Unit-6

DATE: __/__/____
PAGE: _____

Web security

Web security refers to the protective measures and protocols that organization adopt to protect the organization from cyber criminals and threats that use the web channel.

Top web security threats
- Cross-site scripting (XSS)
- SQL Injection
- Phishing
- Ransomware
- Code Injection
- Viruses & worms
- Spyware
- Denial of service.

Security Measures
- Updated softwares
- Be aware of SQL Injection
- Cross-site Scripting (XSS)
- Error Messages
- Data validations
- Password

Secure Socket Layer (SSL)

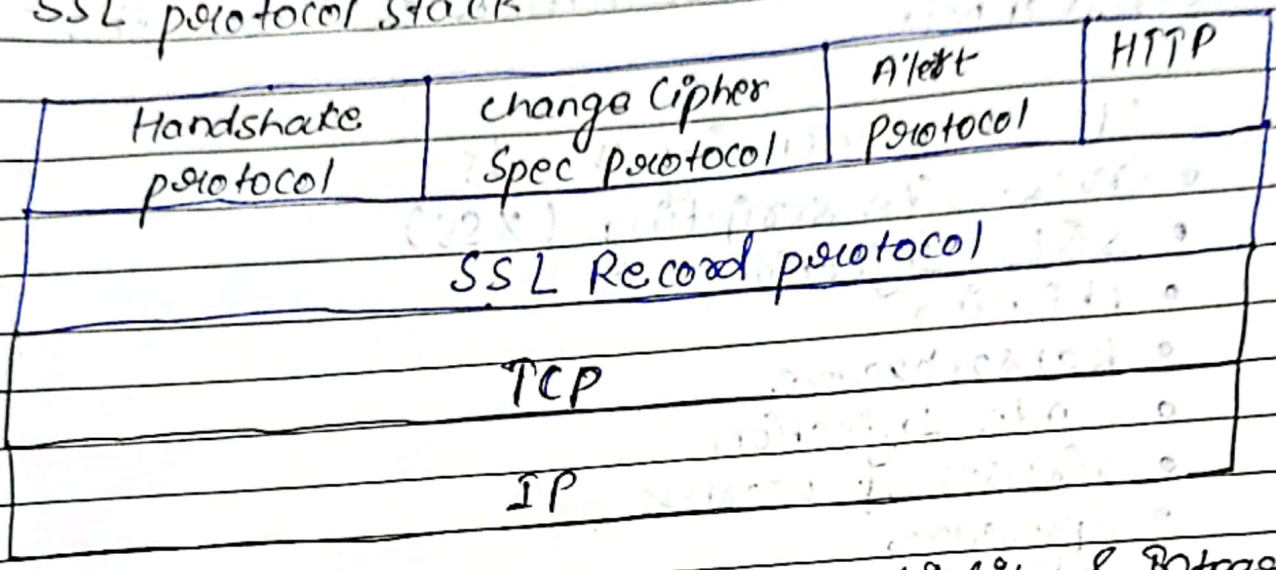
SSL provides security to the data that is transferred between web browser and web server.

It encrypts the link between a web server & browser and which ensures that all data passed between them remain private and free from attack

Good Write

→ lies between application layer and transport layer of TCP/IP

SSL protocol stack



SSL Record protocol (Confidentiality & Integrity)

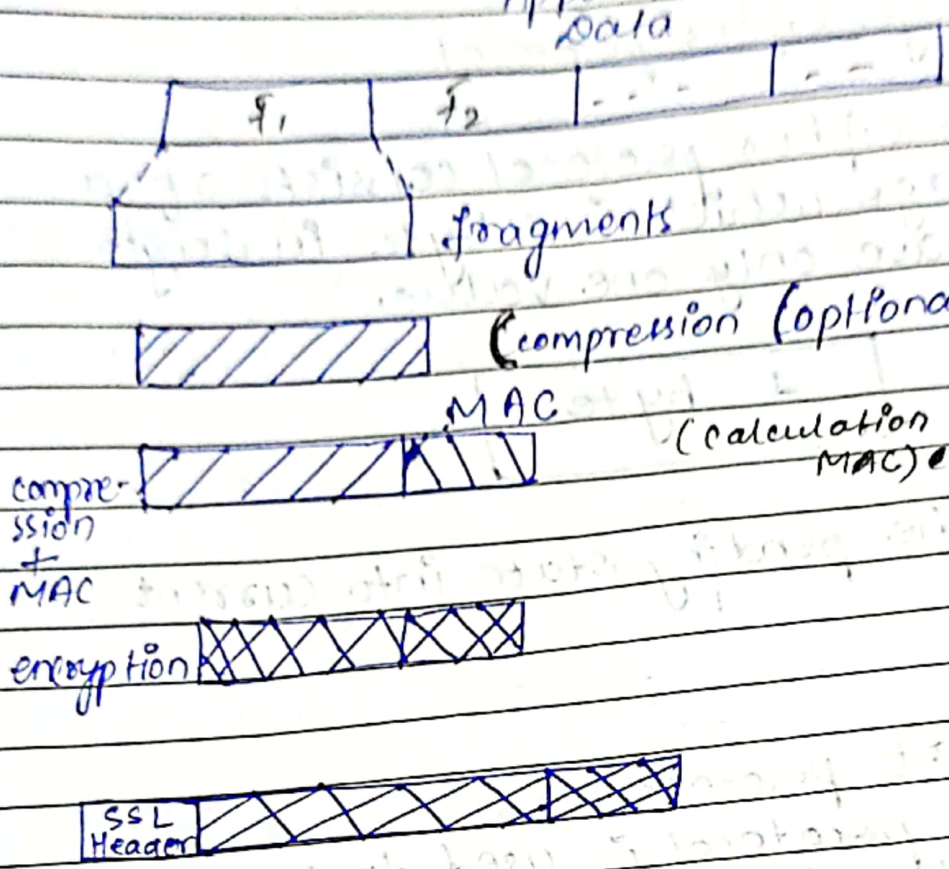
It has two services

1) Confidentiality (done by encryption)
2) Message Integrity (done by MAC)

Working:-

Application data is divided into fragments. The fragments is compressed and then encrypted MAC (Message Authentication code) generated by SHA algo, and MD5 (Message digest) is appended. At last SSL header is appended to the data.

block size or fragment size = 2^{14} bytes



Handshake Protocol

It is used to establish sessions. This protocol allows client & server to authenticate each other by sending a series of message to each other. Handshake protocol uses four phases to complete its cycle.

- Ensure Authentication
- most complicated part in SSL
- key exchange between client & server

working

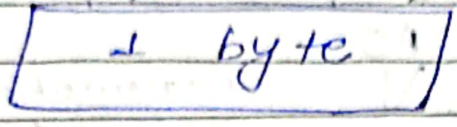
- connection establishment with server
- key exchange from server to client
- ~~Handshake done from server~~
- key exchange from client to server
- Handshake done from server.

Good Write

DATE: __/__/____
PAGE: _____

• SSL change cipher protocol

Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value.



→ copies the pending state into current state.

* SSL Alert protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes

Level is further classified into two parts.

Warning (level = 1)
- Bad certificate
- No certificate
- Certificate expired
- Certificate unknown
- Close notify

fatal Error (level=2)
Handshake failure
Decompression failure
illegal parameters
Bad record MAC
Unexpected message

Features of SSL
- can be tailored to the specific needs of the given application.
- Originated by netscape.
- Designed to make use of TCP to provide reliable end-to-end secure service.
- This is two layered protocol.

Versions of SSL

SSL 1 - Never released because of high insecurity.
SSL 2 - Released in 1995
SSL 3 - " " 1996.

TLS 1.0 " " 1999
" 1.1 " " 2006
1.2 " " 2008
1.3 " " 2018

Good Write

443 → https

DATE: __/__/____
PAGE: _____

Transport Layer Security

→ defined in RFC 2246 (Req. for comments)
→ for providing security in transport layer.
→ derived from SSL
→ ensures that no 3rd party may evasedrop or tempers with any message.

Benefits of TLS

Encryption.
Interoperability
Algorithm flexibility
Ease of Deployment
Ease of Use.

Working

Uses client server handshake mechanism.

1. Key exchange b/w client and server
   (by Diffie Hellman key Exchange Alg)

2. Now TLS protocol will open an encryption channel.
   (by RC4 / IDEA / DES Algorithm)

3. It also ensures that message are not altered.
   (by MD5 / SHA Algo)

* RFC 2246 is similar to SSL V3

Good Write

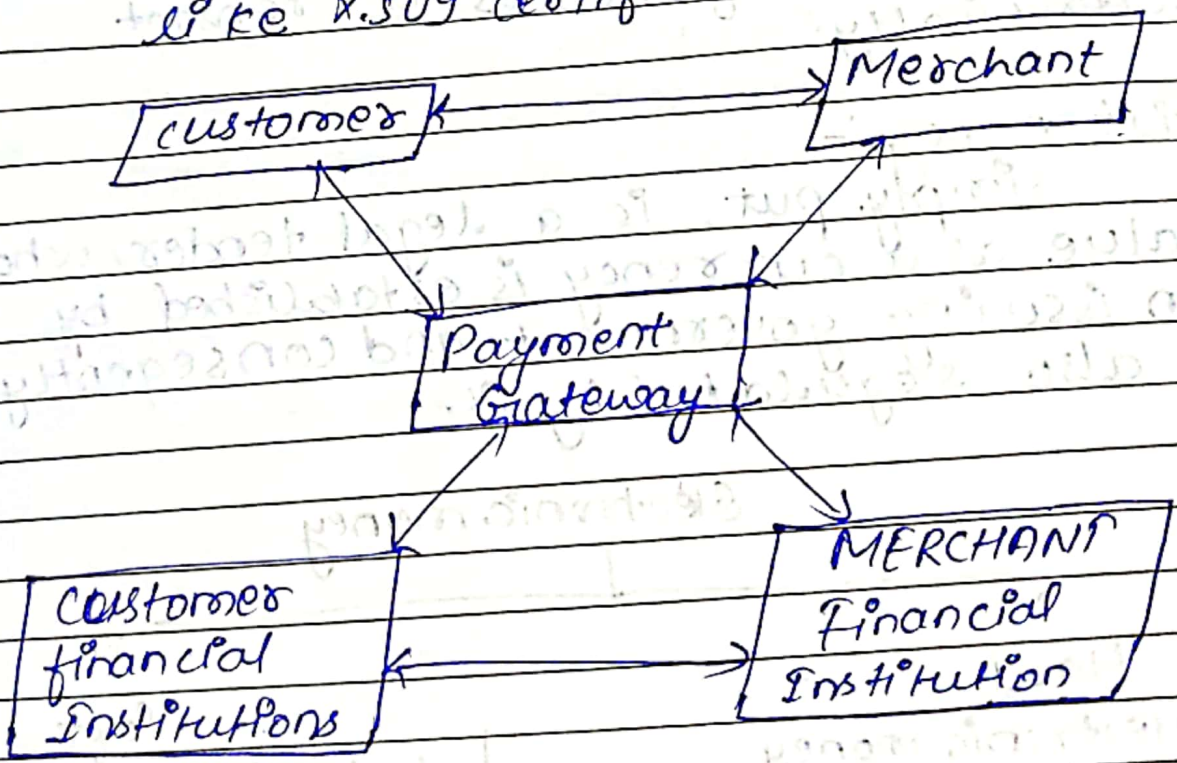
PI = Payment Info
OI = Order Info

DATE: __/__/____
PAGE: _____

Secure Electronic transaction
→ ensures security & Integrity of the electronic transactions done using credit card, debit card, UPI, netbanking)
→ uses different encryptions & hashing techiques to secure payments.

→ Set protocol restricts the revealing of credit card details to merchants (amazon, flipkart) thus keeping hackers and theives at bay.

→ implemented using digital certificates like X.509 certificate.



Requirement that SET protocol need to ma
- Mutual Authentication
- confidentiality of (PI and OI)
- Provid Integrity
- interoperability and security mechanism.

Good Write

participant in SET

Card holder.
Customer bank
Merchant
Acquirer
Certificate authority

Electronic Money :-

Electronic money refers to the currency electronically stored on electronic systems and digital database, as opposed to physical paper and coin money and is used to make it easier for users to transact electronically.

Fiat money :-

simply put, is a legal tender, whose value as a currency is established by an issuing government and consequently is also regulated by it.

Electronic money

Hard	Soft
electronic money that is used for irreversible transactions, highly secured & more or less procedural in nature.	electronic money used for reversible or flexible transactions cancelling a transaction or modifying the payment price.

