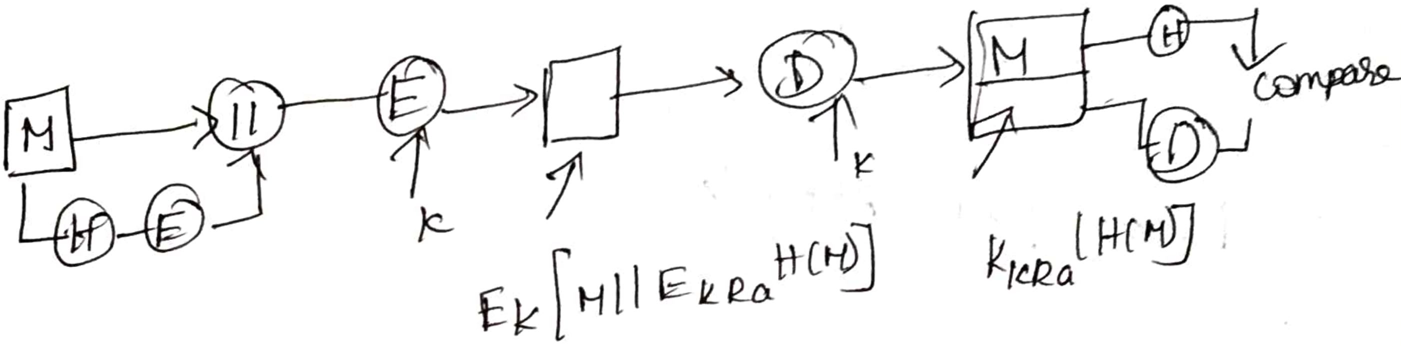


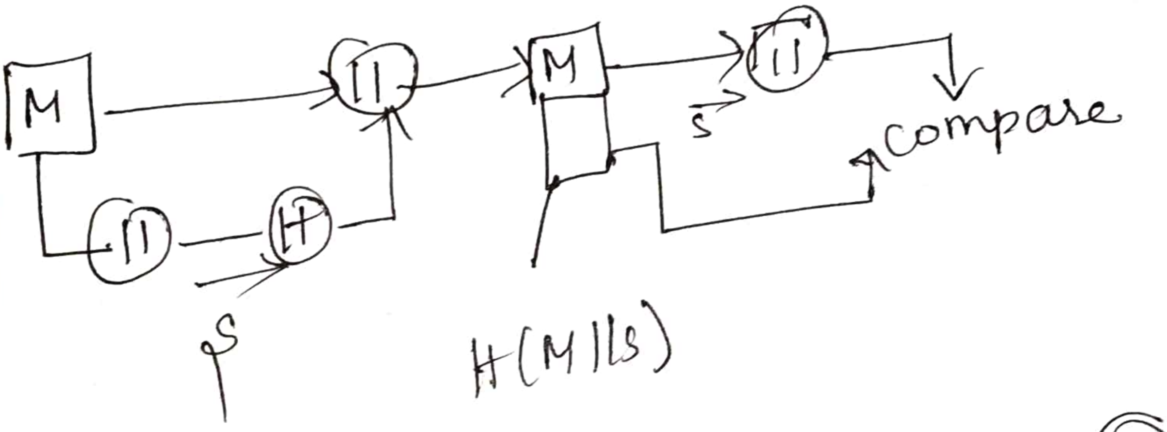
$E_k[M || H(M)]$

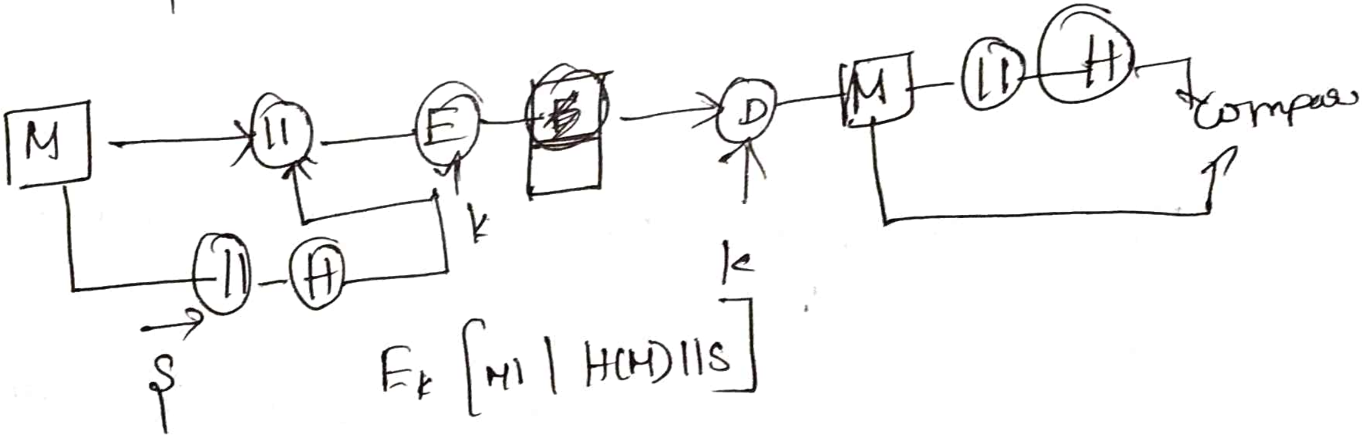


$E_k\ H(M)$.


M
||
M
H
compare
H
E
D
KR_a
$E_{KRa}(H(M))$
K_{ua}


M
||
E
D
M
H
compare
H
E
D
k
k
$E_k[M||E_{KRa}H(M)]$
$K_{KRa}[H(M)]$


M
||
M
||
compare
||
H
S
S
H(M||S)


M
||
E
D
M
||
H
compare
||
H
k
k
S
$E_k[M||H(M)||S]$

Security of Hash functions and MACs

It is a symmetric and public key encryption attacks on hash function and MAC's into two categories

1. Brute force attacks
2. cryptanalysis

Brute force Attacks.

the nature of brute force attacks between differ from some what for hash function and MACs.

Hash function

one way - for any given code h. It is computationally infeasibile to find x such that $H(x) = h$

Weak collision resistance: for any given block x it is computationally infeasibible to find $y \neq x$ with $H(y) = H(x)$

Strong collision resistance: It is computatonally in feasible to find any pair (x, y) such that $H(x) = H(y)$

Message authent icalton code:

A brute force attack on a mAc is more diffcult under the kind it requires known message - mAC pairs

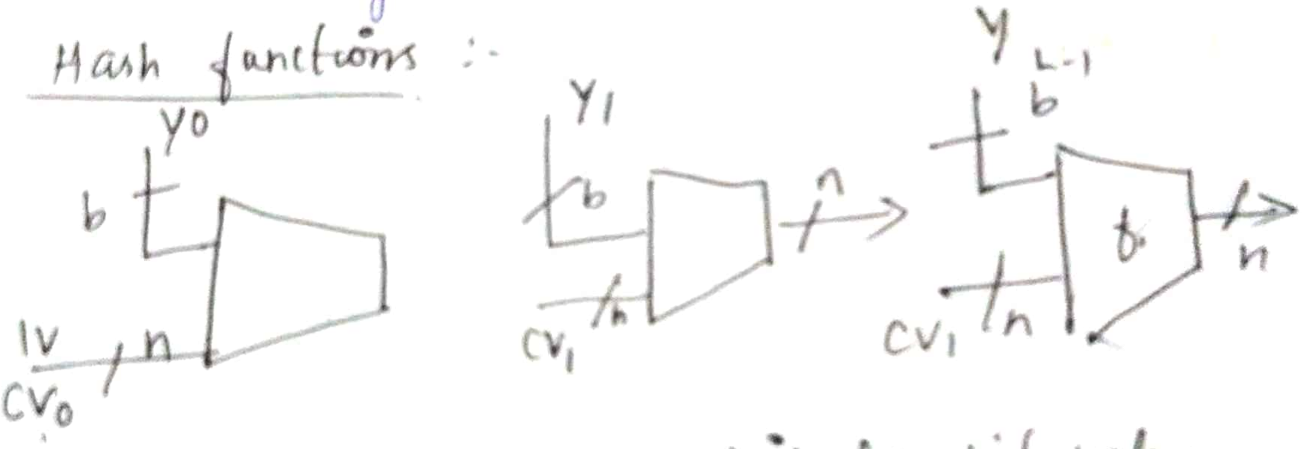
fixed Message x with n bit hash code $h = H(x)$

brute force method finding a collision is pick a random bit string y and check $H(y) = H(x)$

crypto Analysis.

is way measure the resistance of mAC algorithm is cryptoanalysis is compare the strength

Hash functions :-



$CV_0 = IV =$ initial n-bit value

$CV_i = f(CV_{i-1}, Y_{i-1}) \quad 1 \le i \le L$

$H(M) = CV_L$

The input to the hash functions is a message m consisting of blocks $y_0 \cdot\cdot y_1 \cdot\cdot y_2 \cdot\cdot\cdot$

Message authentication codes.

MAC have a variety in structure of MACs then in hash function so it difficult to generalize about crypto analysis of MAC's.

SECURE HASH ALGORITHM (SHA)

SHA developed by national institute of standards and Technology.

It is based on the MD4 algorithm and is design closely models MD5

1. SHA 1 Logic.

The alogorithm takes as a input message with maximum length of less than 2^{64} bits and produces as output a 160 bit message digest

The input is processed in 512 bit block.

Step 1 append padding bits.

the message is padded. So that is length is congruent to 448 module 512 [length = 448 mod 512)

Step 2. Append Length.

A block 64 bits is appended to the message.

Step 3 Initialize MD5 buffer

A - 67542301

B = EFCD AB89

C = 98BA DCFE

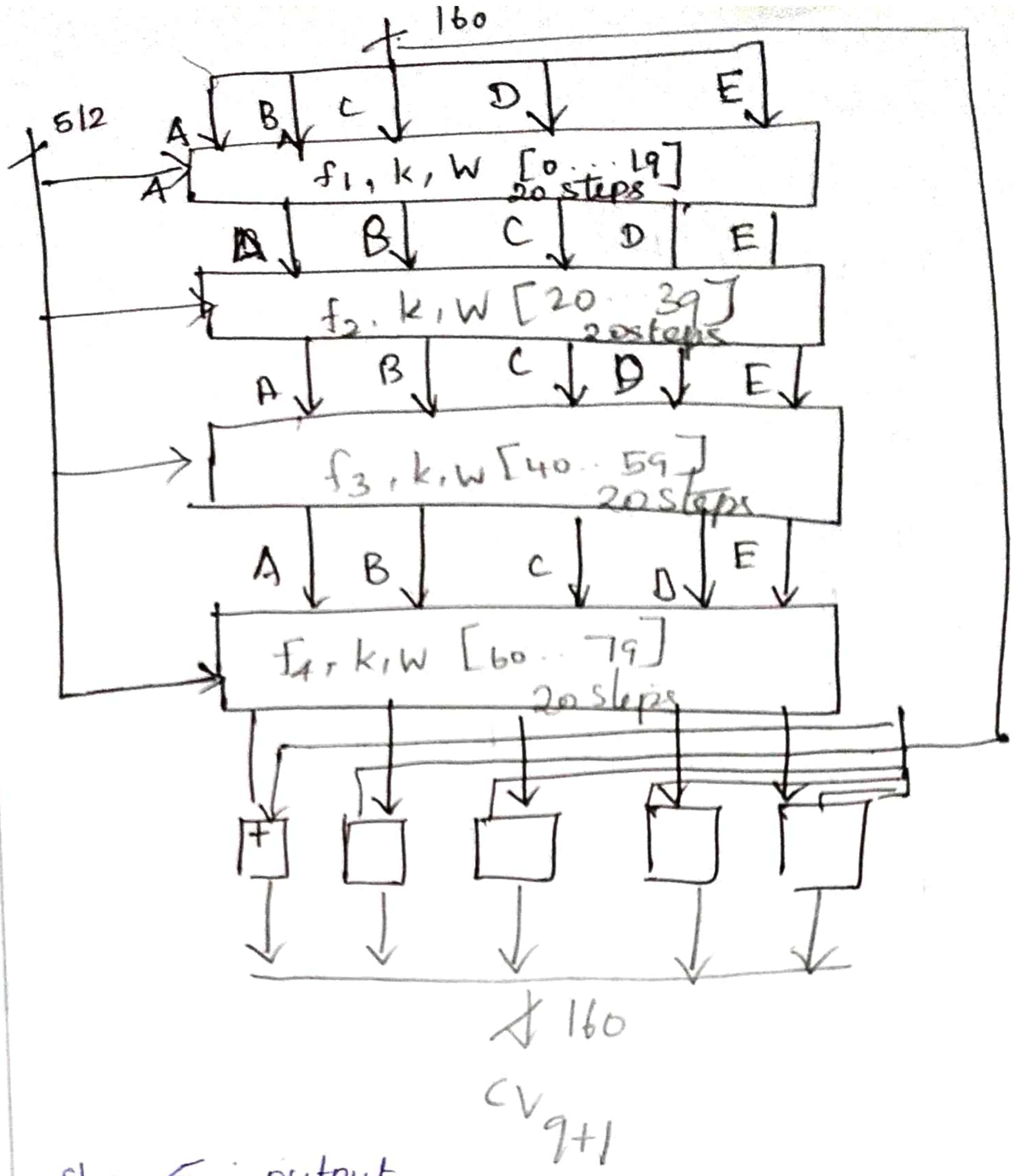
D = 103 25476

E = C3D2 E1F0

Word A :	67	54	23,	01
Word B .	EF.	CD	AB	89
word c	98	BA	DC	FE
word D	10	32	54	76
Word E	C3	D2	E1	F0

Step 4 process message in 512 block (16 word) blocks.

Step number	Hexadecimal	take integer part of
$0 \leq t \leq 19$	K_t = 5A827999	$[2^{30} \times \sqrt{2}]$
$20 \leq t \leq 39$	K_t = 6ED9EBA1	$[2^{30} \times \sqrt{3}]$
$40 \leq t \leq 59$	K_t = 8F1 BB CDC	$[2^{30} \times \sqrt{5}]$
$60 \leq t \leq 79$	K_t = CA626CD6	$[2^{30} \times \sqrt{10}]$



Step 5 : output

$Cv_0 = IV$, $CV_{q+1} = SUM_{32}(CV_q, ABCDE_q)$

$MD = CV_L$

IV → initial value of ABCDE

L → no of blocks in message

MD – final message digest value.

$ABCDE_q$ = o/p of Last round processing q^{th} message block.