Good Write

DATE: __/__/____
PAGE: _____

Features of E-money

- Store of value :-
- Medium of exchange
- Unit of Account
- Standard of deferred payment.

Advantage of electronic money

- Increased flexibility and convenience
- Historical record
- prevents fraudulent activities
- Instantaneous
- Increased security

Disadvantages of electronic money

- Necesity of certain infrastructure.
- Possible security breaches/hacks
- Online scam.

Good Write

DATE: __/__/____
PAGE: _____

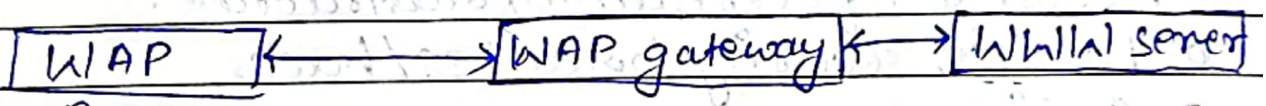
WAP security

It is a specification for a set of communication protocols to standardize the way wireless devices such as mobile phones & radio transceivers, can be used for internet access including email, the web, newsgroups and instant messaging.

Wireless Markup Language was used to create pages that can be delivered using WAP.

How the WAP work?

WAP Architecture



WAP Model & layers

Similar to client - server model but uses an additional WAP gateway as an intermediary between client & server.

WAP protocol stack

Wireless Application Environment
Wireless session protocol
Wireless transaction protocol
Wireless transport layer security
Wireless datagram protocol

DATE: / /
PAGE:

Use of WAP

- Wireless network & mobile phone operator.
- Content providers
- End Users

Not much famous in all countries because of widespread HTML compatibility in mobile phones.

Firewall design pouncipals

A firewall is a hardware or software to prevent a private computer or network of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers & networks.

Pouncipales

- Developing security policy
  Without it, there is increase in risk as there will not be a proper implementation of security solutions.

- Simple solution Design:-
  If the design of solution is complex then it will be difficult to implement, maintain and upgrades by analying more possible threats, efficiency keeping in mind yet simple in struct

DATE: __/__/____
PAGE: _____

- Choosing right device:
  If the outdated device is used for designing firewall, it exposes the network to risk and is almost useless.

- Layered defence
  A network defence must be multi-layered because it gives an edge to the security design and finally neutralize the attack on the system.

- Considers Internal threats
  Sometimes internal threats ~~are~~ is ~~be~~ neglected which makes the network weaker and vulnerable. filtering them adds a new layer in security point of view.

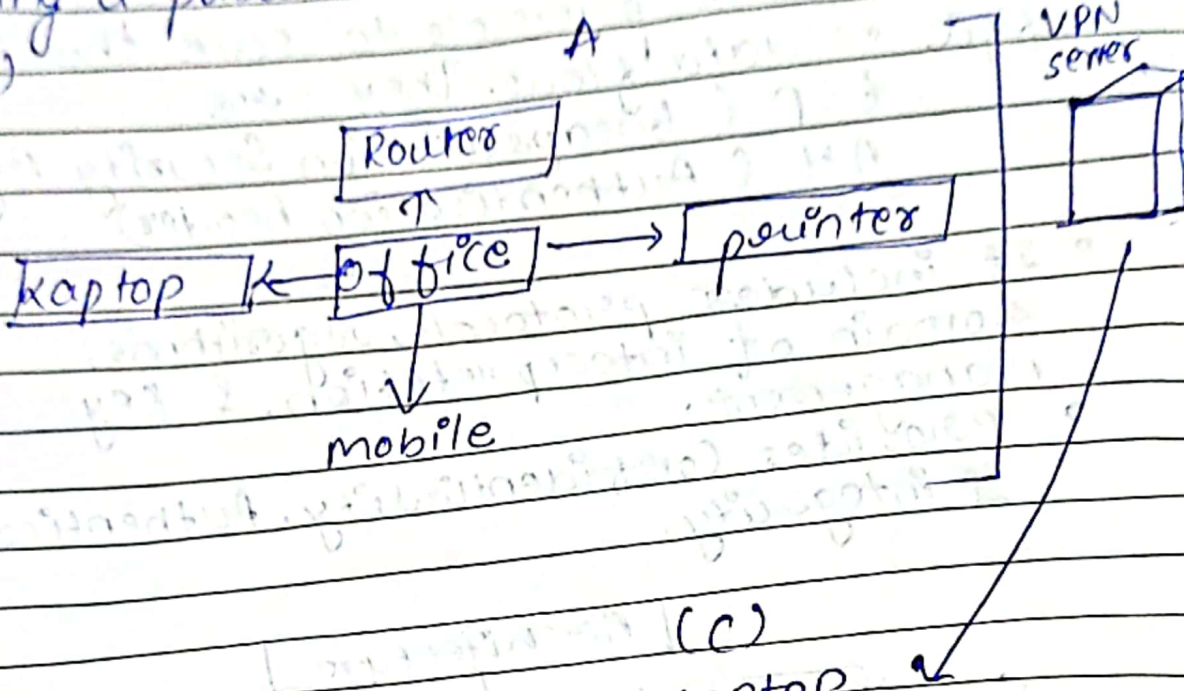
Need & Importance

Different Requirements
Outlining policies
Identifying policies
Setting Restrictions
Indentify Deployment locations

Virtual private Network Security

It is a way to extend a private network using a public network such as internet.

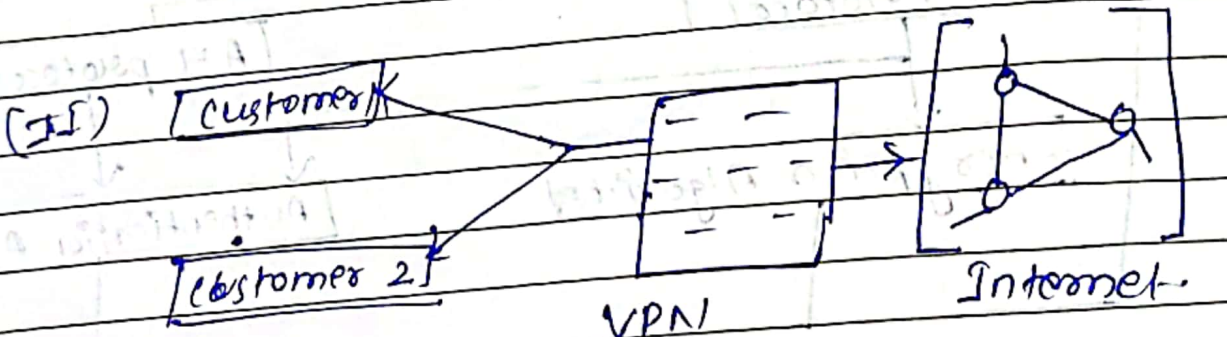
(I)



(C)

laptop

(II)



Good Write

DATE: __/__/____
PAGE: _____

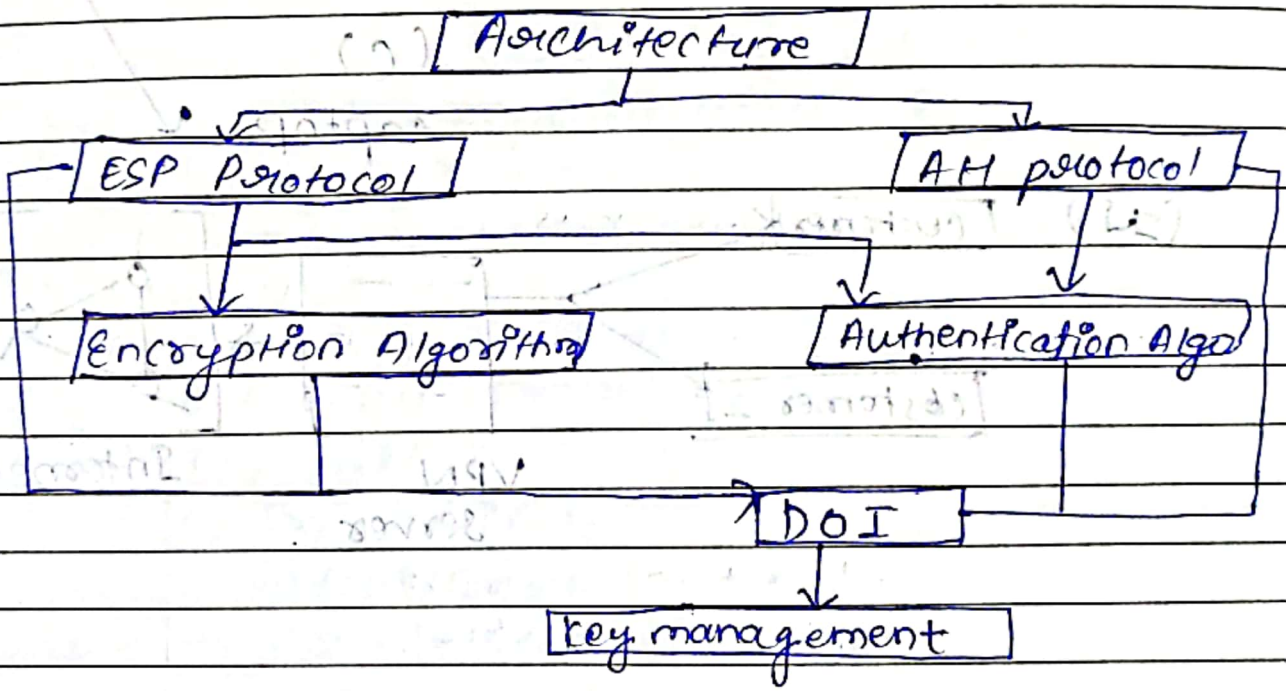
IP Security

It is a framework for protecting communication over IP.

1) Architecture

- It uses two protocols to secure the traffic or data flow. They are
  ESP (Encapsulation Security Payload)
  AH (Authentication header)

- It includes protocols, algorithms, domain of interpretation, & key management.
- provides confidentiality, Authentication & integrity.



Architecture covers the general concepts definations, protocols, algo. and security requirements of IP security technology.

Good Write

2) ESP protocol

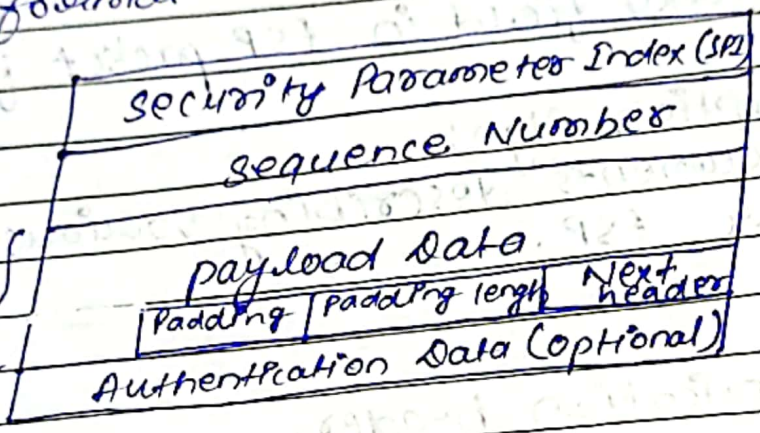
provides a confidentiality service.

Implemented either two ways:

ESP with optional Authentication

ESP with Authentication.

packet format



Security parameter Index (SPI)

used by security association to give unique number to the connection built between the client & server.

sequence number

are alloted to every packet so that on the receiver side packets can be arranged properly.

payload Data :-

It's an actual data that are in encrypted form for confidentiality purpose.

Good Write

padding:-
Extra bits of space are added to the original message in order to ensure confidentiality.

Next header:-
means next payload or next actual data.

Authentication data:-
optional field in ESP packet format.

3) Encryption Algo:-
documents describing various encryption algo for ESP.

4) Authentication header.
provides authentication and integrity service.
Implemented as Authentication with Integrity

Next header	Payload Length	Reserved
Security parameter Index		
Sequence Number		
Authentication Data (Integrity Checksum)		

It covers the packet format and general issue related to the use of AH for packet authentication & integrity.

Good Write

DATE : __/__/____
PAGE : _____

5. Authentication Algo :-
contains the set of documents that describe the authentication algorithm used for AH & for the authentication option of ESP.

6. DOI
Identifier that supports both AH & ESP protocol and contains values needed for documentation related to each other.

7. Key Management :-
constains the document that describes how the keys are exchanged between sender and receiver.

Good Write

DATE: / /
PAGE:

Electronic mail security

It is the process of ensuring the availability, integrity and authenticity of email communications by protecting against the risk of email threats.

PGP (Pretty Good Privacy)

* invented by phil zimmermann in 1991
* N/w security concept which provide email-security.
* It is an encryption that provides cryptographic privacy and integrity also authentication for data communication

* PGP is used for signing, encryption and decrypting texts, emails, files, directories and to increase the security of email communications.

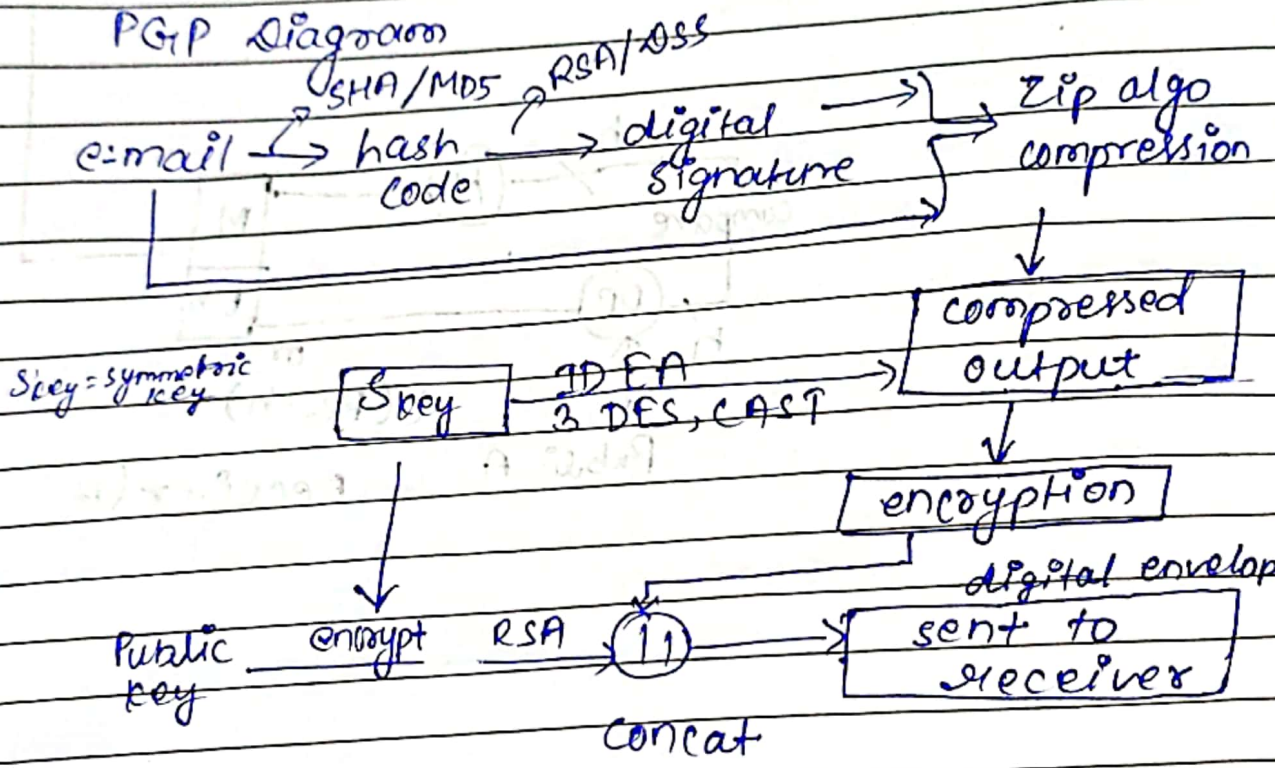
PGP encryption uses a serial combination of (i) hashing
(ii) Data compression
(iii) Symmetric key cryptograph
(iv) Asymmetric key cryptography

and each step uses one of the several supported algorithm like RSA, IDEA, SHA etc.

Services provided by PGP
* authentication (using digital signature)
* confidentiality

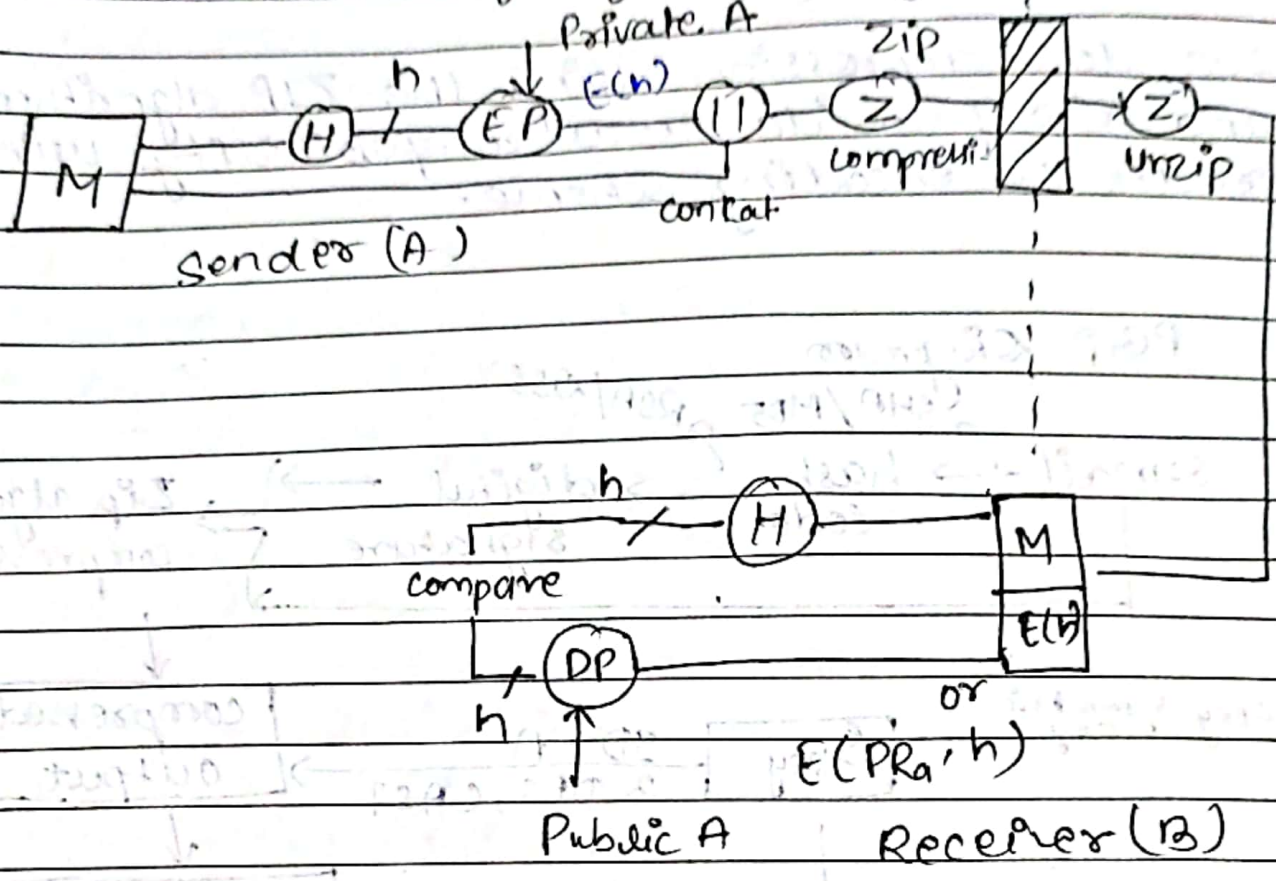
We do compression using the ZIP algorithm and also provide email compatibility using radix-64 encoding scheme.

PGP Diagram



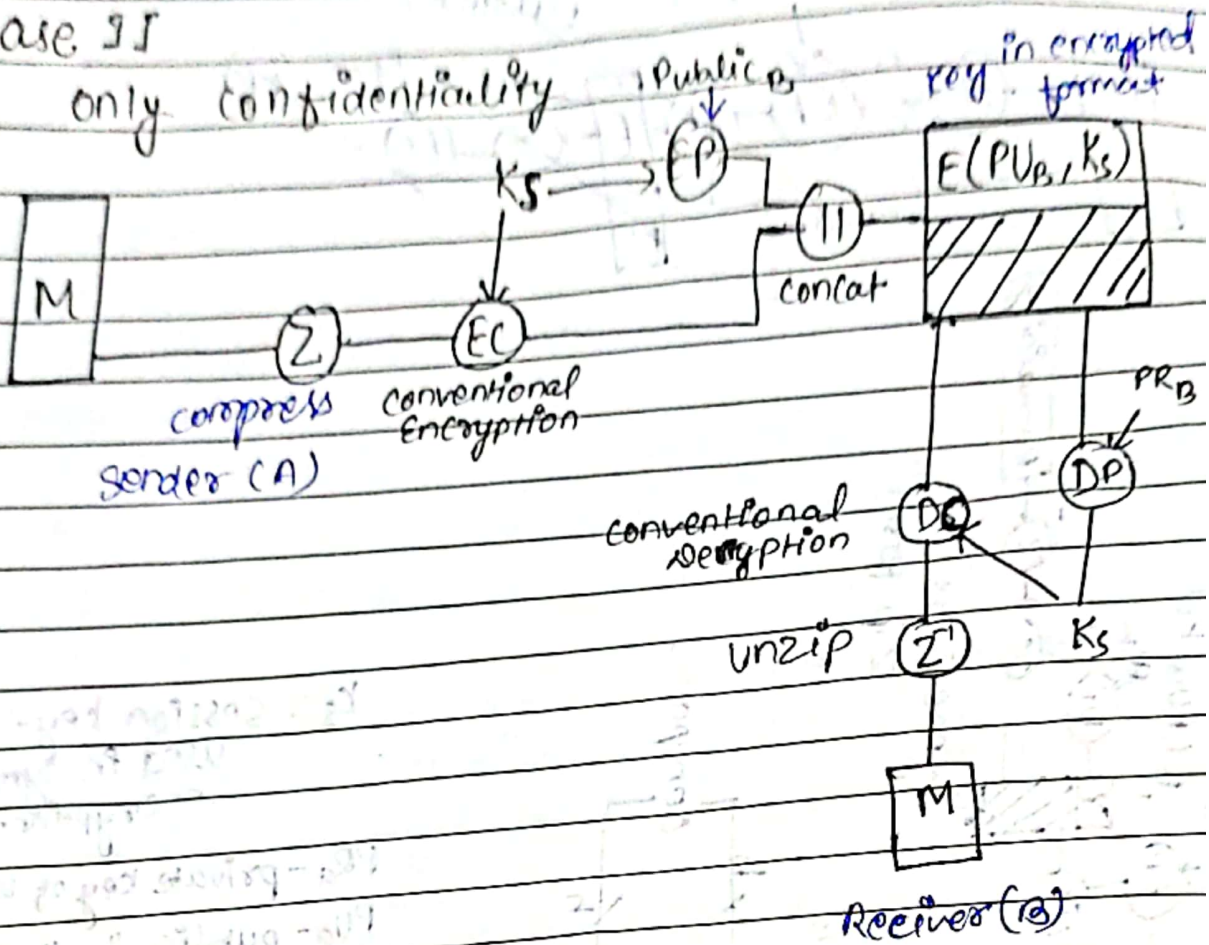
Case-I

authentication + digital signature achieved (No confidentiality)