SHA2

logic of the 80 steps in the processing one 512 bit block

$$A\,B\,C\,D\,E \leftarrow (E + f(t, B, C, D) + S^{5}(A) + W_t + K_t), A, S^{30}(B), C, D.$$

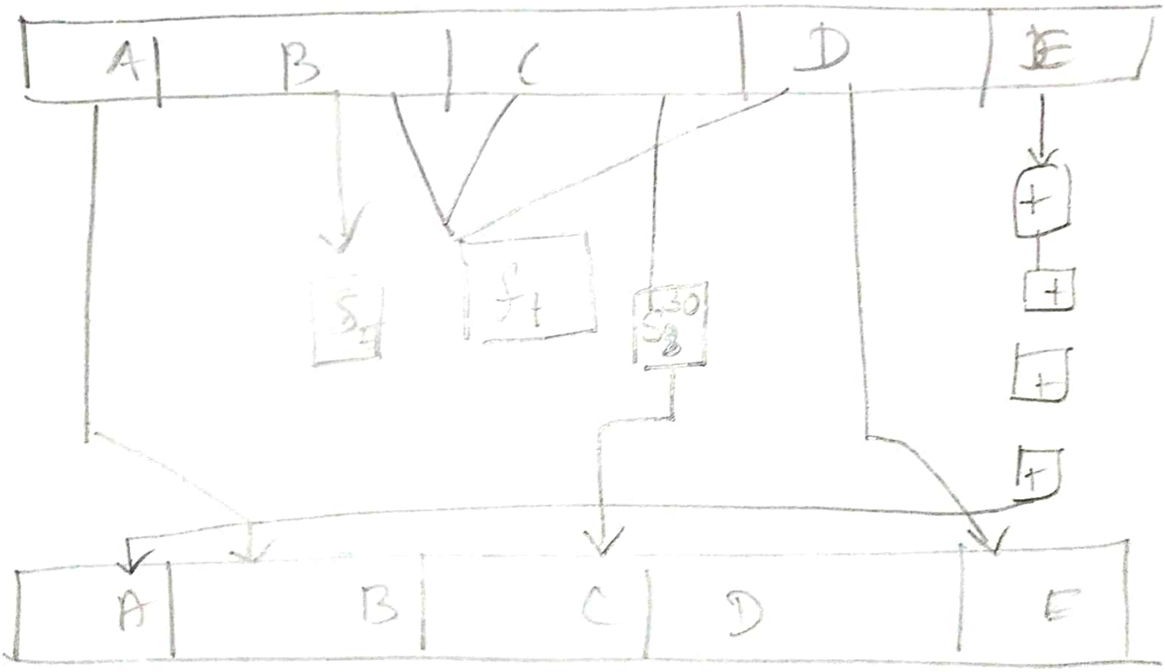
Where

s^k circular left shift of 32 bit

W_t → 32 bit word derived from current 512 bit input block

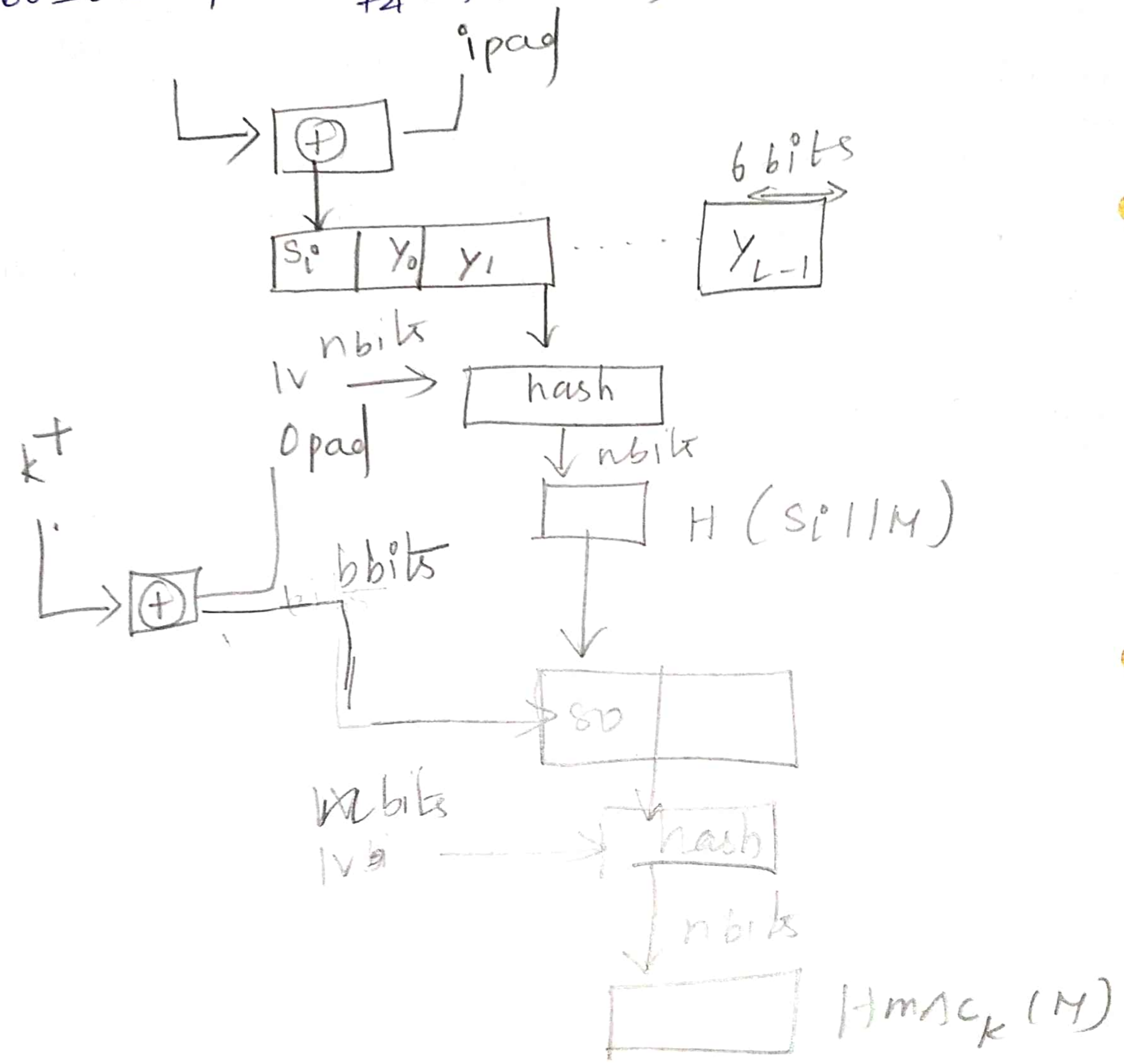
K_t additive constant

t step number



elementry SHA operation

Step no	function name	function
$0 \le t \le 19$	$f_1 = f(t, B, C, D)$	$B \wedge C \vee \overline{B} \wedge D$
$20 \le t \le 39$	$f_2 = f(t, B, C, D)$	$B \oplus C \oplus D$
$40 \le t \le 59$	$f_3 = f(t, B, C, D)$	$(B \wedge C \vee (B \wedge D) \vee (C \wedge D)$
$60 \le t \le 79$	$f_4 = f(t, B, C, D)$	$B \oplus C \oplus D$



Comparsion of SHA1 and MD5

✓ Security agaist brut force

Attacks - 2^{128} operalions for MD5

2^{160} opeoations for SHA1

security against cryptanalysis

SHA1 → (vulnearable eettacks)

speed

SHA-1 (160 bit buffer)

MD5 · (128 bit buffer)

Simplicity and compactness

6) Digital signature.

It provides a set of security capabilities that would be difficult to implement in any other way.

Requirements

message authentication provides the protection two parties who one exchang message from any third party several forms of dispute between the two ano possible.

Scenario: 1

Many may forge a different message and claim that it came from John, Mary would simply have to create message and append an code for authentication using key that John and mary share

Scenario: 2.

John can deny Sending the message. Because it is possible for mary to forge a message there is no way to prove that John did in fact send the message.

properties.

(i) It must verify the author and date & time of the signature

(ii) It must authenticate the contents at the time of signature

(iii) It must be verifiable by third parties to resolve disputes.

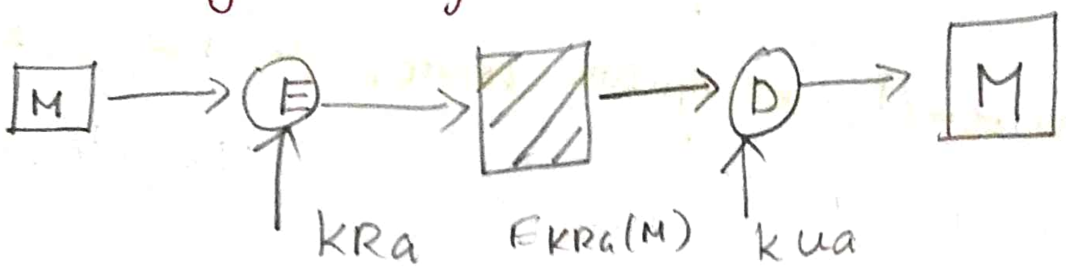
So digital signature includes authentication function.

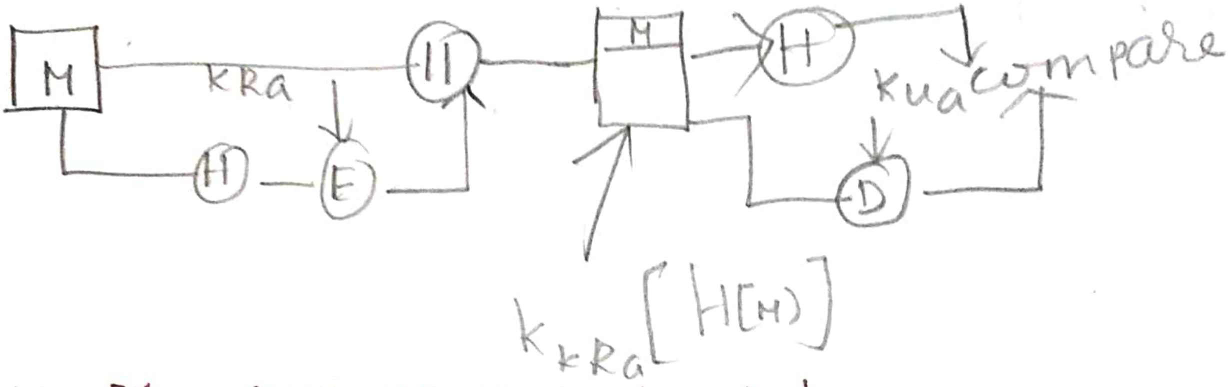
Types

→Direct

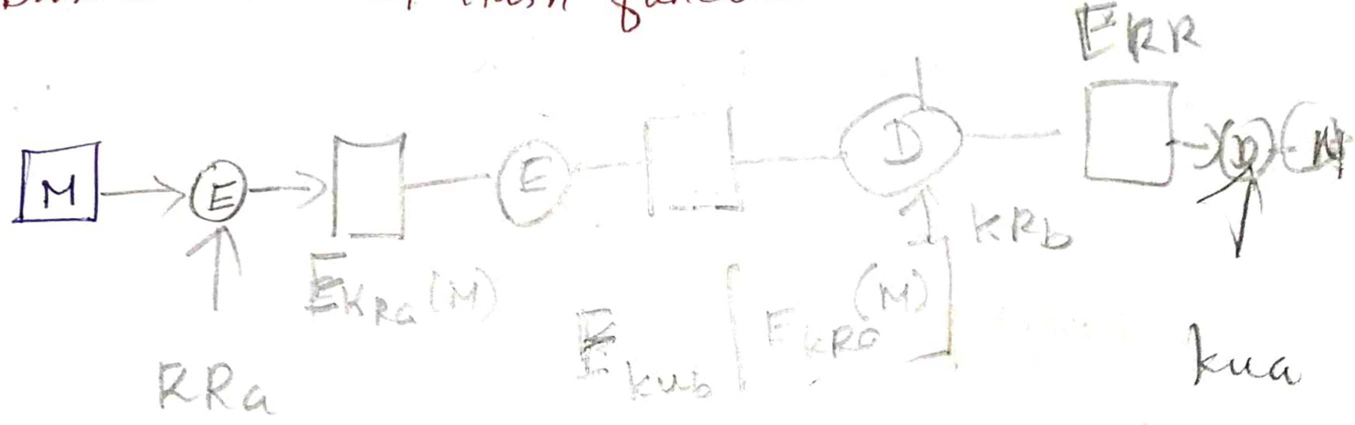
→Arbitrated

Direct Digital signature





Basic uses of Hash function



Public key encryption : confidentiality

Authentication & Signature

Arbitrated digital signature.

1) $X \rightarrow A : M \| E_{Kxa}[ID_X \| H(M)]$

2) $A \rightarrow Y : E_{kay}[ID_X \| M \| E_{kxa}[ID_X \| H(M)] \| T$

conventional encryption, Arbiter does not see message

1) $X \rightarrow n : ID_X \| E_{kxy}[M \| E_{kxa}[ID_X \| H(E_{xy}(M)]]$

2) $A \rightarrow Y : E_{kay}[ID_X \| E_{kay}[M] \| E_{kxa}[ID_X] \|$
$H(E_{kay}[M]) \| T]$

(C) public key encryption, Arbiter does not see message.

1) $X \rightarrow A : ID_X \| E_{KRx}[ID_X [ID_X \| E_{KUy}(E_{KRx}[M])]$

2) $A \rightarrow Y : E_{KRa}[ID_X \| E_{KUy}[E_{KRx}[M]] \| T]$

Advantages

first no information is shared ~~common~~ among the parties before communication, and preventing allowances of de fraud.

finally the content of the message from X & Y secret from A and anymore else

Authentication protocols:

1. Mutual authentication
2. one way authenticatuon

Mutual Authenticatuon

It is a very import area in authentication protocols. so it is enable communicate parties to satisfy them serves mutually about each other's identity and to exchange session keys.

two issues

1. confidentiality
2. Timeliness.

Example of replay attacks.

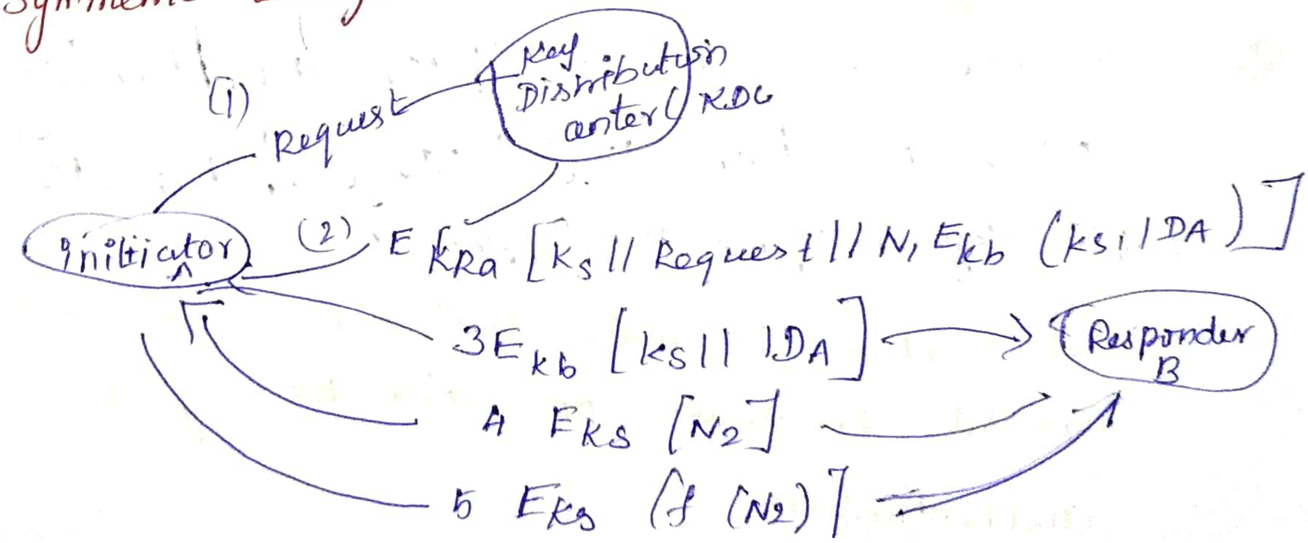
Simple replay

Repetition that can be logged.

Repetition that cannot be detected

Backward replay without modification

Symmetric encryption Approaches:



(i) $A \rightarrow KDC : ID_A \| ID_B \| N_1$

(ii) $KDC \rightarrow A : E_{ka} [k_s \| ID_B \| N_1 \| E_{kb} [k_s \| ID_A]]$

(iii) $A \rightarrow B : E_{kb} [k_s \| ID_A]$

(iv) $B \rightarrow A : E_{ks} [N_2]$

(v) $A \rightarrow B : E_{ks} [f(N_2)]$.