Case II

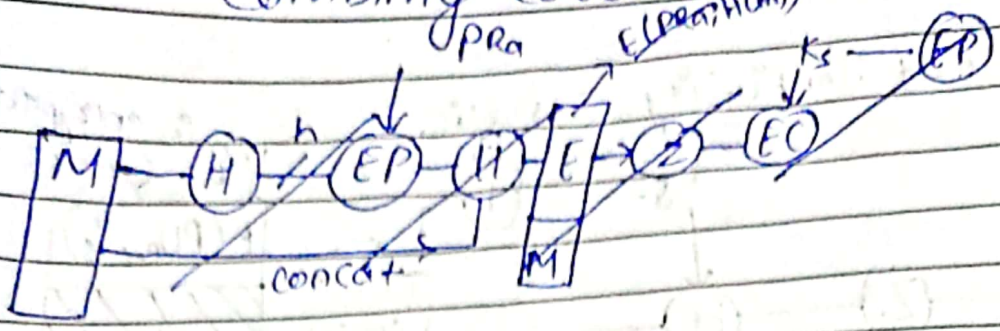
only confidentiality

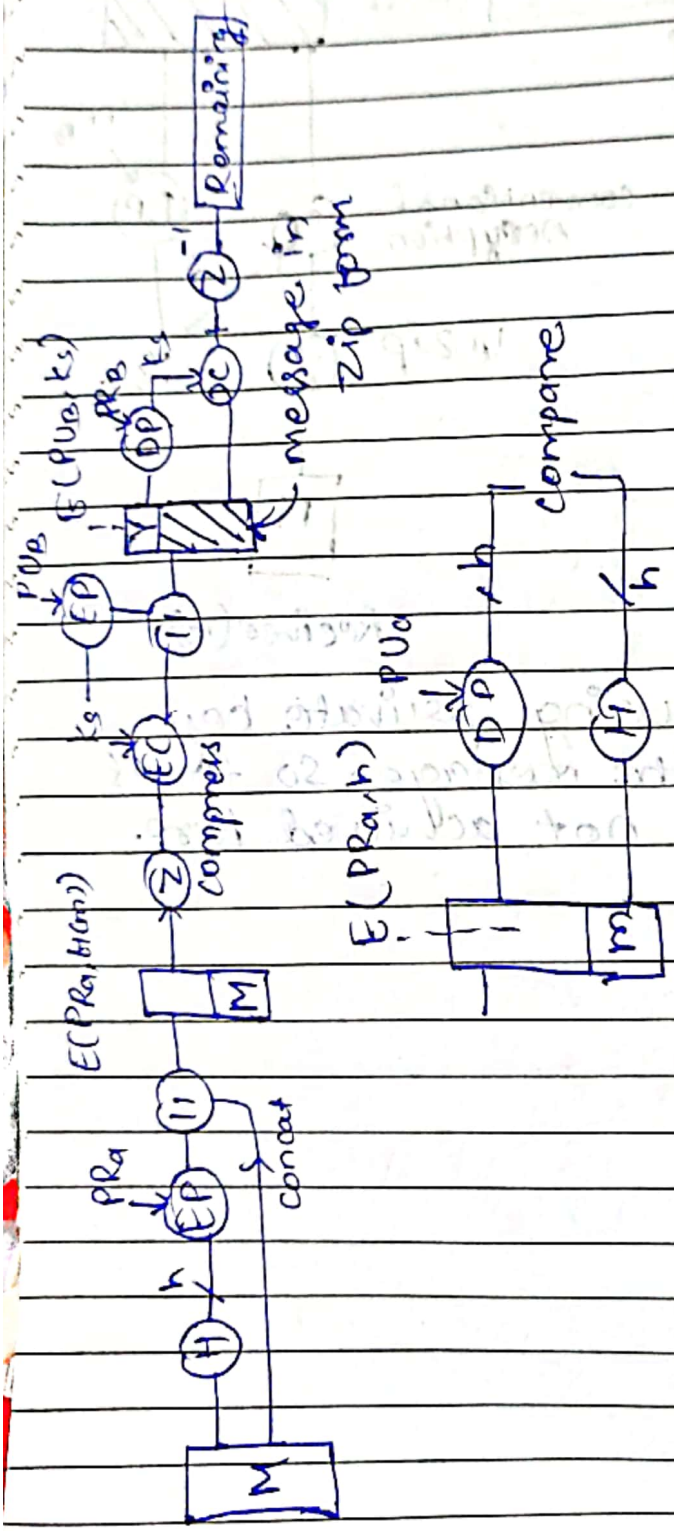


Here we are not using private key of sender to encrypt the message. So that's why authentication is not achieved here.

DATE: __/__/____
PAGE: I I

Combing case 1 and case 2





Ks = session key used in symmetric encryption.

PRa - private key of user A

PUa - public " " " "

EP - public key encryption

DP - public key decryption

EC - conventional symmetric encryption

DC - conventional symmetric decryption.

h = hash code

H = hash function

Z = compression algo

Good Write

DATE: / /
PAGE:

MIME (Multipurpose Internet Mail Extension)

* MIME is a standard which was proposed by Bell Communication in 1991 in order to expand the limited capabilities of email.

Email has a simple structure
Email can send messages only in NVT 7-bit ascii format.

In short, MIME is a supplementary protocol or a add which allows non ascii data to be sent through email (using SMTP)

It allows users to exchange different kinds of data files on the internet like audio video, images etc.

MIME is an extension to the Internet Email protocol.

Email with mime formatting are typically transmitted with standard protocols like SMTP (simple mail transfer protocol), POP (post offices protocol) and the IMAP (Internet Message Access protocol)

Although MIME was designed mainly for SMTP its content types are also important in other communication protocols.

eg) In HTTP protocol for the world wide web servers insert a MIME header field

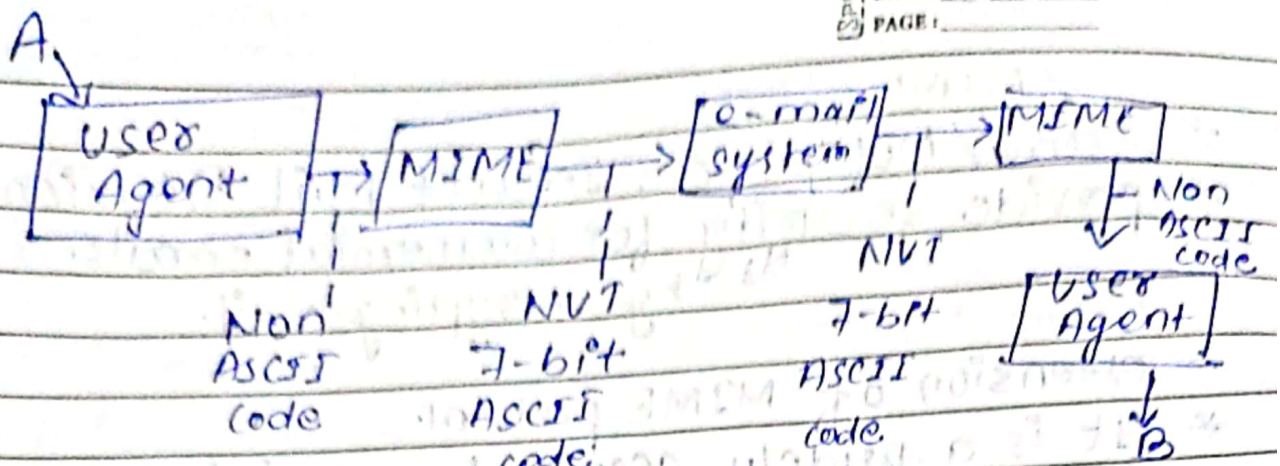
at the beginning of any web transmission.

Limitations of SMTP (need of MIME)

i) SMTP has a very simple structure.
ii) can only send messages in NVT 7-bit ascii format.
iii) cannot be used for languages that do not support 7-bit ascii format such as French, German etc. So in order to make SMTP more broad, we use MIME.
iv) cannot be used to send binary files or video or audio data.

MIME header
added to the original email header section to define transformation
There are 5 headers which we add to the original header.

1) MIME Version - (currently 1.1)
2) Content Type - defines type of data used in msg like audio, video etc.
3) Content Transfer-encoding -
tells method used for encoding (eg 8 bit encoding)
4) Content Id - helps in uniquely identifying the message.
5) content description
it defines whether the body is actually image, video or audio.



MIME Header

MIME: version 1.1
content-type: type/subtype
content-Transfer-Encoding: encoding type
content id: msg id
content description: textual explaination of non textual text/contents

E-Mail body

Good Write

DATE: __/__/____
PAGE: _____

S/MIME

* Secure / Multipurpose Internet Mail Extension.
* provide security for commercial emails.
  (i) by encrypting mail.

* extension of MIME protocol.
* It is a widely accepted method (or more precisely, a protocol) for sending digitally signed and encrypted messages.
  i.e.
  it allows us to digitally sign our email to verify ourselves as the legitimate sender. (& also encryption & decryption of mails)

* S/MIME is based on asymmetric key encryption.

Function provided by S/MIME

(i) Authetication
(ii) Message integrity
(iii) Non-repudiation of origin (using digita signature)
iv) Privacy
v) data security (using encryption)

In short
S/MIME is a protocol used to encrypt emails & digitally signed them.

DATE: __/__/____
PAGE: _____

1st version of S/MIME → 1995
2nd → 1998
3rd → 1999

3rd version is supported in the following.
- Microsoft outlook 2000
- Microsoft exchange 5.5 & later.

* What does S/MIME does?

It provides

(i) Digital signature
(provides authentication + non repudiation)
(ii) msg encryption
(provides confidentiality + data integrity)

DATE: __/__/____
PAGE: _____

Authentication Applications

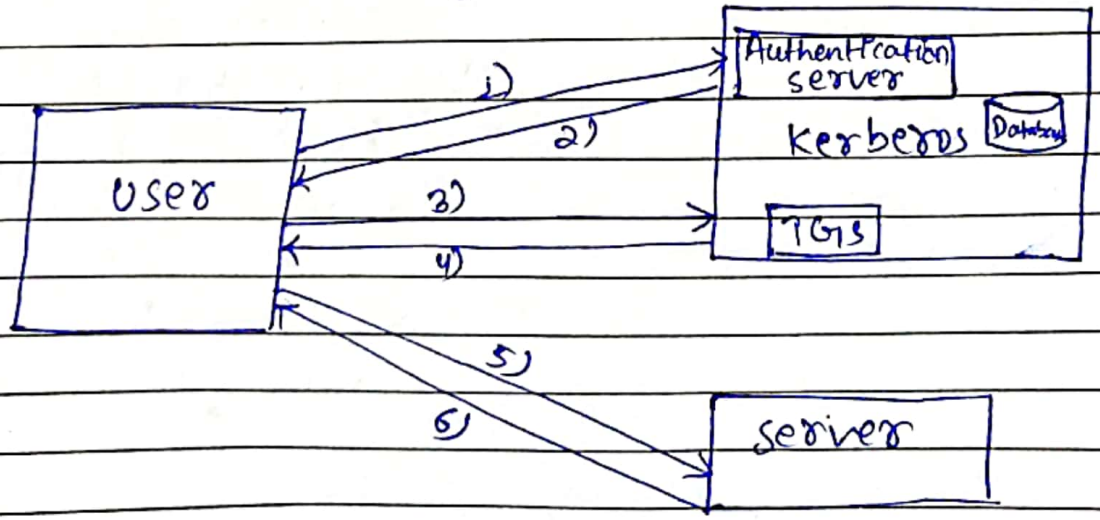
Kerberos provides a centralized authentication server whose function is to authenticate users to servers & servers to users
- client server architecture.
- It runs as a 3rd party trusted server known as key Distribution Center (KDC)
- Symmetric key.

main components of kerberos are :-

- Authentication Server (AS)
  performs the initial authentication & ticket for ticket granting service.

- Database:
  AS verifies the access rights of users in the database.

- Ticket Granting Server (TGS)
  issue ticket for server.



Good Write

DATE: __/__/____
PAGE: _____

Step 1:-
User login and request services on the host. Thus user requests for ticket-granting service.

Step 2:-
Authentication server verifies user's access right using database and then gives ticket granting-ticket and session key. Results are encrypted using the password of the user.

Step 3:
The decryption of the message is done using the password then send the ticket to TGS. The ticket contains authenticators like user name, network addresses.

Step 4:
Ticket Granting Server decrypts the ticket sent by user and authenticator verifies the request then creates the ticket for requesting services from the server.

Step 5:
The user sends the Ticket and Authenticator to the server.

Step 6:
The server verifies the Ticket and athenticator then generate access to the service. After this user can access the services.

Good Write

DATE: __/__/____
PAGE: _____

Kerberos Limitations

- doesnot work well in timeshare environment.
- Secured kerberos server.
- scalability.
- May result in cascading loss of trust.
- Assumes work stations are secure.

X.509

- digital ~~signature~~ certificate accepted internationally.
- doesnot generate any keys but provides a way to access public keys.
- There are several elements in X509 certificate. It has 3 versions

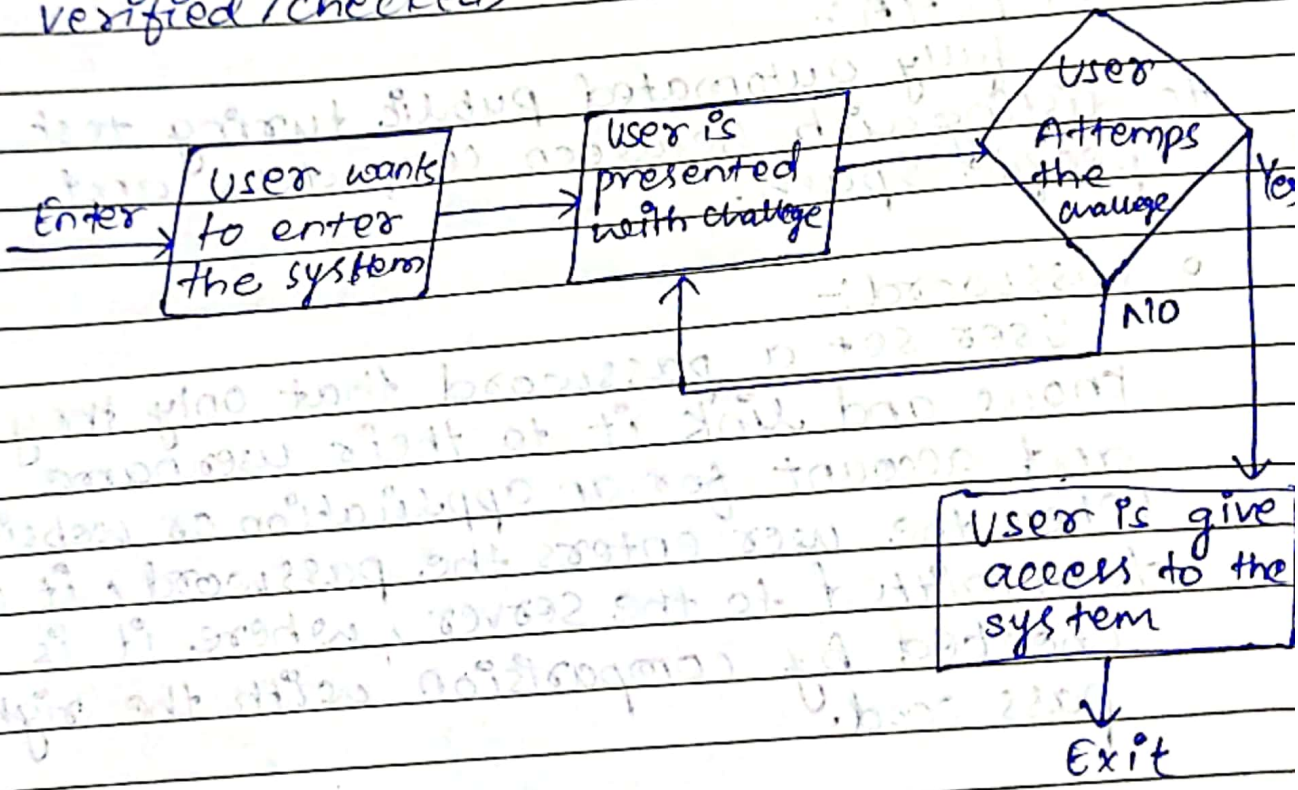
versions	Version 1
Serial Number	Version 2
Signature Algorithm Identifier	Version 3
Issuer Name	
Validity period	
Subject Name	
Public key Information	
Issue unique ID	
Subject unique ID	
Extension	

Good Write

DATE: __/__/____
PAGE: _____

Challenge Response Authentication

- It is most popular method for authenticating operations.
- They are a collection of protocols in which one side issues a challenge (to be addressed) and the otherside is required to respond with the right response (to be verified/checked) in order to be authenticated



* Challenge question comes in two flavour
  - Static question:
    → Security question that you have saved as a part of account set up is static.
  - Dynamic question:
    The task are choosen at random with assumption that user is genuine one.

DATE: __/__/____
PAGE: _____

Methods of authentication:-
Broadly they are of 3 types. They are:-
Knowledge based :- pin, password so on
Property based :- key, smart card so on
Biology based :- facial, iris, and so on

Other additional are :-

- CAPTCHA :-
  fully automated public turing test to distinguish between computers and people spam.

- Password :-
  User set a password that only they know and link it to their username and account for an application or website. When the user enters the password, it is transmitted to the server, where it is checked by comparision with the right password.

- Biometrics
  Every time a user wishes to verify himself he must provide his unique biometric information to authenticating system for verification.

DATE: / /
PAGE:

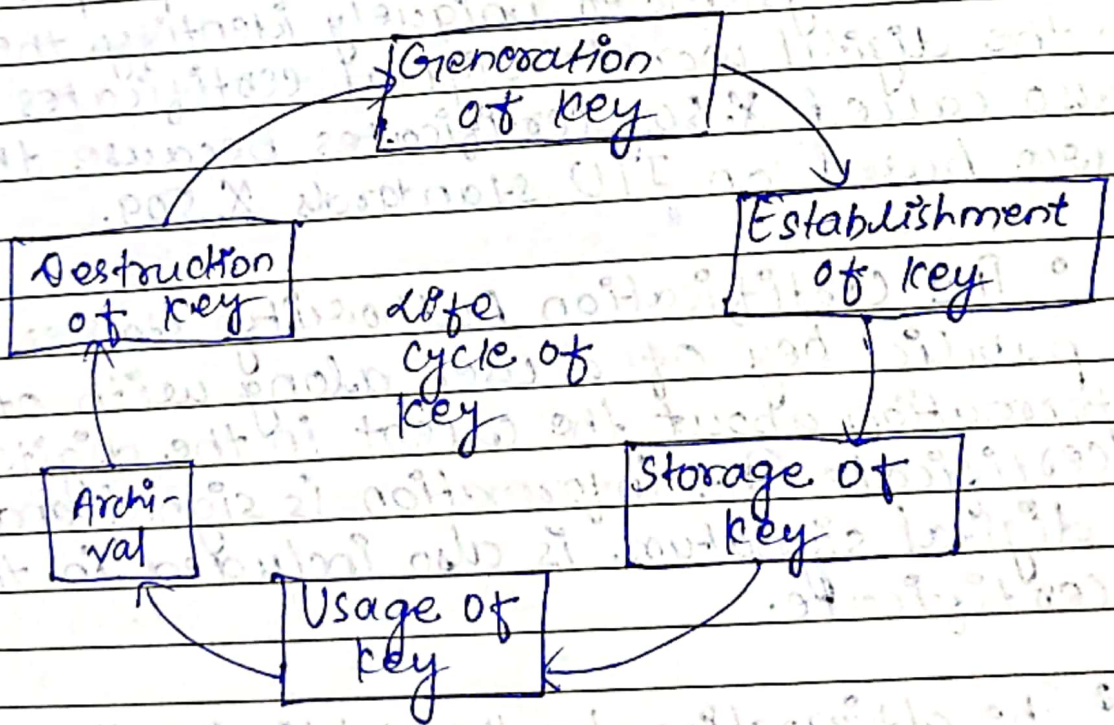
Publick key Infrastructure :-

PKI is the governing body behind issuing digital certificate to protect confidential data and give unique identities to users and systems.

Managing key (key management)

Security of cryptosystem relies on its key. The 3 main areas of key management are as follows:-

- A cryptographic key is a piece of data that must be managed by secure administration.



Good Write

DATE: __/__/____
PAGE: ____

- Public key management further requires
  - keeping the private key secrete.
  - Assuring the public key.

Components of public key Infrastructure

- Digital certificate
- Private key token
- Registration authority
- Certification Authority
- CMS or certification management system (explain)

Digital certificate

Digital certificates are issued to people and electronic systems to uniquely identify them in the digital world. Digital certificates are also called X.509 certificates because they are based on ITU standards X.509.

- The certification Authority stories the public key of a user along with other information about the client in the digital certificate. The information is signed and a digital signature is also included in the certificate.

- The affirmation for the public key then thus be retrieved by validating the signature using public key of certification authority.

Good Write

private key token

while the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. If an attacker gains access to the computer, he can easily gain access to the private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

~~Digital Signatures~~

Certifying Authority (CA)

- the CA issues certificate to client and assists other users to verify the certificate.
- They take responsibility for identifying correctly the identity of the client asking for a certificate to be issued and ensures that the information contained within the certificate is correct and digitally signs it.

function of CA :-

Generating key pairs, issuing digital certificate, publishing certificate, verifying certificate, revocation of certificate.

Registration Authority

CA may use a third party registration Authority to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Good Morning

DATE: __/__/____
PAGE: _____

Digital Signature

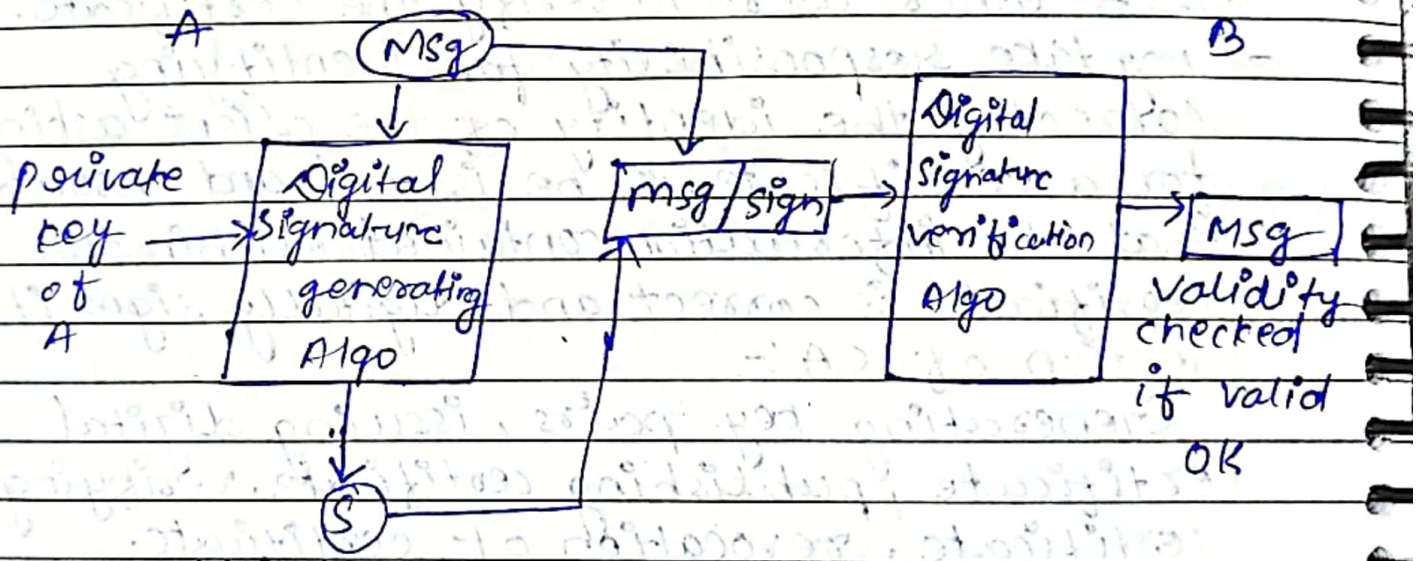
- It is a mathematical technique used to validate the authenticity & integrity of a message, software or digital document.

digital equivalent of a hand written signature or stamped seal, but it offers far more inherent security.

→ based on asymmetric key

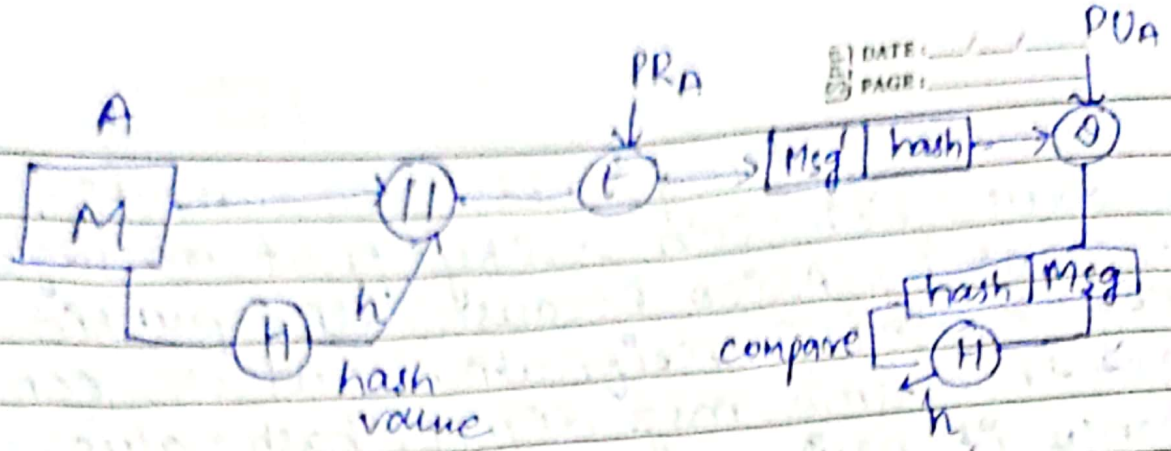
→ use for msg authentication & non-repudiation & msg integrity

→ not used for confidentiality.