Suppose the A and B establish a session using the for mentioned protocoland then conclude this Session . following protocol as follows

(i) $A \rightarrow B : E_{kb} [ID_A \| k_s \| T_b] \; N_a$

(ii) $B \rightarrow A : N_b' \; E_{ks} [N_a']$

(iii) $A \rightarrow B : E_{ks} [N_b']$

One way Authentication.

Main application for which encryption is growing up in popularily is electronic mail (Email)

Symmetric encryption Approaches.

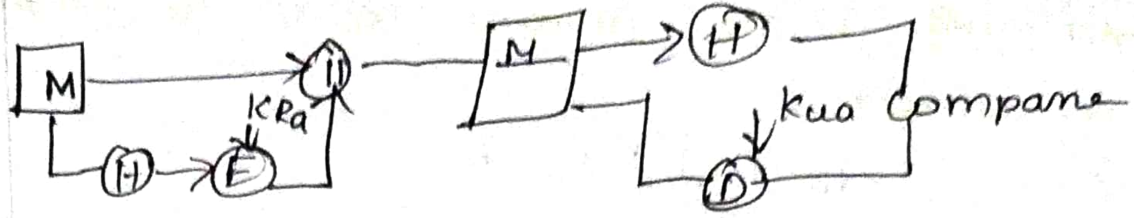
(i) $A \rightarrow KDC : ID_A \| ID_B \| N_1$

(ii) $KDC \rightarrow A : E_{ka} [k_s] \| ID_B \| N_1 \| E_{kb} [k_s] \| ID_A]$

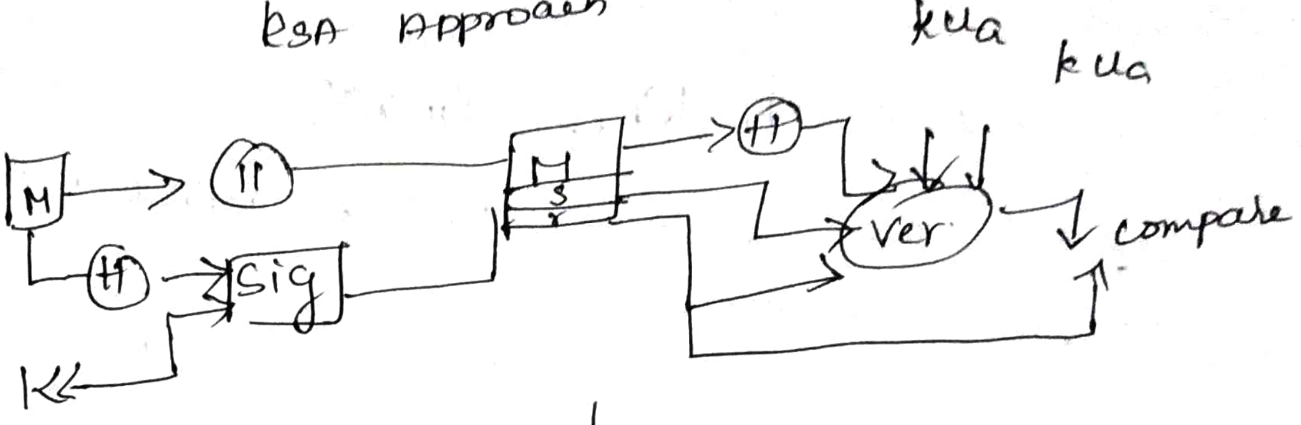
(iii) $A \rightarrow B : E_{kb} [k_s] \| ID_A] \| E_{ks} [M]$

Public key encryption approaches

It is Suited to email, including the straight forward encryption of entire message for confidentiality authentication.



RSA Approach



DSS Approach.

Digital signature Algorithm.

DSA is based on diffculty of computong discrete algorithms is based on schemes orginally Presented by El Gamal and schnorr.

input of DSA

✓ 160 bit prime number q.

✓ prime number p is Selected with a length between 512 and 1024 bits such that q divides (p-1)

✓ g is chosen be form of $h^{(p-1)/q}$ mod p. where h is integer between 1 and p-1) $g>1$

(Rules for DSA)

if confidentiality is the primary concern the following may be efficient

$A \rightarrow B : E_{Krb}[K_s] \| E_{Ks}[M]$

here message is encrypled with one time secret key.

$A \rightarrow B : M \| E_{KRa}[H(M)])$

this method guarantees that A cannot later deny having sent the message.

$A \rightarrow B : M \quad M \| E_{KRa}[H(M) \| E_{KRas}[T \| ID_A \| KV_a]$

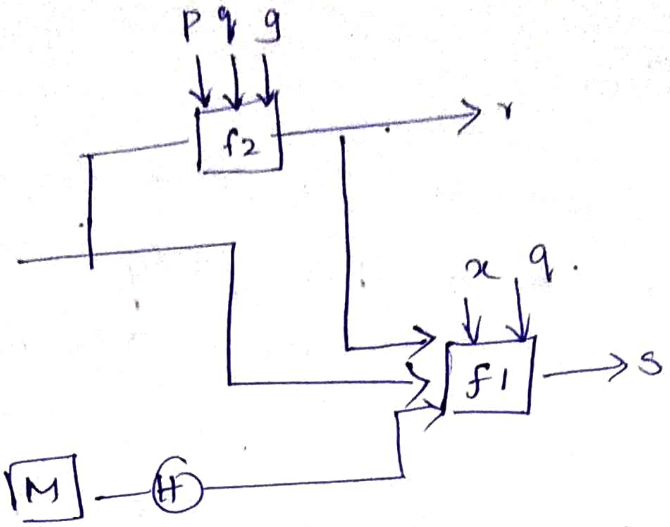
the receipent of the message first uses the certificate to obtain sender's public key to verify the message itself.

if it confidentiality required then the entire message can be encrypled with B's public key.

Digital Signature Standard

It makes the use of secure hash Algorithm (SHA) presents a new digital signature technique also based on RSA and an elliptic curve cryptgrapdy.

DSS Approach: DSS uses an algorithm is desighned to provide only the digital signature function

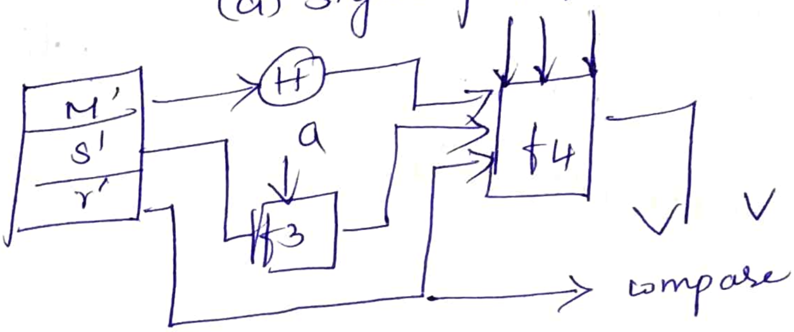


$s = f_1 \; (H(M), k, x, r, q)$

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

$r = f_2 \; (k, P, q, g) = (g^k \bmod P) \bmod q.$

(a) signing



$W = f_3 \; (s', q)$

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

$v = f_4 \; (y, q, g, H(M'), wr')$

$= ((g(H(M') \; w) \bmod q \; yr' \; w \bmod q \; \bmod P) \bmod q$

(b) Verifying

Entity Authentication

→ It is a technique designed do to that one party proves the identity of another party

→ An entity can be Person, a process, a client or Server

→ The entity whose identity needs to be proved is called as a claimant . the party who tries to prove the identity of the claimant is called a verifier.

Data origin

they are two different between message authentication and entity authentication

(i) Message authentication.

It is happened not in a real time. otherwise it is called as Data orgin signature.

~~Atob too~~ Verification categories

In a entity authentication the claimant must identify to the identifier

1. Some thing known.
2. Some thing possessed
3. Some thing inherilent.

Biometrics

1)It is a measurement of physiological or behavioral features that identifies a person

2) It cannot be guessed, or shared.

Components

various components to be needed for biometrics include capture devices, processors and storage devices.

Capturing devices such as readers measures biometrics features.

Processor changes the measured features of the type of data appropriate for saving purpose

storage device save the result of processing for authentication

Authentication

It is done by verification

Verification

Verification ~~person~~ feature is matched against a single record in the database to find if s/he is who claiming to be.

Ex a check the customer Signature on a check in bank process.

Identification

identification a person feature is matched against all records in the database to find if she has a record database.

Eg The company needs to allow access the building only to employees.

Technique.

2 broad ways

1. physiological → it measures physical traits of human body for verification and identification

Finger print, : 8

they are several methods.

1. minutiae based
2. Image based,

Iris.

It measures the pattern within iris that is unique for each person.

Retina

It is used the purpose of examine blood vessels in back of eyeside.

face

This method analyzes geometry of face based on distance between facial features such as nose. mouth & eyes.

~~Face~~ hands.

It measures dimension of hands, that includes the shape and length of fingers.

Voice

voice measures pitch, cadence and tone in the voice.

DNA

DNA is chemical found in the nucleus of all cells of humans and most other organism.

Behavioural technique

It measures some human behaviours traits

1. Signature
2. key stroke
3. Accuracy.
4. face acceptance Rate

Applications

commerical Purpose

1. Access to facilities.
2. Access to information systems
3. Transaction at point of scales.

Low enforcement such as

1. investigation (finger point or DNA
2. forensic Analysis.

Passwords:

oldest method of entity authentication is Password

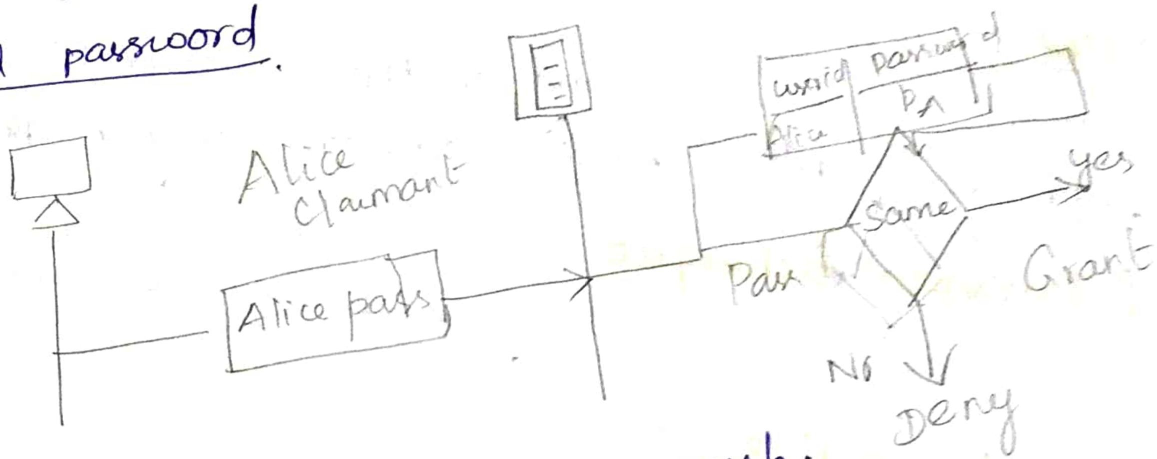
It is used when a user needs to access system to use system resources.

divided two types

1. fixed password

2. one time password.

fixed password



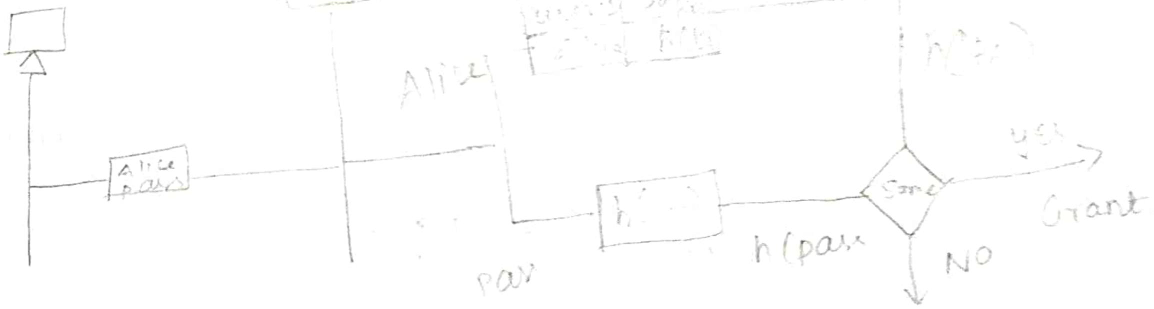
1. It is very rudimentary approach,

2. to access the system resources.

3. The S/m userID is to the find the password in the table if the password sent by user which matches with the password in the table.

Second Approach.

Hashing password.



~~Bpp~~: Disadvantages

1. salting makes it dictionary attack more difficult.

2. this means eve now needs to make a list of 10 million entries and comparsion take much longer

3. salting is very affective if the salt is very long random number.

Challenge Response protocol.

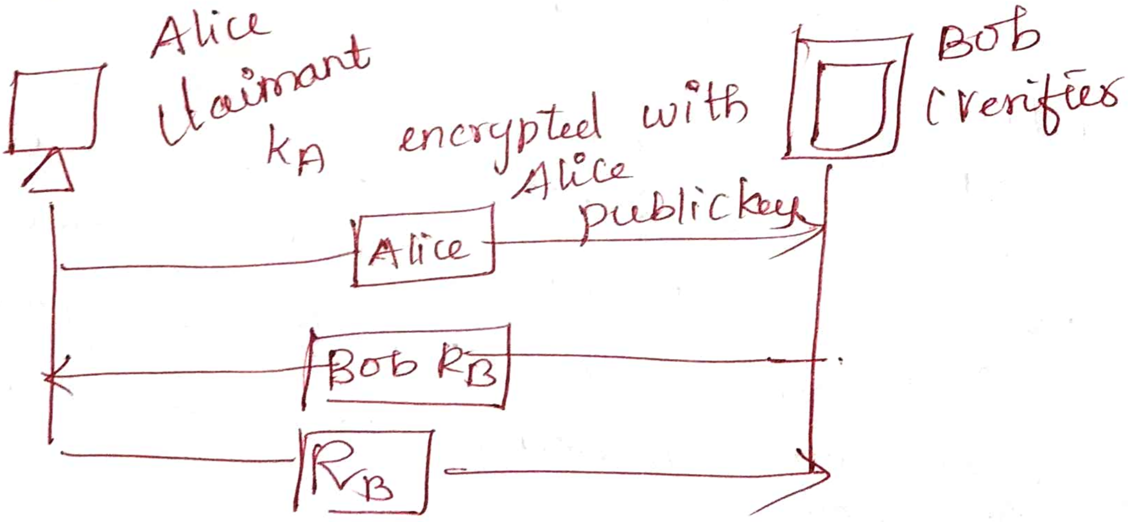
password authentication the claimant proves her identify by demonstrating she knowns a secret the password.

In challenge response authentication the claimant proves she knowns a secret without sending it

using a symmetric key cipher.

Several approaches to challenge response authentication use symmetric key encryption

the secret there is share key known by both claimant and verifier.



10. Authentication ~~protocols~~ Applications

system security in cryptography provides cryptographic include source encoding and decoding of data that aso support as hacking random number generation and message authenticaton

1. Kerberos.

Kerberos is an authentication dialogue services developed as a part of project Athena at MIT

1. A user may gain access to particular workstation and pretend to be another user operating from that workstation

2. A user may alter the network address

Types of Versions:

Version 4 is used in widely function

Version 5 - It is corrects the some of the deficiencies of version 4.
Security

Kerberos function:-

1. provides a centralized authentication Server whose function is to authenticate users to servers and servers to users.

2. It relies exclusively on symmetric encryption making no use of public key encryption.

Motivation

If a set of users is provided with dedicated systems that have no network connection then the user's resources and files can be protected by physically securing each personal computer

it enforces following activities

1. policies based on user identity

2. use logon procedure to identify users.