→ also provides message integrity because if message changed then at receiver side, we will not get exact message achieved using hashing concept using msg digest & hash value.

Good work



general concept of digital signature

Note → The signature use some info unique to the sender to prevent both forgery and denial of service.

Sender sends two document → msg & signature.

It must be easy to produce digital signature.

It must be easy to verify & regconize.

we need (i) key generation algo → to generate private key.

(ii) signing algo i/p → M and private key
o/p digital signature.

(iii) verifying algo → using public key and sign.

we are getting message authentication because bob can verify that message is sent by Alice because alice public key is used in verification and we can get the same msg digest / hash value only if private key of Alice is used Therefore authenticity achieved.

message Integrity

If the message is changed between anyhow then, receiver will not get the same hash value / msg digest so if hash value / msg digest not same then message changed.

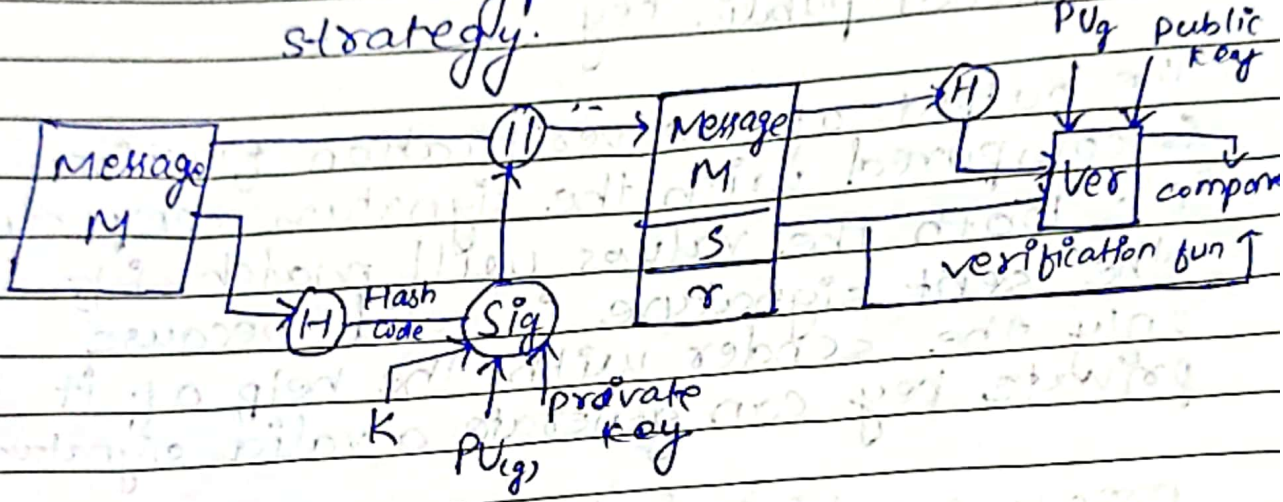
∴ Hash function helps in preserving the integrity of message

Non-repudiation:-
achieved by using a trusted 3rd party.

Digital signature standard (DSS)

It is a federal information processing standard (FIPS) which defines algorithms that are used to generate digital signature with the help of (SHA) for authentication of electronic document.

provides digital signature algorithm no encryption or key exchange strategy.



Sender side

hash code is generated out of message and following inputs are given to the signature function.

1) The hash code
2) random number 'k' generated for particular number
3) The private key of sender $PR_{(a)}$
4) global public key i.e $PU_{(g)}$

These input to the function will provide us with the output signature containing two components - 's' and 'r'. Therefore, the original message concatenated with signatu

Good Write

DATE: __/__/____
PAGE: _____

Receiver side

At the receiver end, verification of the sender is done. There is a verification function which takes the following inputs

1) The hash code generated by the receiver
2) signature components 's' & 'r'.
3) Public key of sender.
4) Global public key.

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

~~proof of digital signature Algorithm~~

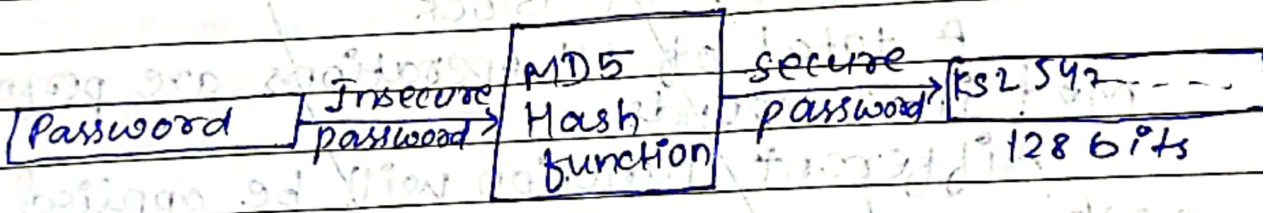
Downloaded doc for it.

MD5
Message digest Algorithm

- developed by Rivest
- Fast and produces 128 bit message digests

Its a hashing algorithm, is one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

Use of MD5
- used for file authentication
- used for security purpose in a web application.
- can store our password in 128 bits format



Working of the MD5 algorithm

1) Append Padding bits
We add padding bits in the original message in such a way that:

length (original message + padding bits) = 512*i - 64

Good Write

2) Append Length Bits!
We add the length bit in output of first step.

output of 1st step = 512 * n - 64
length bits = 64
After adding both we will get 512 * n i.e the exact multiple of 512.

3) Initialize MD buffer:-
Here we use 4 bit buffer i.e J, K, L and M. The size of each buffer is 82 bits.

- A = 0x67425301
- B = 0xEDFCBA45
- C = 0x98CBADFE
- D = 0x13DCE476

4) Process Each 512-bit Block
A total of 64 operations are performed in 4 rounds
Different function will be applied on each rounds

f(K, L, M) = (K and L) OR (NOT K AND M)
G(K, L, M) = (K AND L) OR (NOT L AND M)
H(K, L, M) = K XOR L XOR M
I(K, L, M) = L XOR (K OR NOT M)

In each bit position, f act as conditional If K then L else M. The function f can have been represented using + instead of v since

Good Write

Difference between digital signature & certificate.
Difference between SHA and MD5

DATE: / /
PAGE:

K L and not K(M) will never have 1's in the similar bit position.

Step 5 Output

The message digest created an output including A, B, C, D. The output from the final round is the 128-bit hash result or message digest it can acquired after it can have incrementally processed all t 512-bit block of the message.

Secure Hash function

invented by national security agency. in 1993.

SHA introduced a new process which develop the 16-word message block input to the compression function to an 80-word block between other things.

Algo:-

Step 1: Append padding bits:

The original message is padded and its duration is congruent to 448 mod 512 padding includes a single 1 followed by essential numbers of zeros.

Step 2: Append length

64 bit blocks is added to original length of message to make complete length equal to multiple of 512

Good Work

Step 3: Initialize buffer
buffer includes 5 registers of 32 bits each. They are initialized as,

A = 67 45 23 01
B = ef cd ab 89
C = 98 ba dc fe
D = 10 32 54 76
E = c3 d2 e1 f0

Same as MD5, but is SHA, these values are saved in big-endian format which defines that most essential byte of the word is located in the low-address byte position.

step 4 :- Process message in 512-bit block
The compression function is divided into 20 sequential steps includeds four rounds of processing, where each round is made up of 20 steps.

The four rounds are structurally same as one another with the only difference that each round need a differenent Boolean function which it can define as, f_1, f_2, f_3, f_4 and one of the four multiple additive constants k_t ($0 \leq t \leq 79$) which is based on the step under consideration.

Output :-
After processing the final 512 bit message block t (considering that the message is divided into t 512-block), and it can obtain 160-bit message digest.

Good Write

Message Authentication and Hash function:-

Authentication Requirment

- Revelation
- Analysis of Traffic
- Deception
- Modification in the content
- Modification in the sequence
- Modification in the timings
- Source Refusal
- Destination refusal

Message Authentication function:
Based on two functionality level

- Lower Level
  there is a need for a function that produces an authenticator, which is the value that will further help in athentication of messages.

- higher level
  Lower level funtion is used in order to help receivers verify the authenaity of messages.

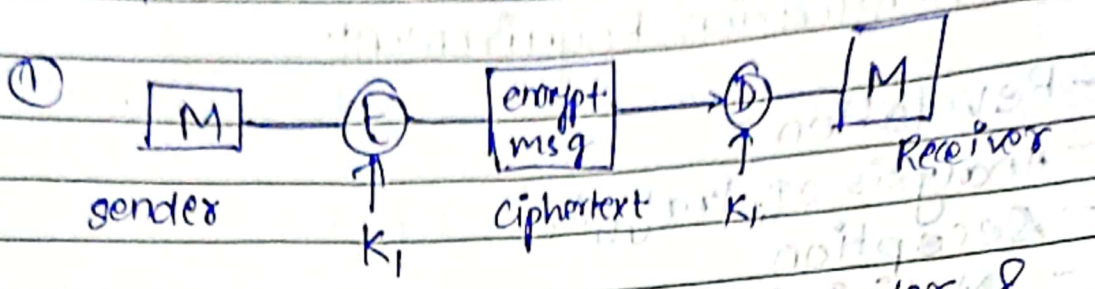
An authenticator must be there to authenticate the message.

Types of authentication function

I) Message encryption
II) Message Authentication Code
III) Hash function

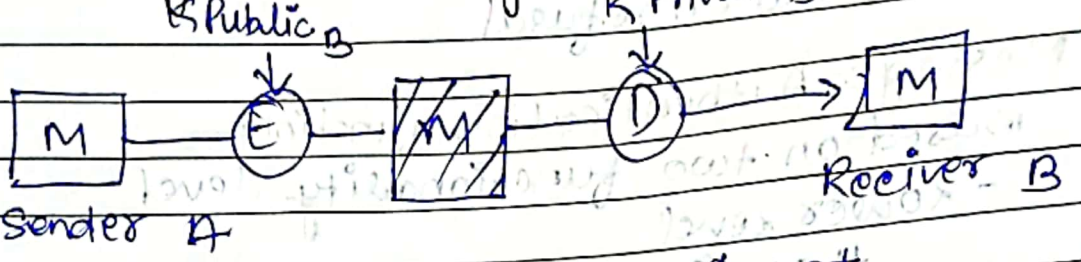
DATE: __/__/____
PAGE: _____

(1) Message encryption:-
ciphertext act as authenticator

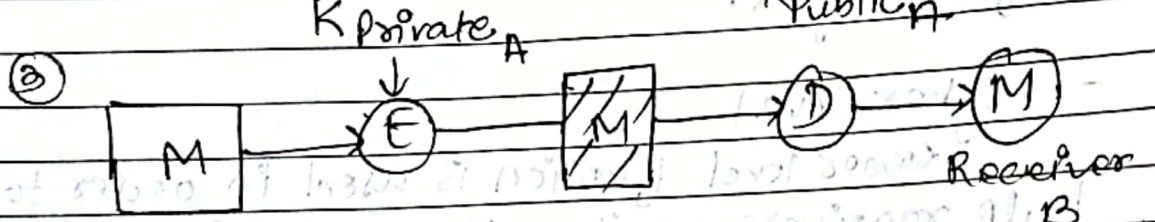


key K_1 share between sender & receiver.

(2) for asymetric encryption.

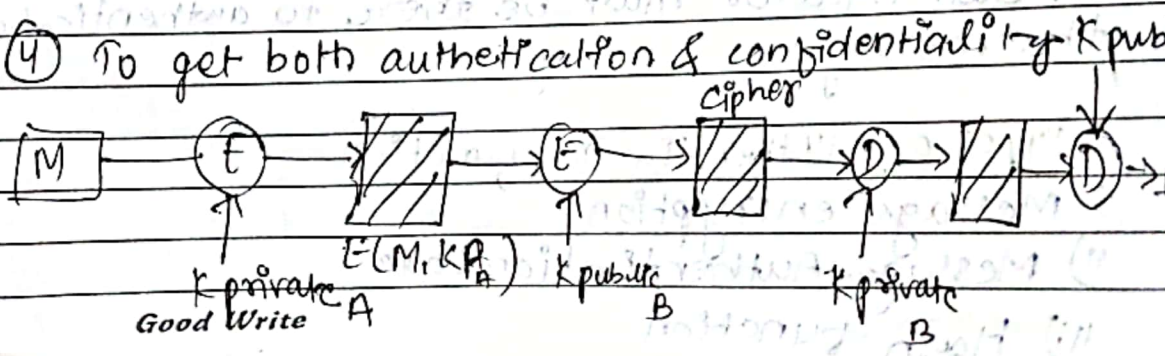


Authentication is not
Confidentiality yes.



Authentication yes
Confidentiality No

(4) To get both authetication & confidentiality



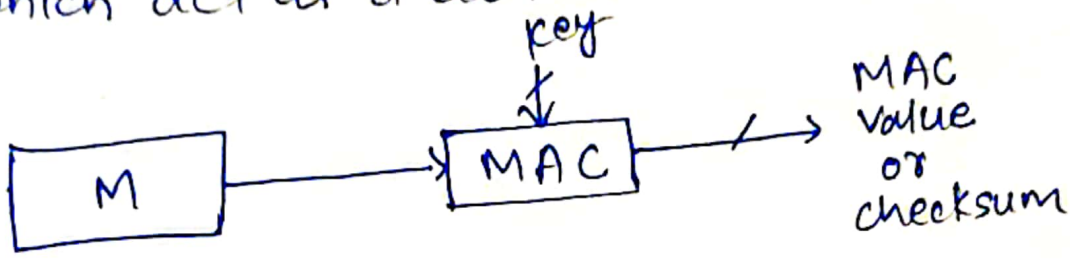
- Message athentication code

ciphertext + key = MAC.

We will have some authentication function and we apply them on plain text along with the key which produce a fixed length code called MAC

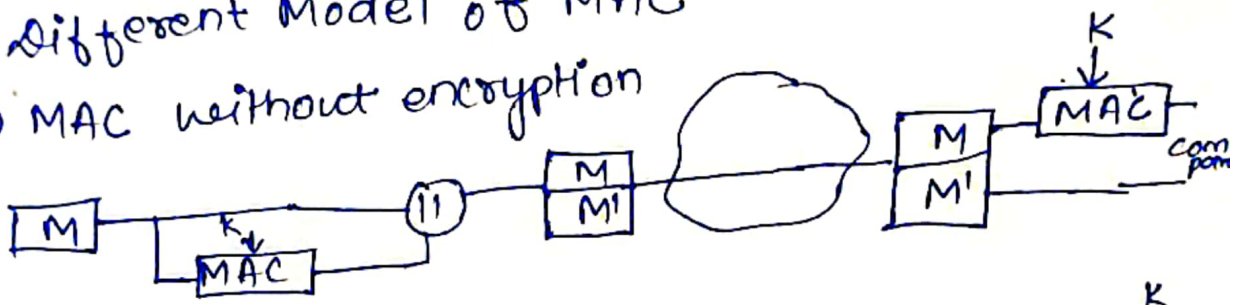
C (M, K) = fixed length code

which act as a authenticator here.

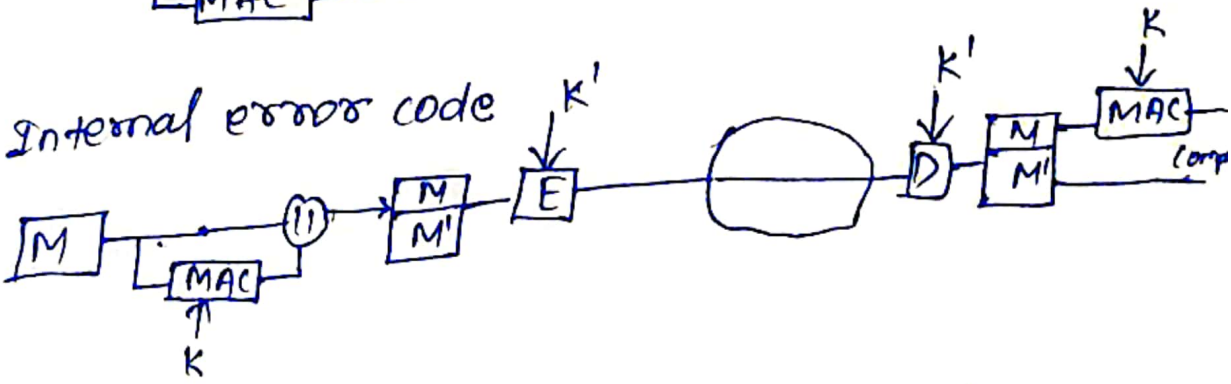


Different Model of MAC

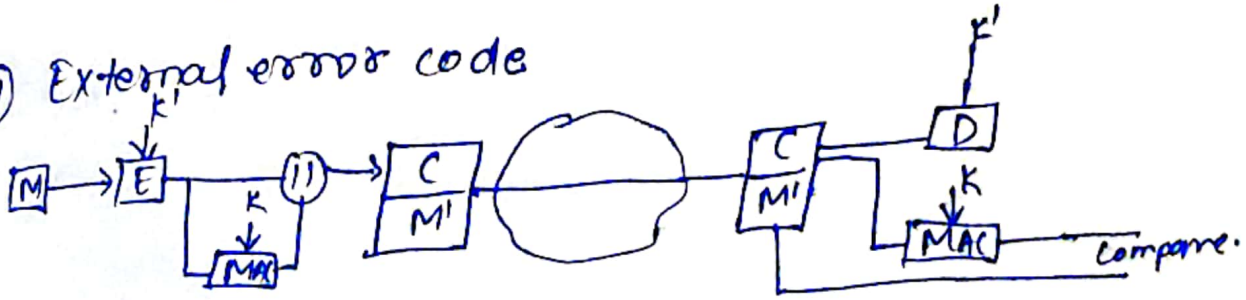
i) MAC without encryption



ii) Internal error code



iii) External error code



(iii) Hash function

→ similar to MAC (Message authentication code) but it doesnot use a key.

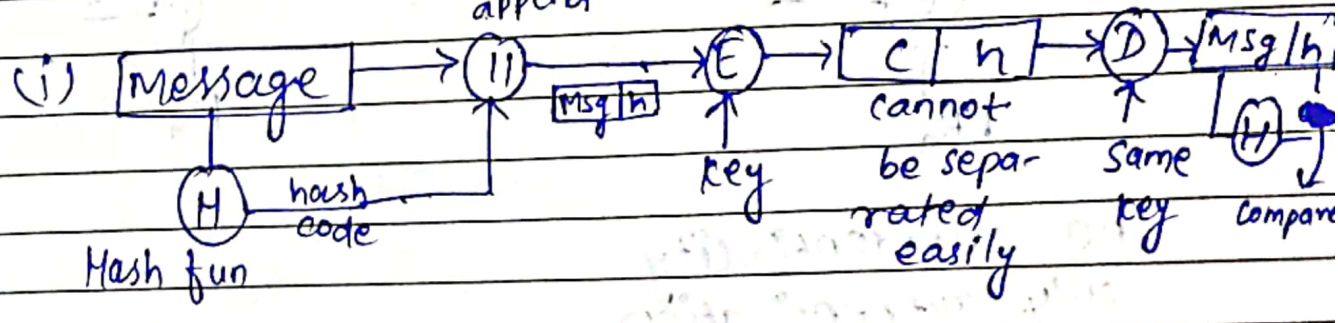
→ Takes in variable size message and produce a fixed output
caued Hash code / Hash value / message digest

→ The only input is message

→ A hash value 'h' is generated by function H
as,
$H(M) = h$
↑ ↑
variable length message. fixed length code 'h'

They are also called as compression function.
There are different methods to provide authentication in different situation

(i)

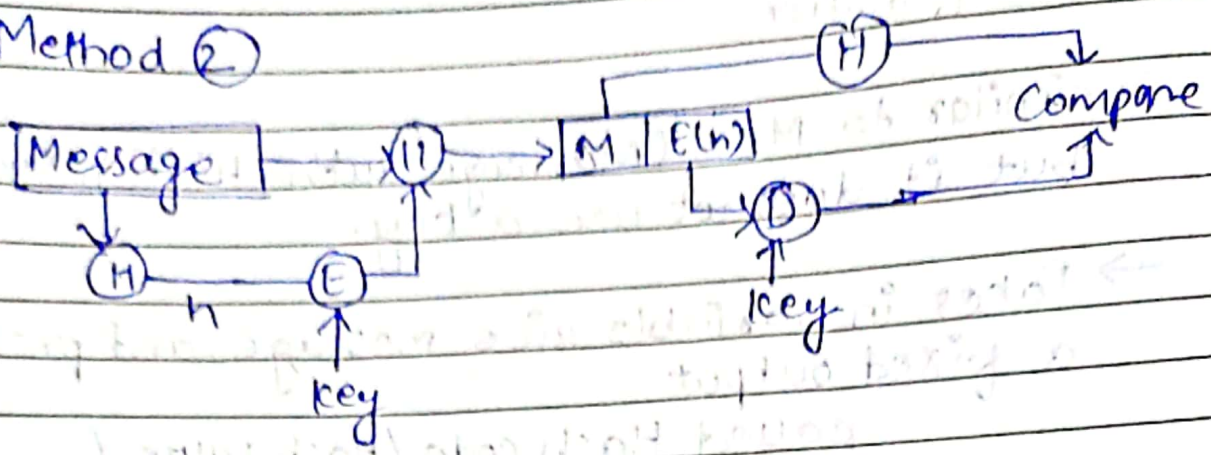


authentication + confidentiality maintained because msg was encrypted before sending

if both hashcodes equal in the end because only A & B share the secrete key

Good Write

Method (2)

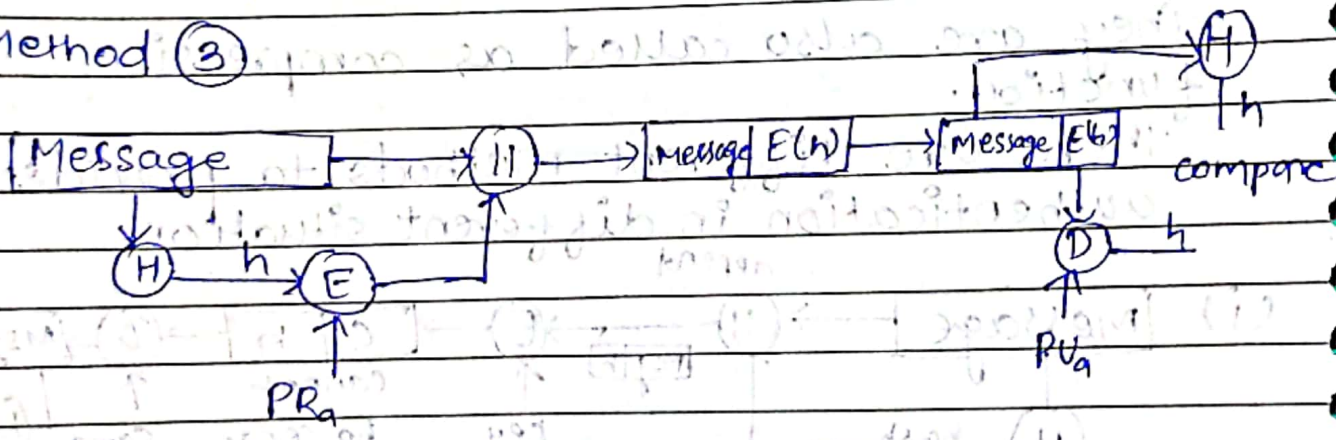


only authenticity
not confidentiality

because only hash code is encrypted not the message as whole.

we can use this method if the message is not private, because it will take less processing time since we are not encrypting message.

Method (3)

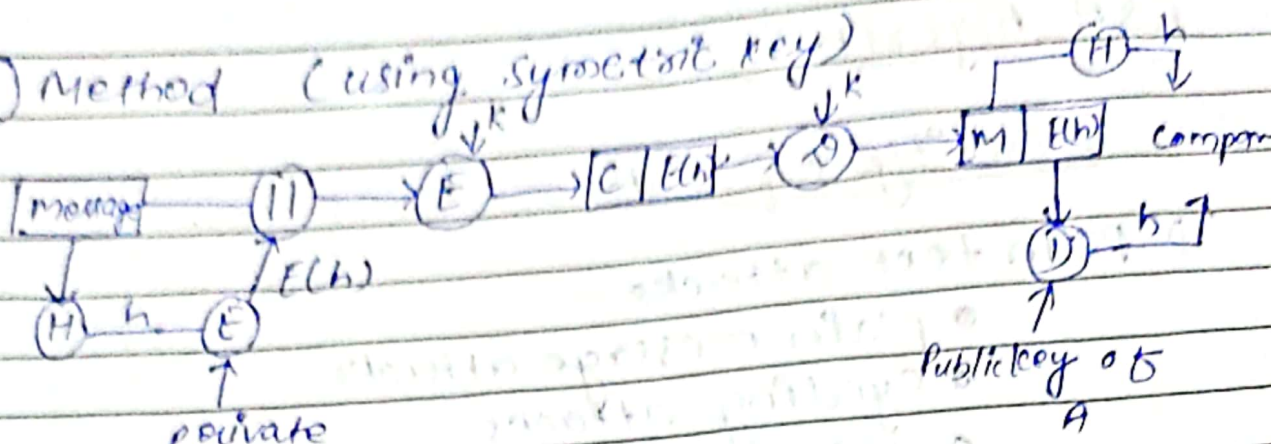


no confidentiality
only authentication

processing time will be less as the message is not encrypted.