Third approach used as open network.

1. Secure

2. Reliable

3 Transparent

4. Scable.

Keberos version 4 :

Version 4 of Kerberos makes use of DES to provides authentication service.

A simple authentication dialogue.

An alternate is to use an authentication server that known the passwords of all users and stores these in centralized database.

Assume the hypothetical dialogue.

1) $C \rightarrow AS$: $ID_C \| P_C \| ID_V$

2) $AS \rightarrow C$ Ticket

3. $C \rightarrow V$ $ID_C \| Ticket$

Ticket = EKv | IDc || ADc | IDv

Disadvantages

1. Passcoord is plaintext, any opponent can capture the ticker in message of second approach and impersonate the client.

2. The overcome above drawbaek, a more secure authentication dialogue is required

X. 509 authentication service

x. 509 is a part ~~of~~ x. 500 series of recommendations define a derectory ~~service~~,

the directory is serve as a respository of public key certificates.

If consist of following certificate format.

(i) S|MIME

(ii) IP securuby

(iii) SSL |TLS

(iv) SET

Certificates

Heart of the x 509 scheme is a public key certificate associated with eachother this user certificates are assumed to be Created by some certificate authority. place in the directory by the CA or by the user

1) Version - 1) Default version 1

2) issuer unique ID.

3) If one or more extension

2) Serial no

3. signature algorithm ID.

4. Issuer name

5. subject public key information

7. subject unique ID

8. extensions

9. signature

10. subject name.

CA << A >> = CA {V, SN, AI, CA, TA, A, Ap}

Y << X >> = certificates of user X issued by certification authority Y

Y{F} = signing of I by Y

In the notation of x 509 Chain is expressed as

X1 <<X2 ~~>>~~ X2 <<B>>

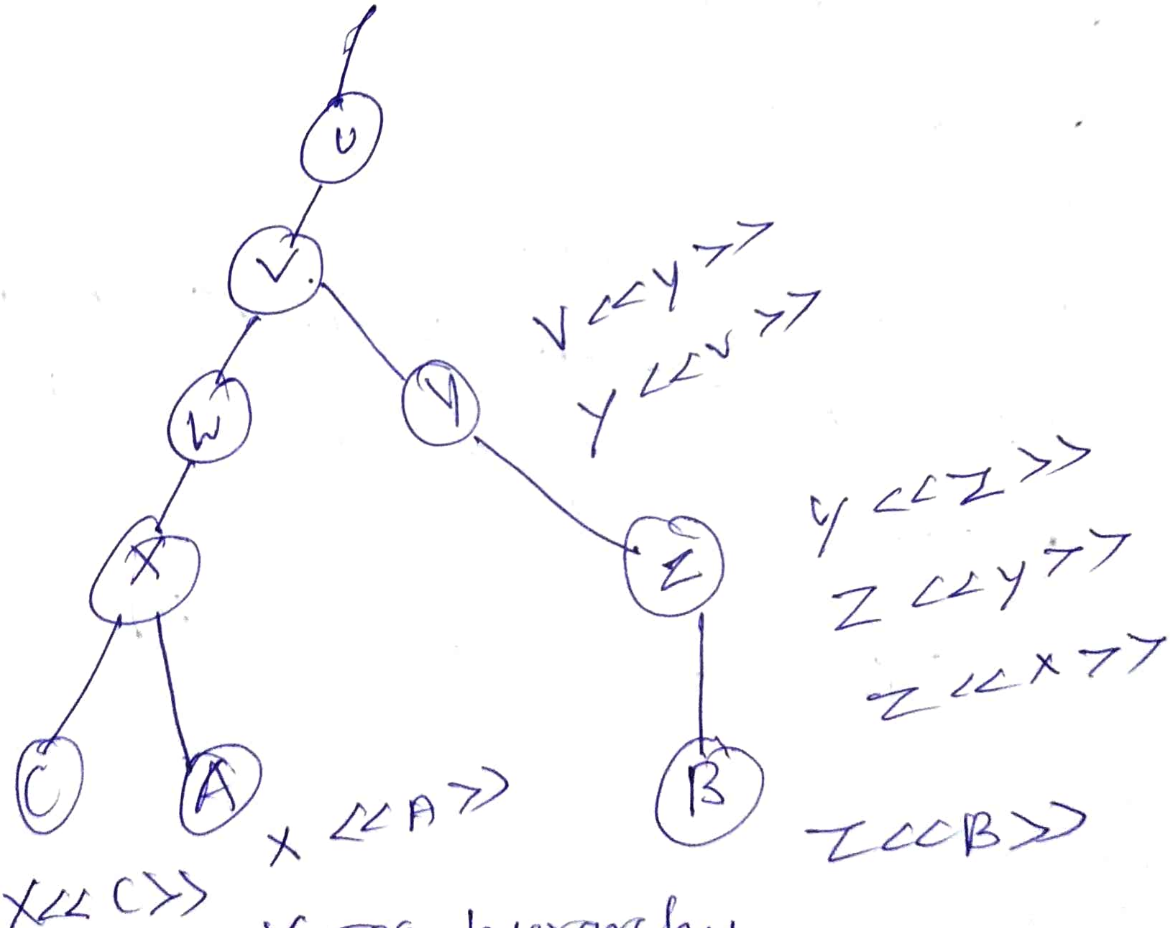
In same function, B can obtain A's public key with reverse chain.

the chain of two certificates

X1 <<X2 >> X2 << X3 >> .. XN<<B>>

they are two type.

1. forward certificates
2. Reverse certificate



X.509. hierarchy.

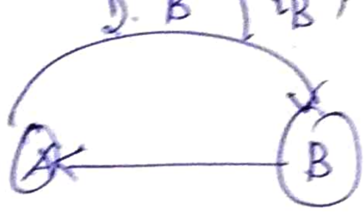
Authentication procedures.

$A = \{ t_A, r_A\ ID_B, \text{sgrData}, E_{kub}(ab\}$

Oneway ~~comm~~ authentication

1. $A \{ t_A . r_A , ID_B , \text{SgrData}, E_{kub}[kab] \}$

2. $B \{ t_B , r_B , ID_A , r_A , \text{sign Data}\ E_{kva}[k_b])$



two way Authentication

Oneway

The identity of A and message was generated by A

That the message was intended for B.

Two way

1) The identity of B and that reply message was generated by B.

2) that the message was intended for A

3 The integrity and originality of the reply.

Three way authentication

a final message. From A and B is included which contains the signed copy of nonce r_B. the intent of the design is timestamps need not be checked.

unit 5

Security practices and system security

E-mail Security

email. security provides more search , while use e-mail

the simplest form of electronic mail message is based on the sender and receiver.

(i) Example : Alice sender a message to Bob!

To : Bob

From : Alice

care to meet me in any apartment to right

(ii) Multiple senders such as

To : Bob, carol, Ted

From : Alice.

case to meet me in any apartment to night

there are two ways to implement a disribution lists

1. Remote exploder

2. Local Exploder

The simplest form of electronic mail consists of sending message diretly from source machine to destination machine

(i) Message Transfer agents

(ii) user agent

1) Pretty Good privacy :-

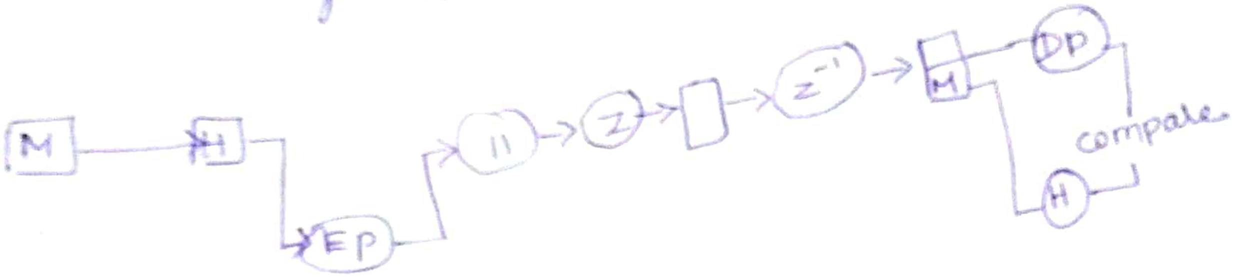
PGP is a outstanding occurance

PGP provides

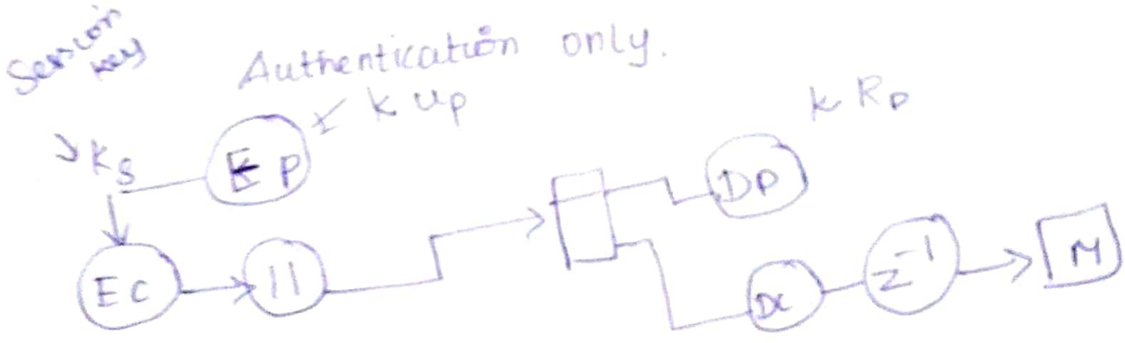
1. confidentiality
2. authentication service
3. compression
4. e-mail compatibility

It used for

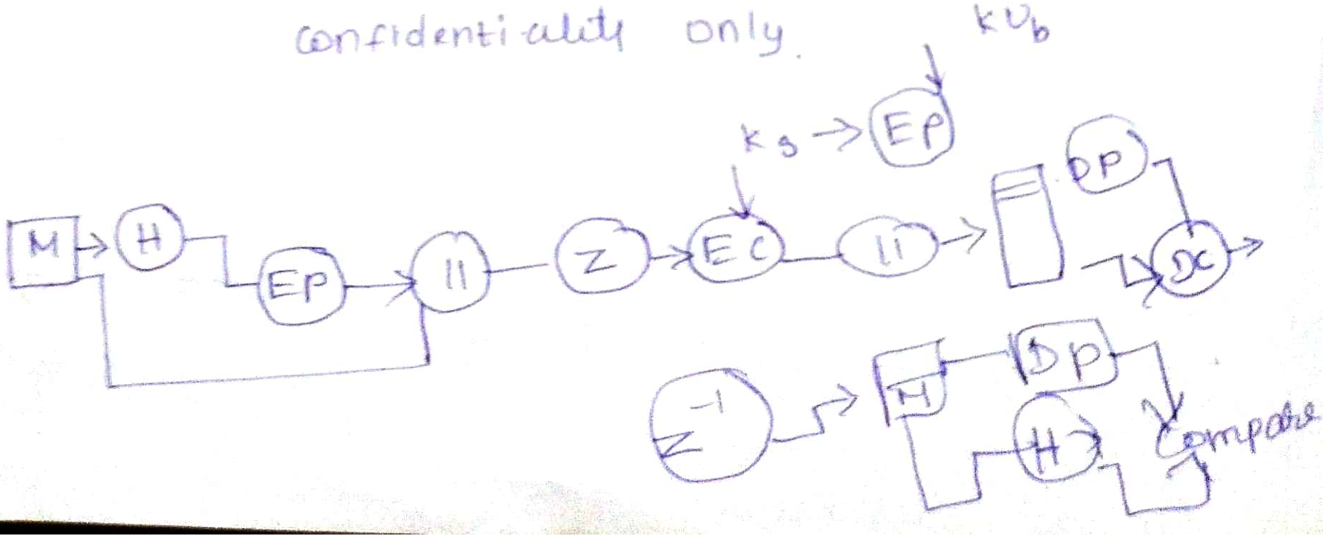
file storage applications.



Authentication only.



confidentiality only.



Authentication :

1. The sender creates a message.

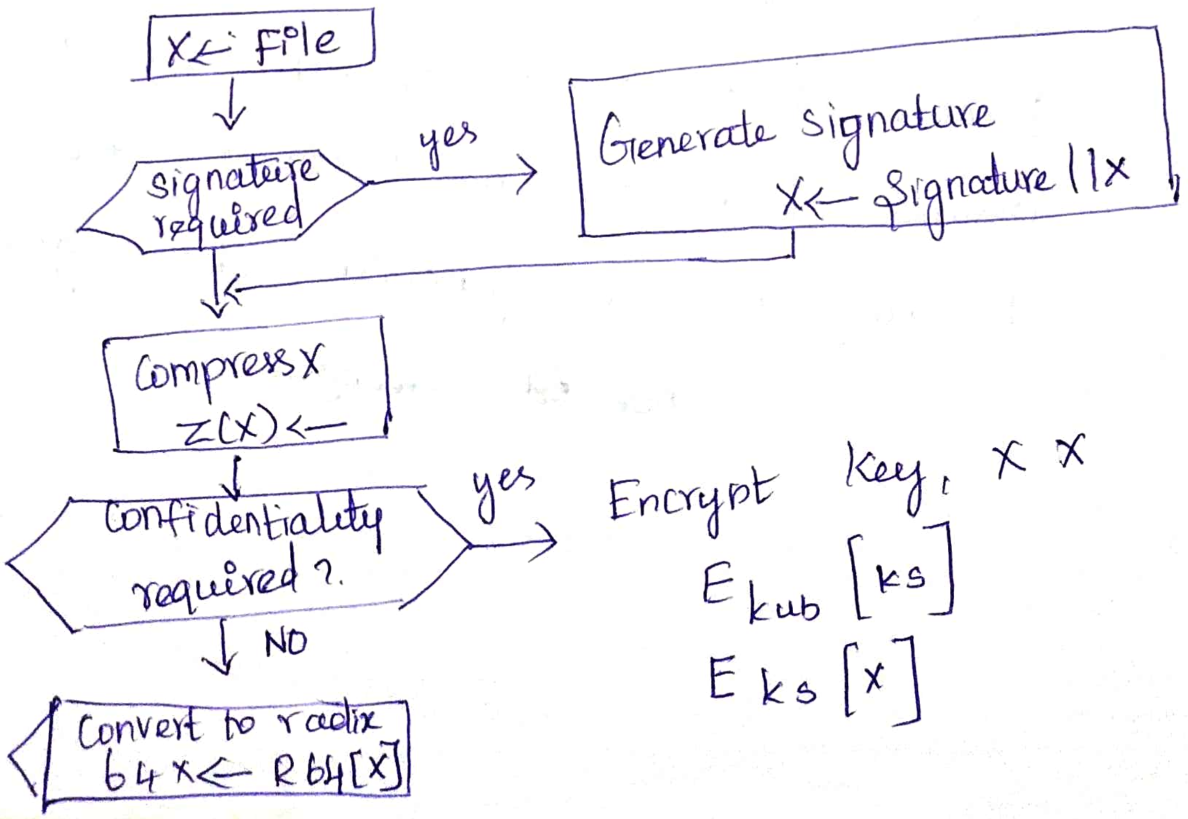
2. SHA-1 is used to generate a 160 bit hash code of the message.

3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message

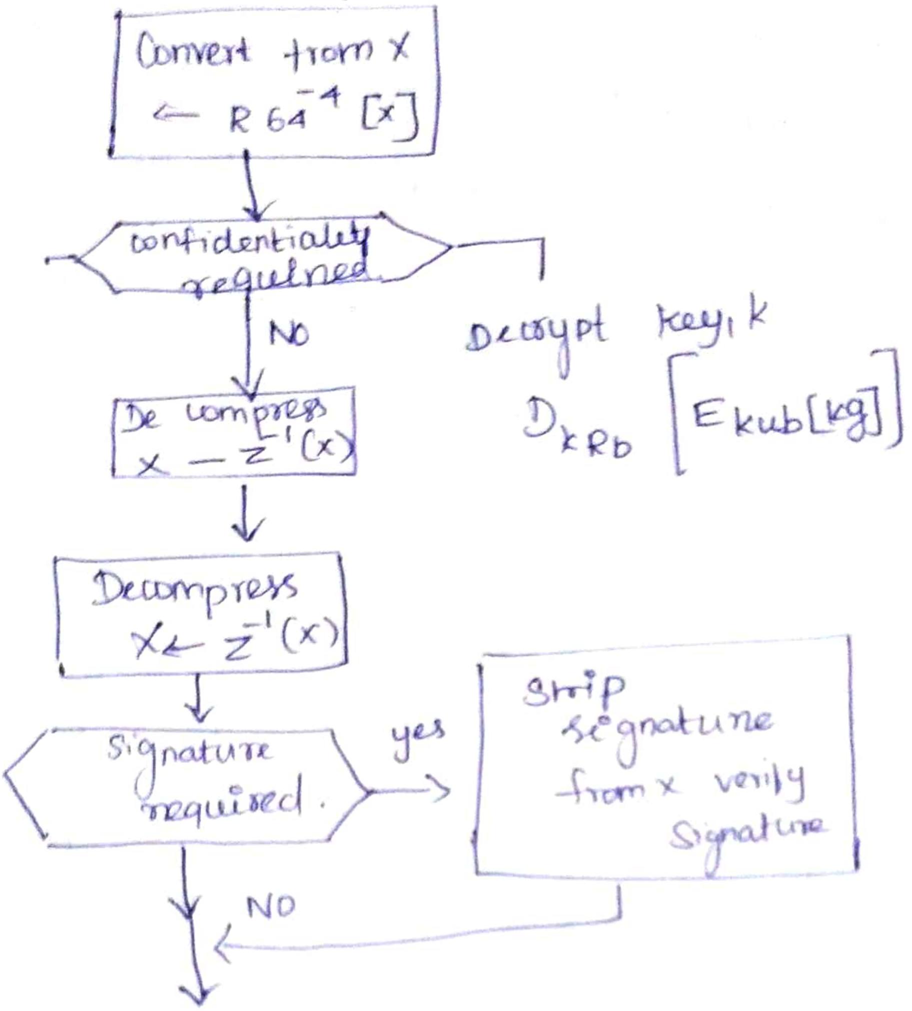
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.

5. The receiver generates a new hash code for the corresponding message and compares it with the decrypted hash code. if the two match, the message is accepted as authentic. (fig 1).

Generic transmission diagram



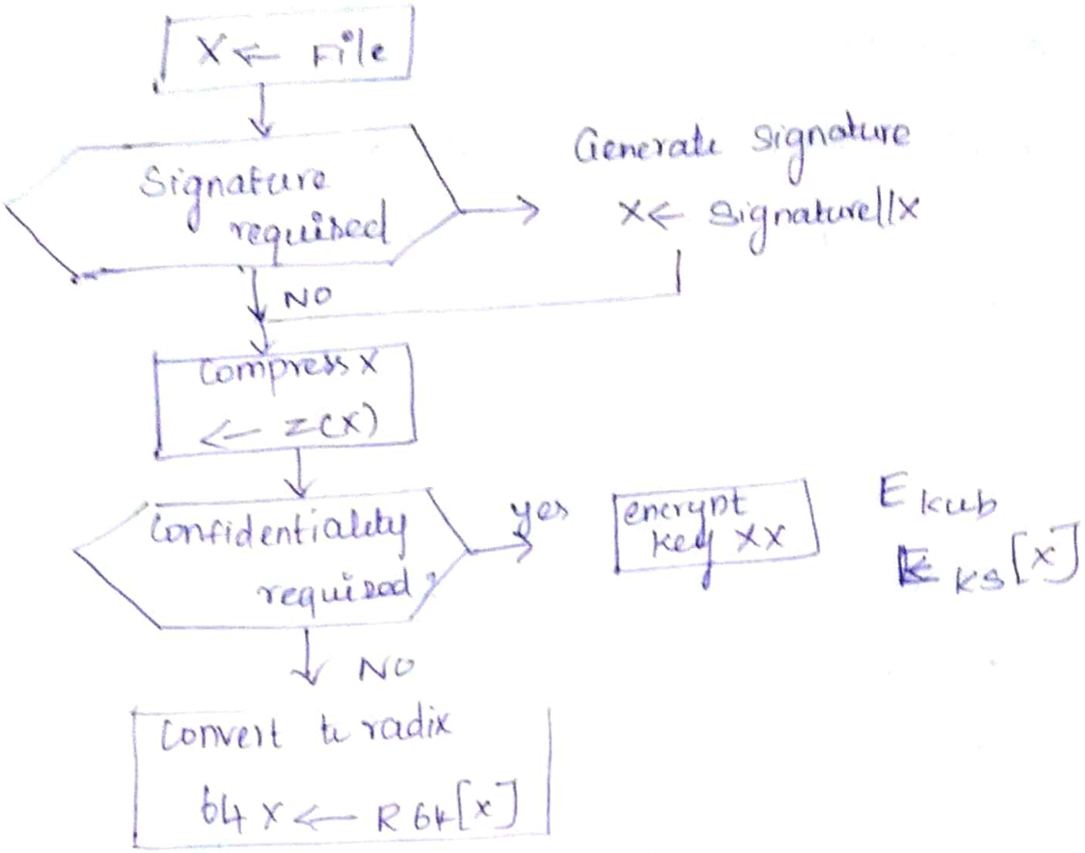
Generic reception diagram



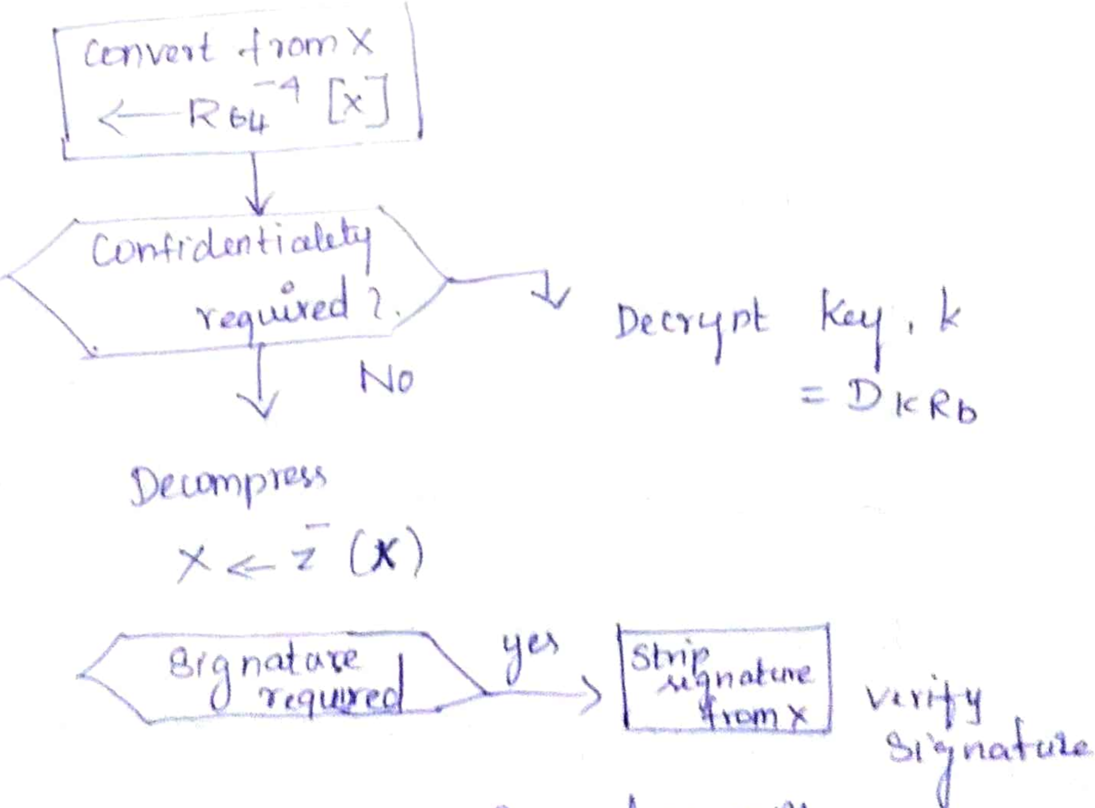
The combination of SHA-1 and RSA provides an effective digital scheme.

Because of the strength of RSA, the recepient is assured that only one possessor of the maching private key can generate the signature.

Due to strength



Generic transmission diagram



(b) Generic reception diagram

Confidentiality

fig (2 X'i) The Sender generates a message and a random 128 bit number to be used as a session key for this message only

The message is encrypted using CAST-128 with the session key.

The session key is encrypled with RSA using Recipients public key and is prepended to the message.

The receiver uses RSA with is private key to decrypt and recover the session key.

The session key is used to decrypt the message.

Compression :-

1. The Signature is generated before compression for two reasons.

a) It is preferable to sign an uncompressed message So that one can store only the uncompressed message. together with the signature for future verification.

b) even if one of the user willing to generate dynamically a recompressed message for verification, Pgp's compression algorithm present a difficalty achieve different tradeoffs in running speed versus compression ratio and as a result products

The five header fields ~~fields~~ defined in MIME are follows.

MIME version → parameter value 1.0

Content type : Describes data contained in the body with suffcient detail.

Content description : A text description of the object with the body. this is useful, when the object is not readable (ex: Audio data)

MIME content type.

Type	Subtype	Description
Text	plain	unformatted text
1	enriched	provides greater format flexibilty
Mutipart	parallel	Differs from mixed only in that no order is defined for delivering the part of receiver.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822
image	Jpeg gif	the image is in JPEG format the image is GIF format
Video	mpeg	MPEG format
Audio	Basic	single channel 8 bit ISDN

MIME Transfer encoding

7bit → short lines of ASCII characters.

8 bit → lines are short

→ binary
→ quoted printable
→ base 64
→ x token

Canonical form

canonical form is a format, appropriate to the content type that is standardized for use between system

SIME Functionality

Functions

1. enveloped data → encrypted content of any type
2. signed data → digital signature is formed by taking the message digest of the content to be signed and then encrypted that with the privat key of the signer.
3. clear signed data → digital signat~~ature~~ure is formed only digital signature encoded using base 64.

Cryptographic Algorithms.

1. hash functions SHA-1, MD5
2. digital signatures. DSS & RSA
3. Session key encryption
4. message encryption.

tradeoff in running speed versus compression Ratio.

→ AS a result produce different compressed form

→ different compression Algorithms are interoperable because ary versus ~~compression~~ ~~rat~~ algorithm can correctly decompress the output of any other version.

→ Applying the hash function and signature after compression would constrain all pgp implementations to the same version of the compression Algorithm

→ Message encryption is applied after compression to strengthen cryptographic security.

→ Because the compressed message has less redundancy than the original plaintext,

→ cryptoanalyses is more difficult. the uses of compression algorithm used is zip.

EMail compatibility

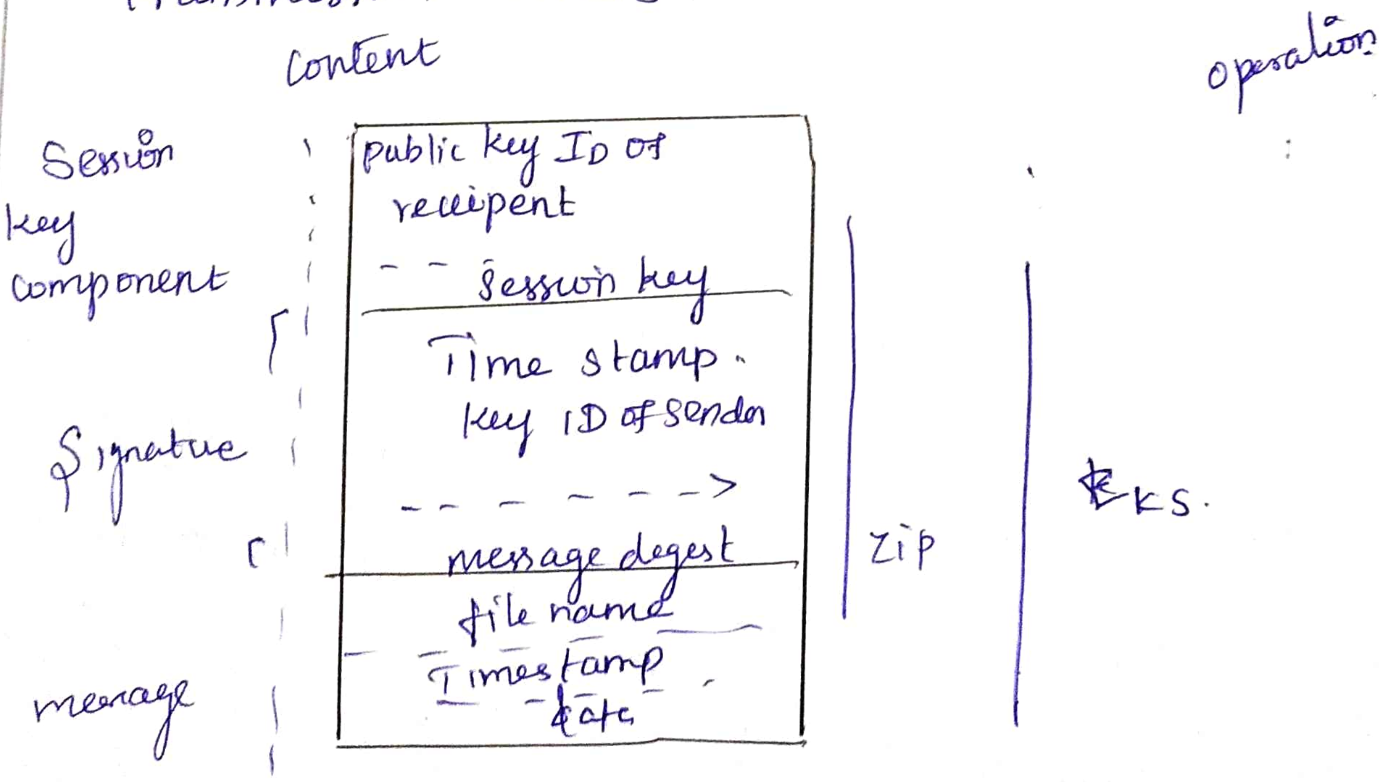
1) When PGP at least part of the block to be transmitted is encrypted

2) if only signature service is used, then the message digest is encrypted (private key)

① if the confiendiality service is used, the message plus signature (if present) are encrypted (with one time syammetric key)

-> the scheme used for this purpose is radix 64- conversion, each group of three octets of binary data is mapped into four ASCII characters,

-> This format also appends a CRC to detect transmission errors.



S/MIME in CRyptoGraphy

* secure /multipurpose Internet mail extensions

* It provides Security for commercial e-mails

* extension of mime protocol.

* It is a widely accepted method (or more precisely a protocol for sending.

digitially signed and encrypted message

(ie)
It allows as to degitally sign our email to verify ourselves as the legimate sender (and also encryption. & descryption of mails.

S/MIME is based on asymmetric key encryption

Function
It. provides two security services

1 Digital signature (It provides authentication reputation

2. Msg encryption
It provides confidentiality + data integrity

It is a supplementry protocol that allows non ascii data to be sent through email

It cannot send not videos.

1. SMTP cannot transmit excutable files on binary objects

2. SMTP cannot transmit data includes national Language characters because these are ~~compressed~~ represented by 8 bit codes with codes with values of 128 decimal or higher

3. SMTP servers may reject mailmessage over a certain size

4. SMTP servers ~~may~~ ~~ray~~ gateways that translate between ASCII and the character code EBCDIC consistent set of mappings, resulting in traslation problems.

5. SMTP gateway that translate between ASCII and the character code EBCDIC consistent set of mapping resulting in translation process.

6. SMTP gateway to X.400 electronic mail networks cannot handle non textual data included in X 400 message.

Overview :-

.MIME specification includes following elements

1. Five new message header
2. A no of content format
3. Transfer encodings.

Ip Security :

IP security Architecture ·

Internet protocol. → 'protocols b/w two communication points across the IP network that provide

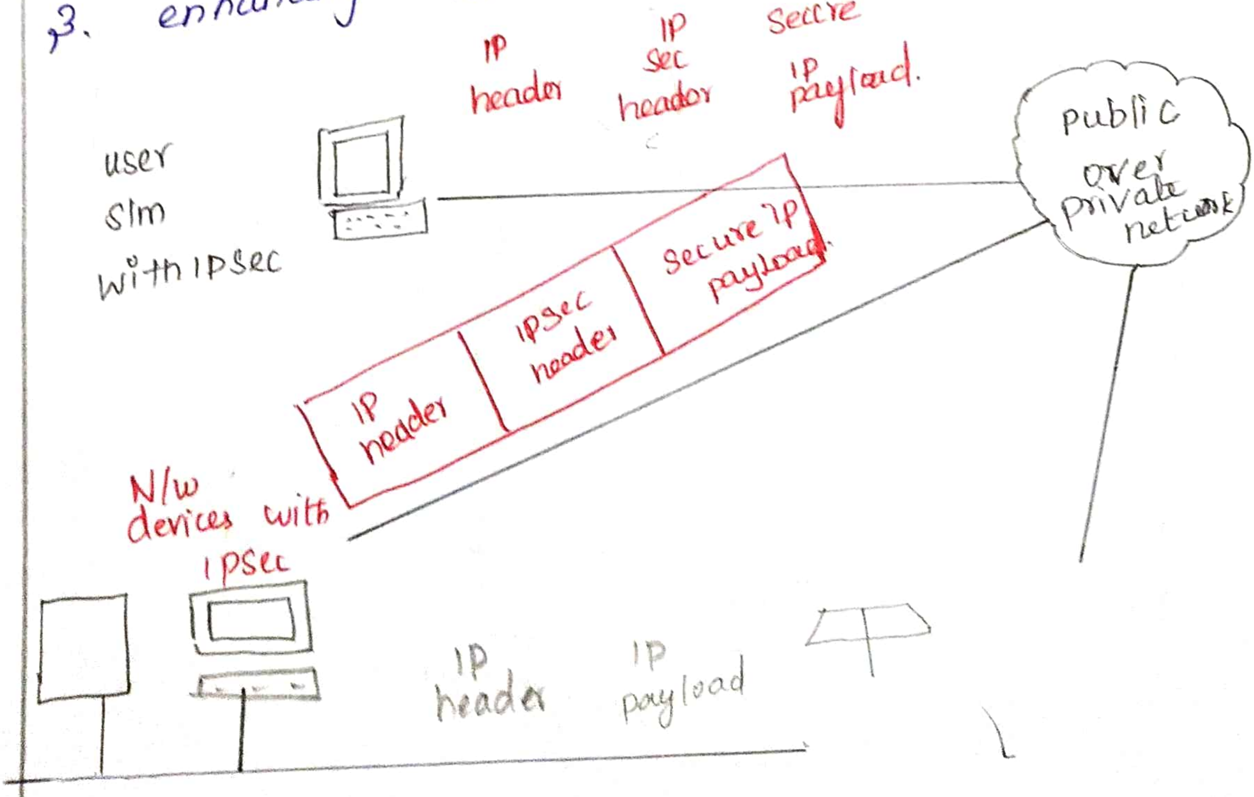
1. data authentication
2. integrity
3. confidentiality.

→ IP security known as "IPsec"

→ IP v6 is Successor of IP V4 has authentication and encryption.

Applications of IPsec:

1. Secure branch office connectivity over the internet or over public WAN
2. Secure remote access over the internet.
3. enhancing electronic commerce security.



benefits of IPsec

IP sec implemented in a firewall or router. it provides strong security can be applied to all traffic.

IP sec can be transparent to end users.

IP sec provide security for individual users it needed.

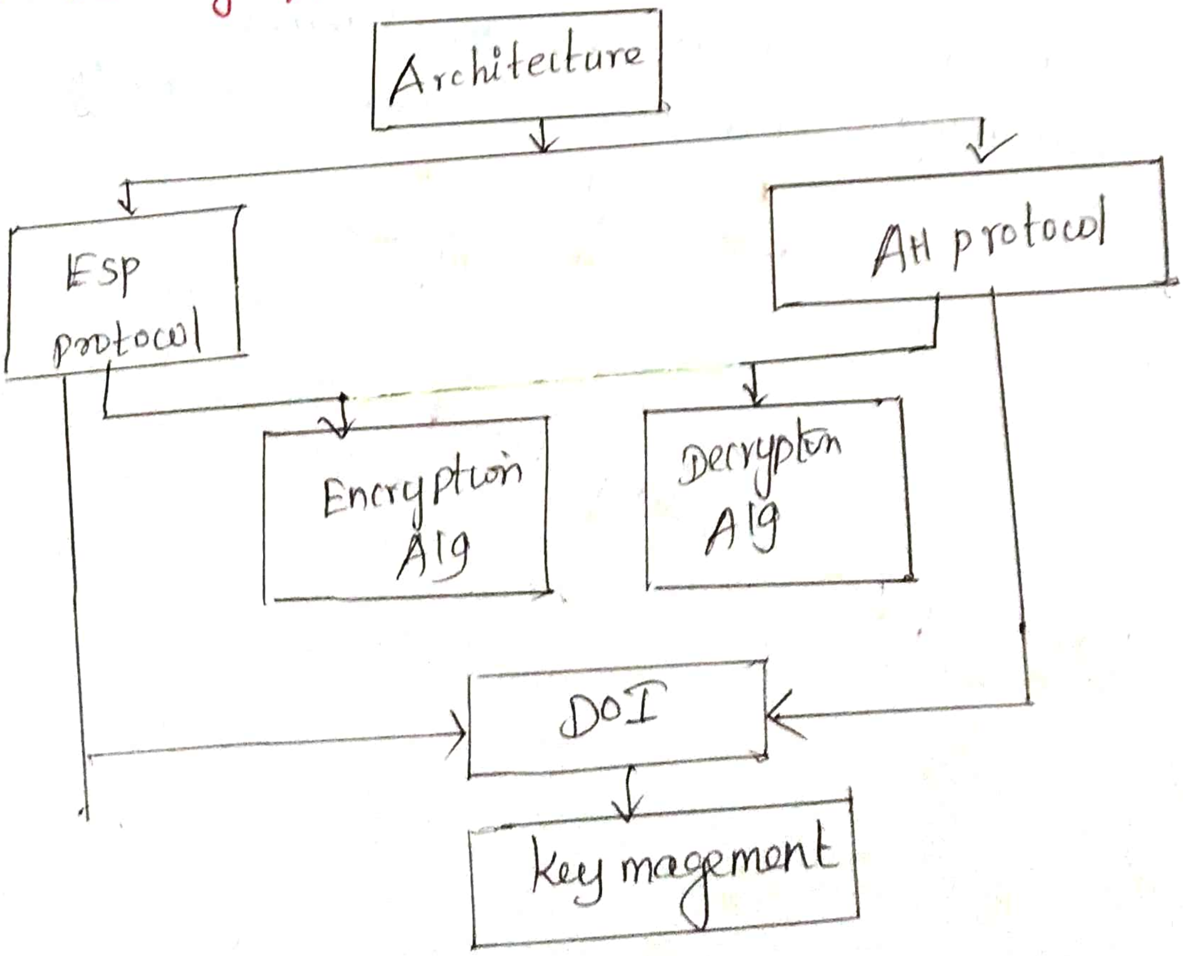
Routing Applications:

i) A router advertisement comes from an authorized router.

b) A redirect message comes from the ~~router~~ to which the initial packet was sent

c. A routing update is not forged.

IP Security Architecture.



The IP documents is divided into seven groups.

1. Architecture
2. Encapsulating security payload.
3. Authentication header
4. Encryption Alg
5. decryption Alg
6. key management.

The services such as.

1. Access control
2. connection less integrity
3. Dat orgin authentication
4. Rejection of replayed packets
5. confidentiality
6. Limited traffic flow confidentiality.

Security Associations.

1. A key concept in both. authentication and confidentiality
2. It is oneway relationship between a sender and a receiver that affords security services to the traffic.
3. If a peer to peer relationship is needed for two way secure exchange.

Three unique parameters

1. Security parameter Index.
2. IP destination Address.
3. security protocol identifier.

The IP documents is divided into seven groups

1. Architecture
2. encapsulating security payload
3. Authentication header
4. Encryption Alg
5. decryption Alg
6. key management.

The services such as.

1. Access control
2. connection less integrity
3. Dat orgin authentication
4. Rejection of replayed packets
5. confidentiality
6. Limited traffic flow confidentiality.

Security Associations

1. A key concept in both. authentication and confidentiality
2. It is oneway relationship between a sender and a receiver that affords security services to the traffic.
3. If a peer to peer relationship is needed for two way secure exchange.

Three unique parameters

1. Security parameter Index.
2. IP destination Address!
3. security protocol identifier.

SA parameters

1. Sequence no ~~[illegible]~~ counter
2. Sequence counter overflow
3. Anti replay window.
4. AH Information
5. IPsec protocol mode.

SA Selectors :

-> IP sec provides user with considerable flexibity security policy database.

-> IP traffic is related to specific SA is an nominal security database.

Transport and tunnel mode.

AH and Esp both used the two types of modes.

Transport mode.

This mode provides the protection of packet payload for upper layer protocols.

example.

include a Tcp or UDP Segment or an Icmp packet

Tunnel mode :-

-> It provide protection to entire packet IP packet

-> The Esp is a tunnel mode encrypts and authenticated packet not a outer header.

-> tunnel mode authenticate entire packet and selected outer bits.

AH	Authenticate ip payLoad & selected portions of IP header and ip v6 extension on header	Authenticate entire inner ip packet plus Selected portions of outer ip heads and outer IPV6 header
ESP	encrypts ip payLoad and IPv6 extension headers following ESP header.	encrypt inner ip packet
Esp with Authentication	encrypt ip payLoad and any ip v6 extension deader following ESP header Authenticate ip payload but not ip deader	encrypt inner ip packet Authenticate inner ip packet

orig IP header	Tcp	data

orig IP header	extension headers of present	Tcp	data

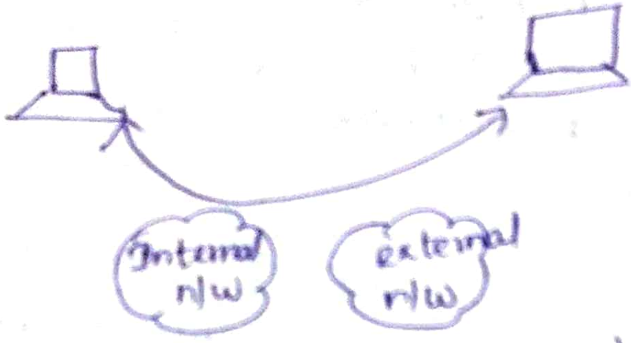
Transport mode.

orig IP header	AH	Tcp	data.

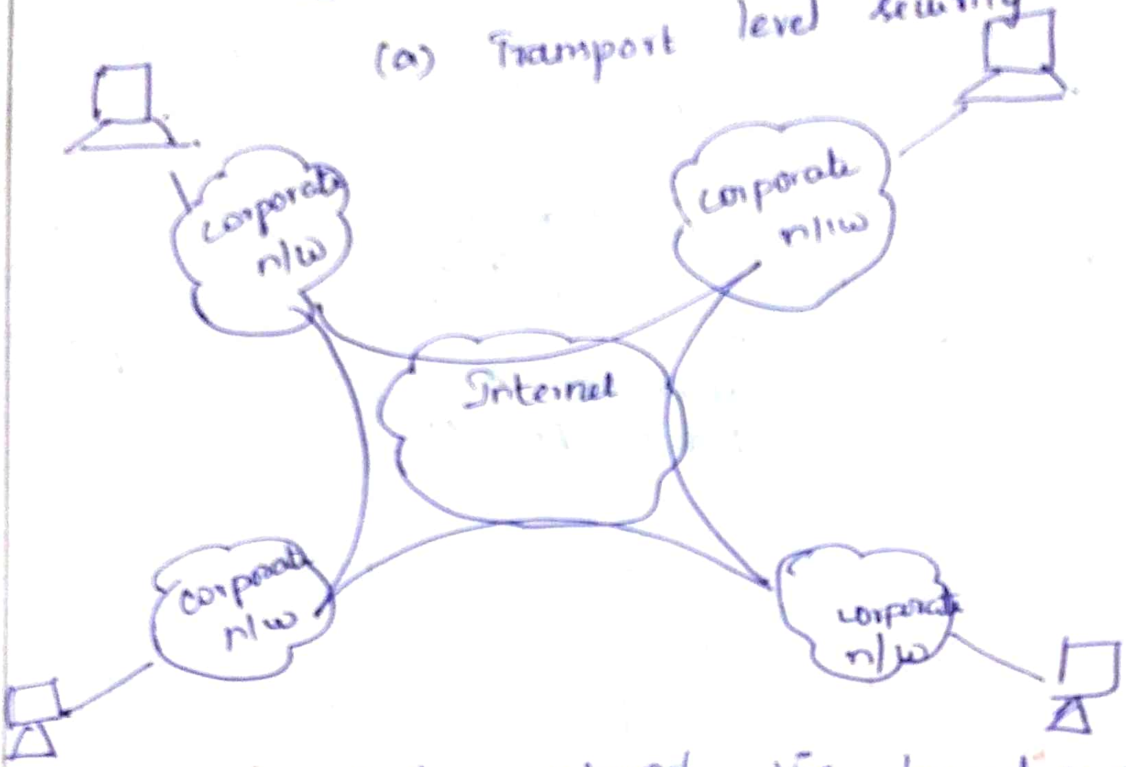
← Authenticated except for mutual fields.

Esp

Transport and tunnel modes.



(a) Transport level security



A virtual private network via tunnel mode 4

Authentication plus confidentiality

encryption and authentication can be combined in order to transmit an ip packet that has both confidentiality and betw hosts

1. Transport mode Esp
2. Tunnel mode Esp.

Advantage:

This approach over simply using a single ESP SA with ESP authentication option, is that covers more fields include source and destination ip address

Dis advantage

The overhead of two SAS verges on SA.

Key management:

The key management of ipsec involves. determination and. distribution of Select keys.

1. oakley key determination protocol.

2. Internet key determination protocol.

oakley key Determination protocol

D-H Algorithm involves interaction between users A and B.

A selects a random integer XA as a private key and transmits to B public key

$Y_A = a^{X_A} \mod q.$

B.

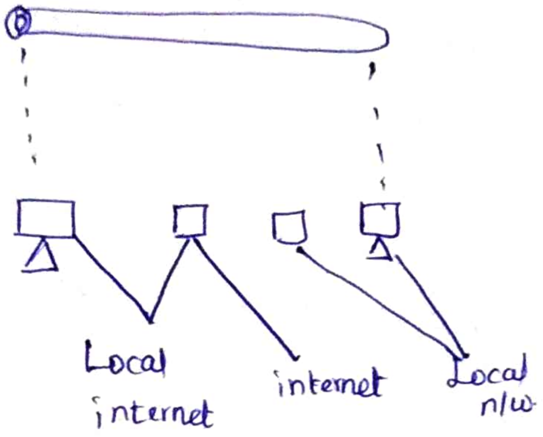
$Y_B = a^{X_B} \mod q.$

Both side have some same secret key

$k = (Y_B)^{X_A} \mod q = (Y_A)^{X_B} \mod q$

$= a^{X_A X_B} \mod q$

ones o more SAS.



(a) case 1

key management.

The key management portion of IPsec involves the determination & distribution of secret keys.

Types.

Manual : A system administrator mutually configures each system with its own keys & with the keys. of ther communicating systems.

Automated

the default automated key management protocol for ipsec is referred to ISAKmp/ oakley and consists of the following elements

protocol:

is a key exchange protocol based on the Diffie hellman algorithm but providing added security.

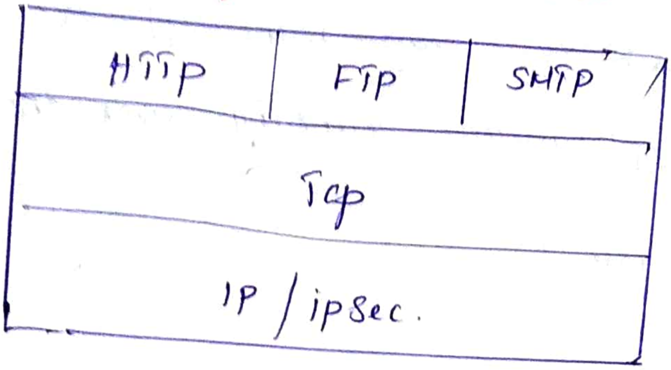
WEb Security.

The world wide web is fundamentally a client / server applications running over the Internet and Tcp / IP intranets.

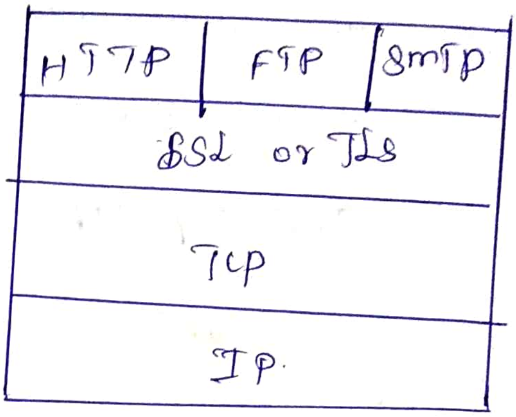
Compassion

Integrity	Threats	consequences	Counter measures
integrity	1. modification of userdata 2. Trojan horse browser 3. modification of memory.	Loss information	Cryptographic checksums
confidentiality	1. Eaves dropping on the net 2. Theft of info from server	Loss information Loss of privacy	encryption web proxies
authentication	1. Implementation of 1. legitimate users 2. Data forgery	misrepresentation of user belief that false information is valid	Cryptographic techniques

Web Security traffic Approaches

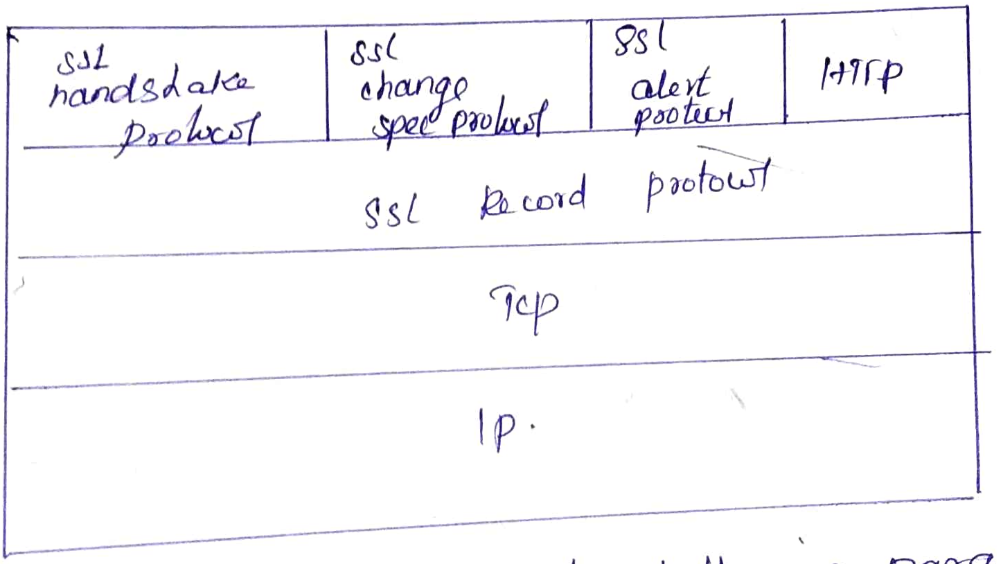


N/w Level



(b) maniport level.

SSL protocol stack



A session state is defined following parameters

1. session identifier
2. peer certificate
3. compression meldod
4. cipher spec.
5. Master secret

Communication State

1. Server and client random
2. Server write MAC Secret
3. Client write MAC Secret
4. Server write key
5. Client write key
6. Initialization vector
7. Sequence number.

SSL record protocol.

1. confidentiality
2. message Integrity

Payment capture !

1. capture request
2. capture respons.

the merchant generates signs and encrypts a capture request block includes payment amount and transaction ID

System Security

Intruder

It is the most publicly threats to security is intruder generally referred to an hacker or cracker.

three classes of intruder.

masquerader :

An individual who is not authorized to use the computer and who penerates system access controls to exploit the legitimate user's account.

misfeasor :

A legitimate user whor accesses data programs or resources. for whic such access is not authorized or who is authorized for each success but misuses his or her privileges

clandestine user.

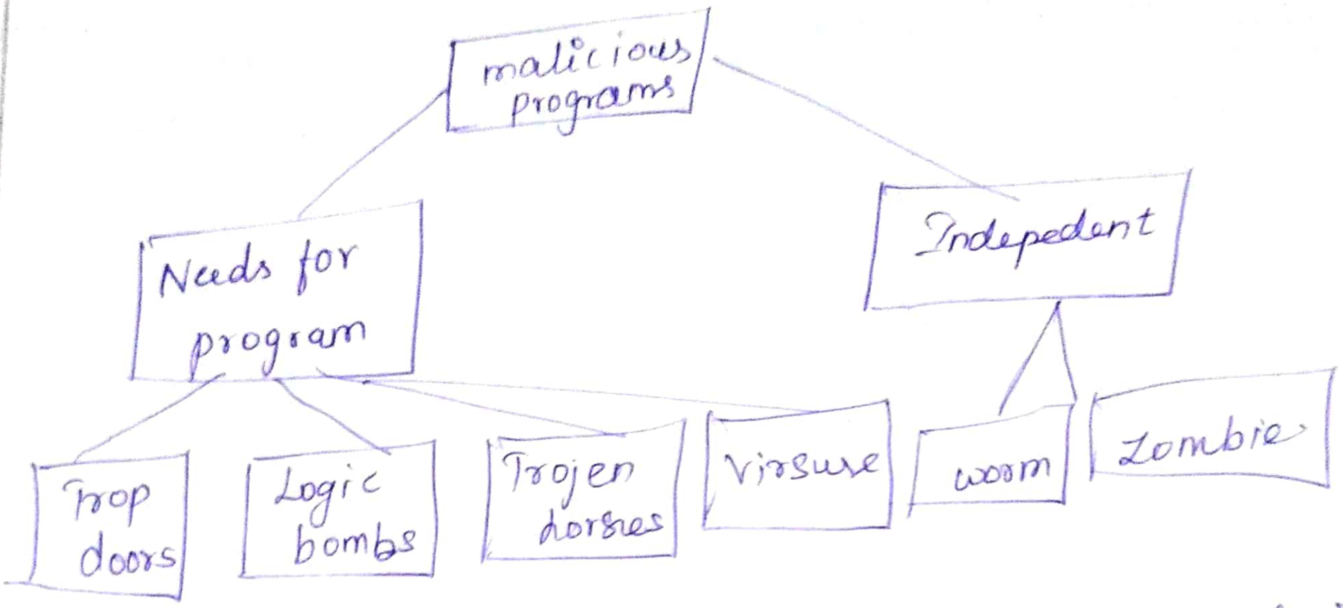
An individual who sizes supervisory control of the system and the use this control or suppress credit collection.

Malicious software

overall taxonomy of software threats or malicious programs.

these threats divided in to two categories.

1. Needs host program
2. Indepedent.



Trap Doors.

It is a secret entry point into a program allows some one aware of the trapdoor to gain access without going through the usual security access procedures.

this code recognizes some special sequence of input or is triggered by being a run form the certain user id.

Logic Bomb.

It is the oldest types of program threat predating virus and worms this code is to be embedded is some Legiter Make program set to the explode when.

Some condition are met.

Trajan Horse.

It is a useful or apparently useful, program or command procedure contain containing hidden code. when invoked, performs some wanted or harmful function.

It can be used establish functions indirectly an unauthorized user could n't contact directly.

Zombie

→ Zombie program secretly takes over another internet attached computer and the uses that computer to launch attacks that are difficult to trace the zombie's creater.

virus :

→ The most sophisticated types of threats to computers presented by programs exploit vulnerabilities in computing systems

Nature of Virsuses.

→ A virsus is a program that can "infect" other program by modify them

→ It includes copy of virus program, which can then go on to infect other program

Biological virsus are tiny scraps of generic code - DNA or RNA.

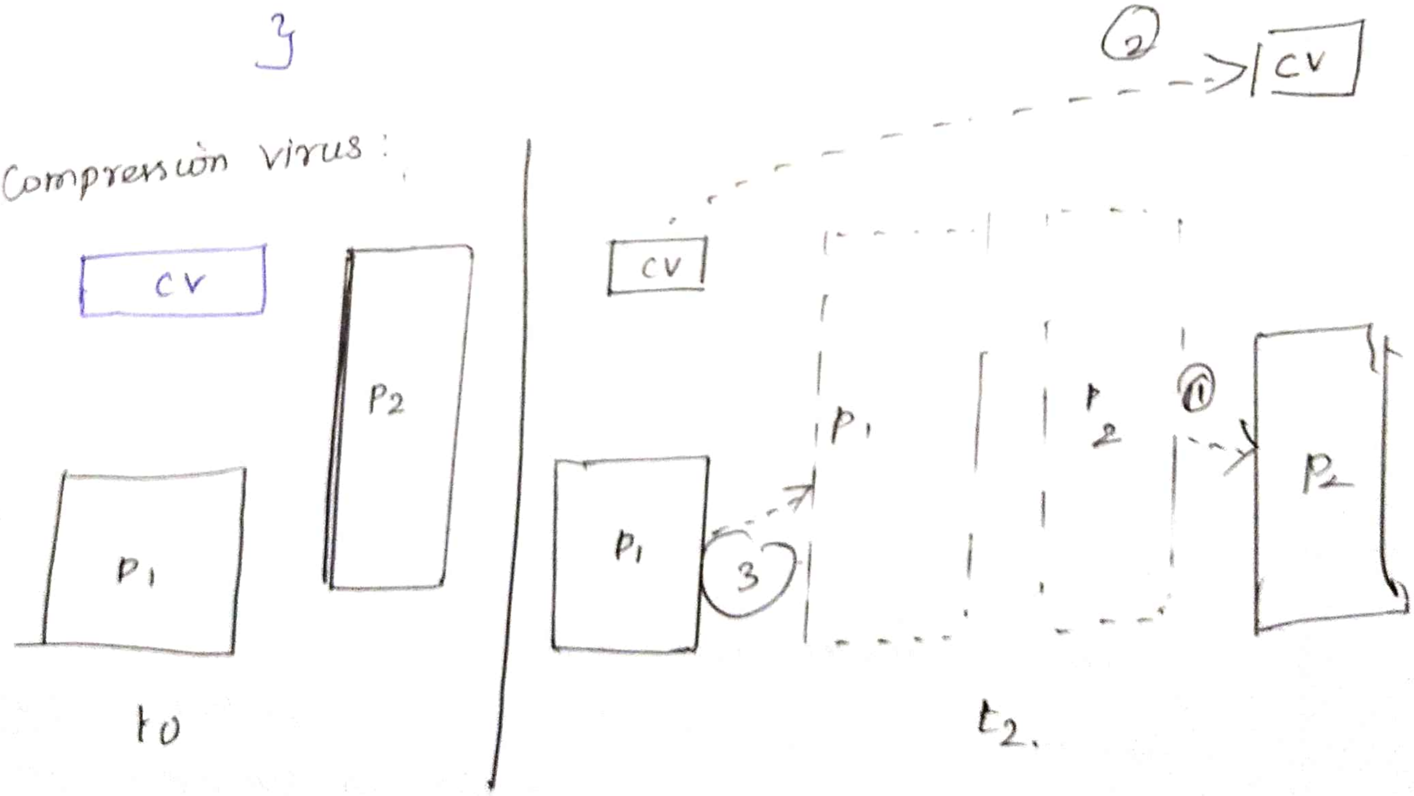
Virsus Structure:

Virsus canbe prepended or post pended ~~or~~ postpended to an excutable program or it can be embedded through some techniques.

Sample

```
program V :=
{
  go to main :
    1234567 :
  // source code related to subroutine and
  main program blocks
        next ;
      }
```

Compression virus:



(i) for each uninfected file P2 that is found compresses file to produce P2.

(ii) A copy of the virus is prepended to the compressed program

(iii) compressed version of original infected program

P1 is un compressed.

Types of virsus.

(i) Traditional common from viruses.

(ii) It attaches itself to excutable files and replicates when the infected program is executed by findind other excutable files to be infect.

Memory resident virsus.

bodges in main memory as a part of system program

Boot Sector virus.

infects a master boot record.

Macro virsus.

This is a newest types of viruses the macro virsus. compare to all virsus macro virsus constitutes 2/3 rd of ratio.

1) macro virsus is platform indepedent

2) macro virus infect the document

3) it is easily spred ex: email

Advantage. In microsoft word,

1. Auto execute
2. Auto macro
3. command macro

Email Virsuses.

1) It sends itself to everyone on the mailing list in the user's mail package.

2) It does Local damage

worm:

1) email facility - worm mail a copy of itself to other system.

2) Remote execution capablity

3. Remote login capablity

Morris worm.

the best known worm released by robert morris in 1998.

main process: It is a spread process.

* The worm performed this task through a lists and tables, which other machines trusted by this host.

Four Generation of Antivirsas.

1st generation

Simple scanners → It requrie a virsus signature to identify a viruse

2nd generation

It does not rely on a specific signature.

Recent worm attacks.

1. client to client via email
2. It spreads to web server by active scanning

Firewall Related Terminology.

1. A general. definition of Firewalls and their purpose
2. Terminology which is needed to better understand the Axs.

Firewall definition:

A firewall protects the network from unlawful access (ie) hackers, by blocking incoming connections which are not desired or unauthorized, It is inspecting incoming network packets.

Rules :

A firewall rule. is a smallest configurable component of the AXS GUARD firewall, A rule determines how a certain network packet is handled.

policies

A firewall policy is a logical set of firewal set of firewall rules organized in a certain order which is critical.

Security Level.

The level at which a firewall policy is assigned. (ie) an AXS GUARD group. user, group computer or system.

firewall Rights.

1) General term used to describe firewall Permissions and restrictions at a given security level ; (ie) the services a given user, group or computers and the system

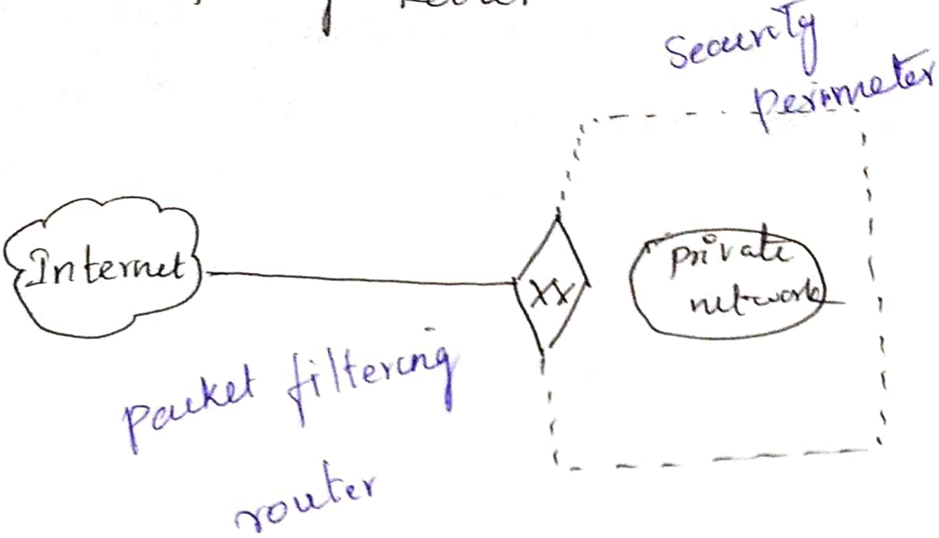
Types of firewalls.

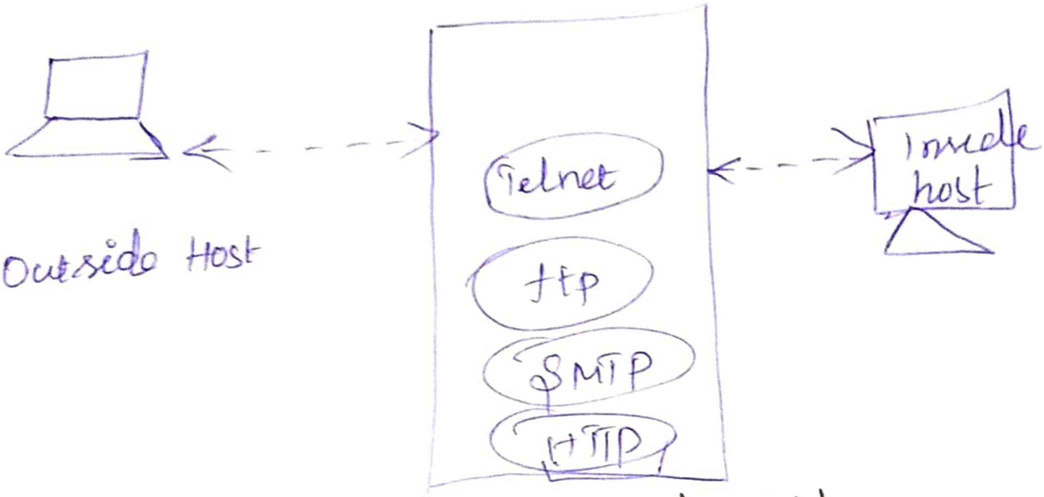
(i) packet filtering

(ii) Application level gateway

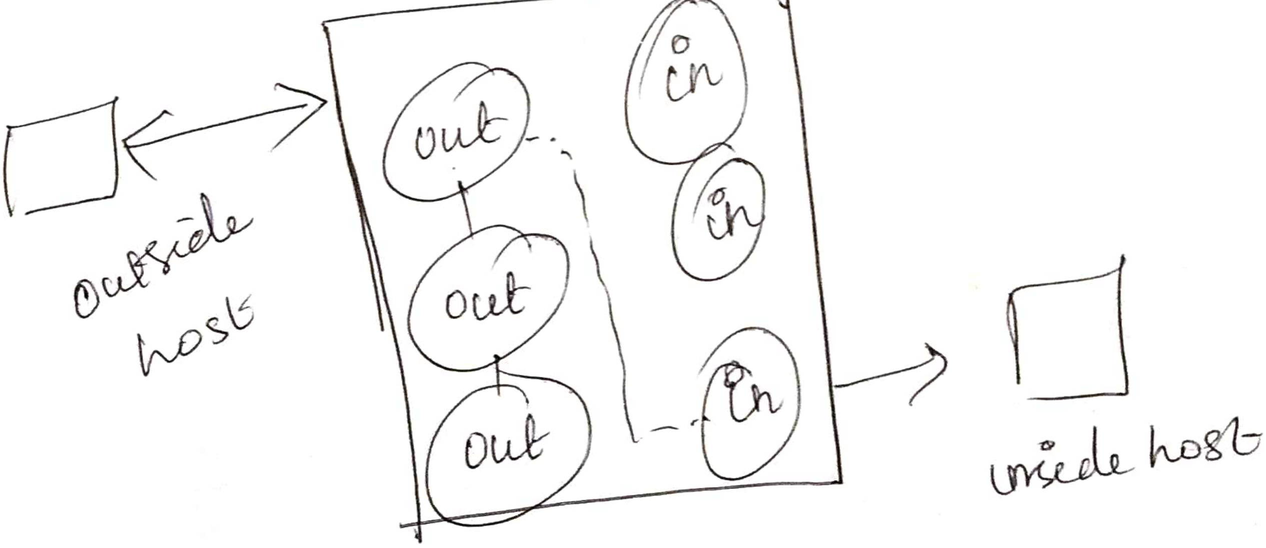
(iii) circuit level gateway

Packet filtering Router





circuit level gateway



Advantages.

(i) packet filtering is its ~~comp~~ semplicity

(ii) Transparent to users and very fast

Application level gateway

second level → proxty level

the user contact the gate way using a Tcp/IP application, such as telnet or ftp and the gateway asks user for name of the remote host to be accessed

circuit level gatway.

1. one between itself and a Tcp user on an inner host

2. one between itself and Tcp user on an outside host

firewall configuration.

it consist of following types.

1. screened host firewall

2. Screened host firewall

screened subnet firewall

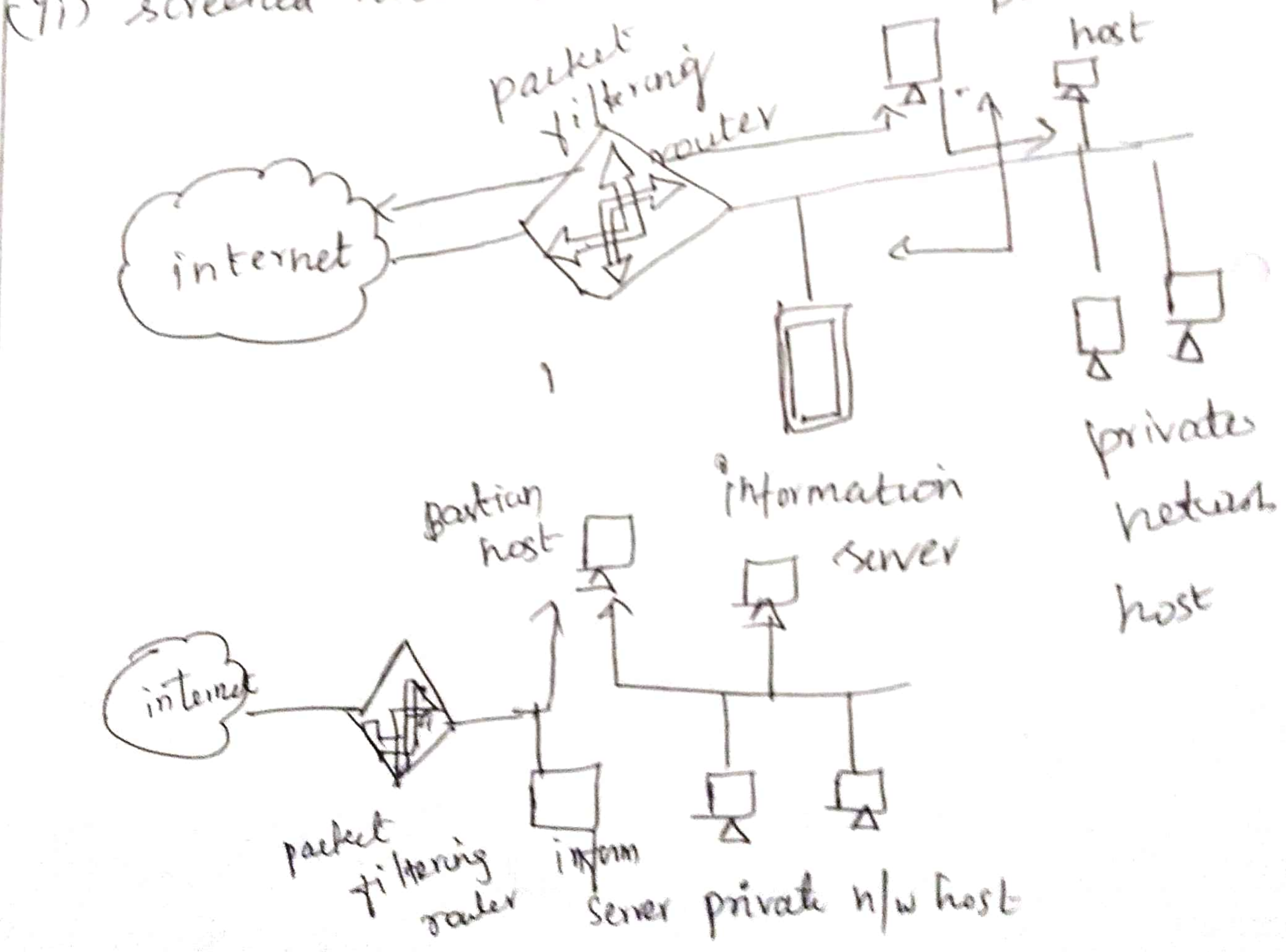
screen host firewall.

1) packet filtering router

2) A bastion host

packet filtering → for traffic · from the internet only ip packets from the bastian host are allowed out

(ii) screened host - dual home bastian



firewall need some specific specificatcons

1) h/w
2) cpu RAM, Disk
3. scabilily
4. Extensibility
5. high availabilty
6. compatebility
7. ease of use.

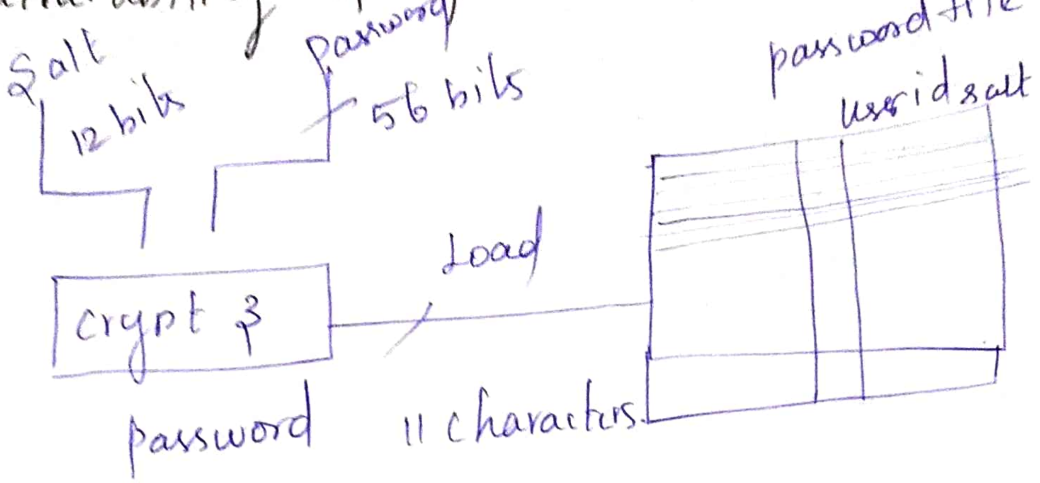
Password production

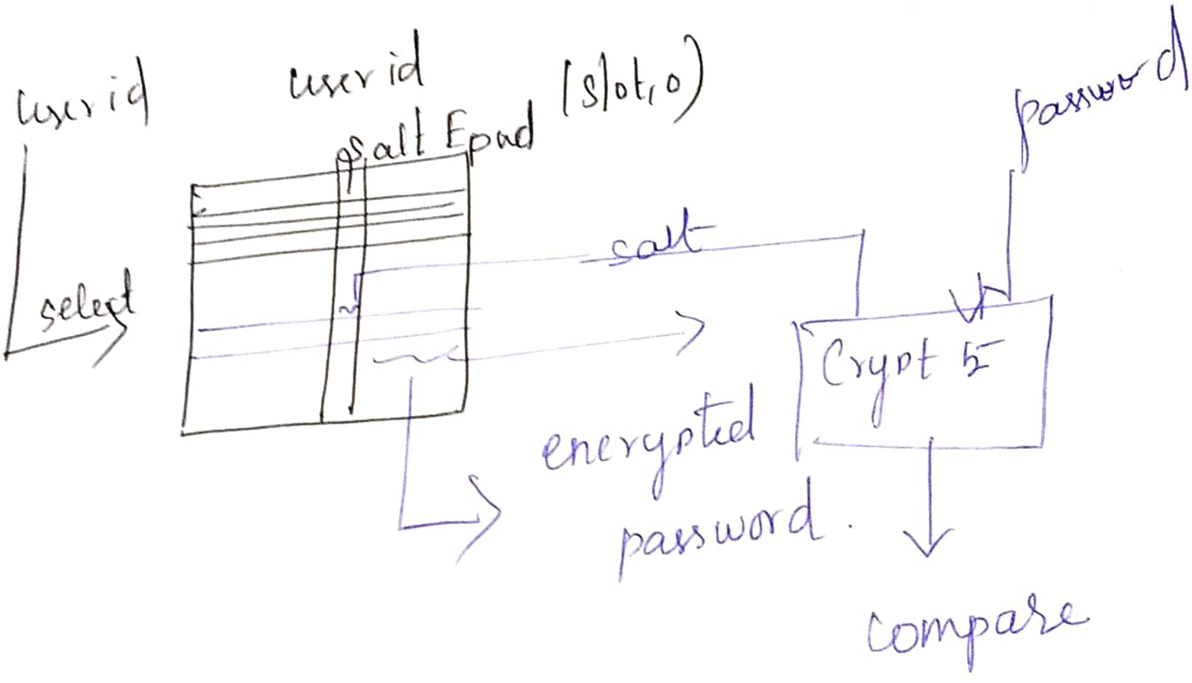
4 rules.
① without fire wall ~~[illegible]~~ policies.
② with firewall policies at the user level
③ with firewall policies at the group level

The front line of deffense against intruders is the password system, the password serves to authenticate the iD of the individual logging on the system.

1) the id determines whether the user is authorized to gain access to the system

vulnerability of passwords.





Password selection strategies.

1. user education
2. computer generated passwords
3. Reactive password checkeng
4. Practice password checking

the markove model is a quadraple $[M, A, T, k]$

$M \rightarrow$ No of states in the model

$A \rightarrow$ state space $\quad T \rightarrow$ matrix of transition probablities.

$k \rightarrow$ order of the model

$M = \{e\ \{a, b, c\}, T, 1\}$ where

$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

In transition matrix.

i^{th}, j^{th}, k^{th} char

$$t_{(ijk)} = \frac{f(i,j,k)}{f(i,j,\infty)}$$

$H_p(x_j) = y_i$; $1 \le i \le k$ $\quad 0 \le y \le N - 1$

$1 \le j \le k$

x_j → jth password dictionary

D → No of word$_k$ in password.

$$p \approx \left(1 - e^{kD/N}\right) = \left(1 - e^{k/R}\right)^k .$$

or equivalently

$$R \approx \frac{-k}{\ln\left(1 - p^{1/k}\right)}$$

k → no of hash functions

N → no of bits hash table

D → No of words in dictionary.

R → N/D Ratio of hash table size to dictionary size.