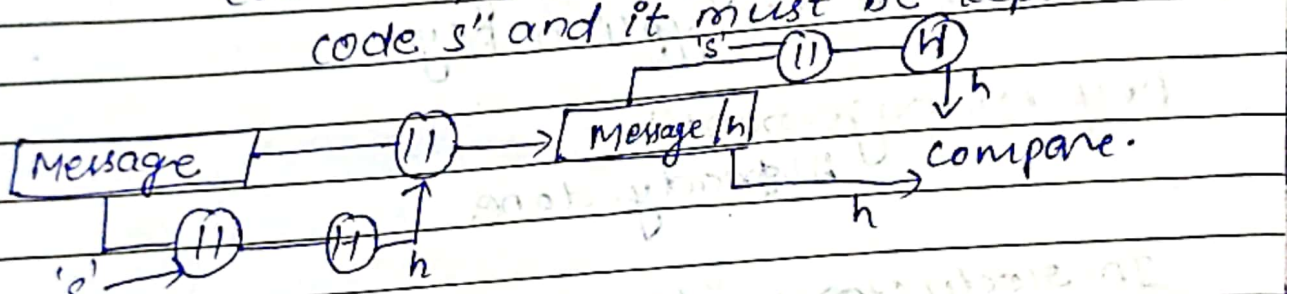
Good Write

(4) Method (using symmetric key)



Method-5

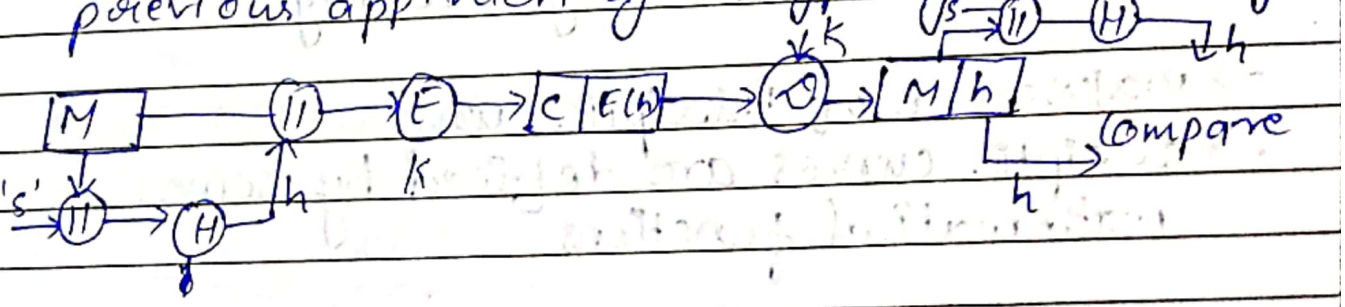
(sender & receiver will have a secret code 's' and it must be kept secret



No ~~confidentiality~~ confidentiality (we get in method 6)
only authentication.

Method-6

confidentiality can be added to the previous approach by encrypting the message



Good Write

DATE: __/__/____
PAGE: _____

RSA Algorithm

Security of RSA

1) Plain text attacks
   - plain message attacks
   - cycling attacks
   - Unconcealed Message attack

2) Chose cipher attack
3) Factorization attack
4) Attack on Encryption key
5) Attack on decryption key

Key management:
Already done

Introductory idea of Elliptic curve coyptography:-

→ It is asymmetric / public key ecosystem.
→ It provides equal security with smaller key size (eg:- as compared to RSA)

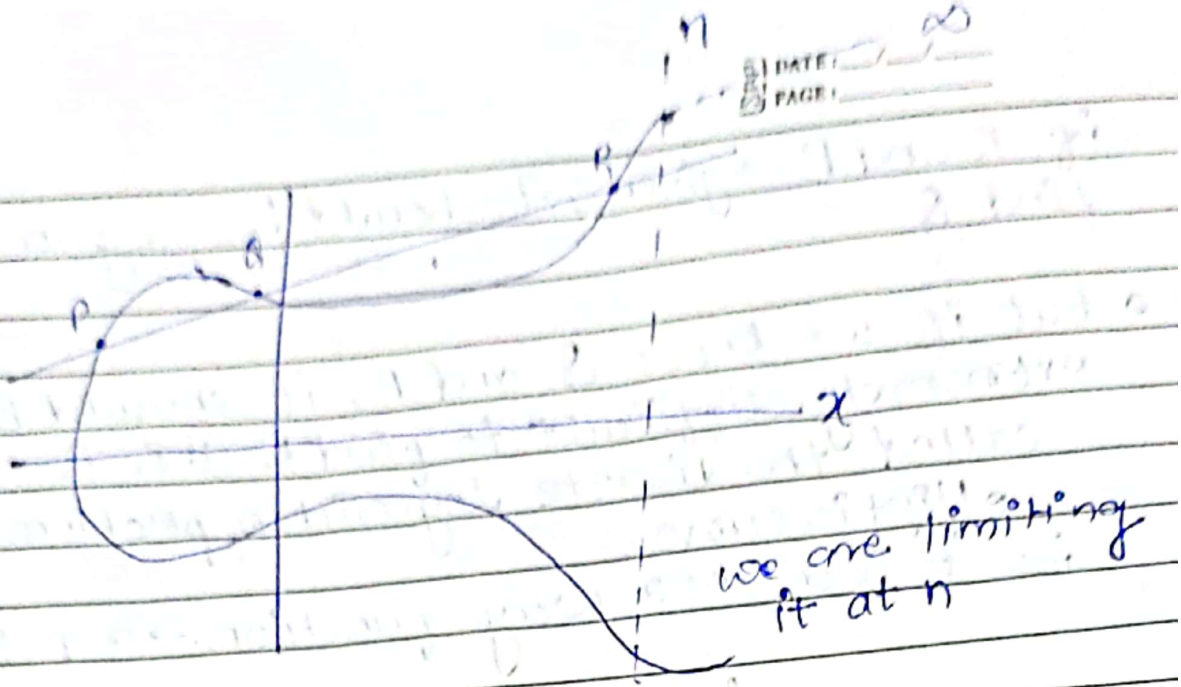
small size + high security

→ makes use of Elliptic curve
→ Elliptic curves are defined by some mathematical functions

eg $y^2 = x^3 + ax + b$

equation of degree 3

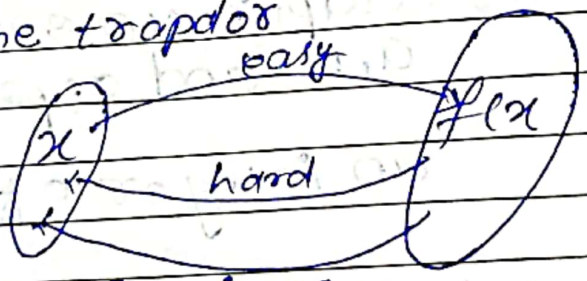
Good Write



→ symmetric to x-axis

→ If we draw a line, it will touch a max of 3 points.

A Trapdor function is a function that is easy to compute in one direction, yet difficult to compute in opposite direction (finding its inverse) without special info called the trapdor



- Let $E_p(a,b)$ be the elliptic curve
- Consider the equation $Q = kP$
  where $Q, P \rightarrow$ points on curve and $k < n$

if K and P → given, it should be easy to find Q

- but if we know Q and P, it should be extremely difficult to find K. This is called the discrete logarithm problem for elliptic curve.

ie it is a one way function. → trap fun

A → B easy to compute
B → A very difficult.

Algo is somewhat same to Deffie Hellman

ECC key exchange

Global public elements.

Eq(a, b): elliptic curve with parameters a, b and q (prime no or an integer of form 2^m)

G: point on the curve whose order is larger value of n.

User A key generation

Select private key n_A, $n_A < n$

calculate Public key $P_A = n_A \times G$

DATE: __/__/____
PAGE: _____

User B key generation:

select private key n_B : $n_B < n$

calculate public key $P_B = n_B \times G$

calculation of secrete key by user A

$$K_A = n_A \times P_B$$

calculation of seccrete key by user B

$$K_B = n_B \times P_A$$

Here secrete key has been exchanged.

ECC encryption

Let the message be M

- First encode this message M into a point on elliptic curve.
- Let this point be P_m

↓

Now this point is encrypted

for encryption, chose a random positive integer K

The cipher text will be

$$Cm = \{ kG, P_m + kP_B \}$$

↗ for encryption private key of B used

DATE: / /
PAGE:

This point is sent to the receiver.

Decryption

for decryption, multiply 1st point in the pair with receiver's secrete key.

i.e $KG * n_B$ // for decryption private key of B is used.

Then subtract it from 2nd point / coordinate in the pair

i.e $P_m + KP_B - (KG * n_B)$

but we know $P_B = n_B \times G$

so,

$P_m + KP_B - KP_B$

$= P_m$ (original point)

So, receiver gets the same point.
Now, after decoding it the receiver will get the message.

DATE: / /
PAGE:

Elgamal Encryption

- is a public key cryptosystem (asymmetric key concept is used)

→ This cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}

Idea of Elgamal encryption decryption.

suppose Alice wants to communicate with Bob

1. Bob generate public and private keys:

- Bob chooses a very large number q and a cyclic group f_q.
- From the cyclic group f_q, he chooses any element g and an element 'a' such that $gcd(a, q) = 1$.
- Then he computes $h = g^a$
- Bob publishes f, $h = g^a$, q and g as his public key and retains a as a private key.

DATE: / /
PAGE:

Elgamal Encryption

- is a public key cryptosystem (asymmetric key concept is used)

→ This cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}

Idea of Elgamal encryption decryption.

Suppose Alice wants to communicate with Bob

1. Bob generate public and private keys:

- Bob chooses a very large number q and a cyclic group fq.
- From the cyclic group fq, he chooses any element g and an element 'a' such that gcd (a, q) = 1
- Then he computes $h = g^a$
- Bob publishes f, $h = g^a$, q and g as his public key and retains a as a private key.

DATE: __/__/____
PAGE: _____

2. Alice encrypts data using Bob's public key

- ~~Alice encrypts data~~
- Alice selects an elements k from cyclic group f.

  $\therefore gcd(k, q) = 1$
- Then, compute.

  $P = g^k$ and $s = h^k = g^{ak}$
- Mutiplies with

  $s * M$
- Then she sends $(p, M*s)$

  $= (g^k, M*s)$

3. Bob decrypt the message

- Bob calculate $s' = p^a = g^{ak}$
- He devides $M*s'$ by s' to obtain M as $s' = s$

Good Write

B Unit

DATE: / /
PAGE:

Introduction to group, ring and field

Group:-

A group is a set G which is CLOSED under an operation * and satisfies the given ~~Expect~~ or following properties

1) A_1 - closure $a, b \in G$, then $(a * b) \in G$
2) A_2 - Associative $a*(b*c) = (a*b)*c$ for all $a, b, c \in G$
3) A_3 - Identity $(a*e) = (e*a)$ for $a, e \in G$
4) Inverse element $(a*a') = (a'*a) = e$ for all $a, a' \in G$

The group is said to be Albelian group if it satisfies

A5 - commutative $(a*b) = (b*a)$ for all $a, b \in G$

Rigs

A ring 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

* Group (A1-A4), Abelian Group (A5) under addition.

Good Write

DATE: __/__/____
PAGE: _____

(2) Associative of multiplication (X)

for every $a, b, c \in R$

$a * (b * c) = (a * b) * c$

(3) Distributive properties

$a(b+c) = ab + ac$ for all $a, b, c \in R$.

or, $(a+b)c = ac + bc$ "

(4) closure property.

for all $a, b \in R$

$a * b$ also belong to R.

Note

commutative Ring

A ring is said to be commutative if it satisfies additional conditions

commutativity of Multiplication

(My) : $ab = ba$, for all $a, b \in R$

Field

A field is a set F which is closed under two operation + and * such that

1) F is an abelian group under '+'

2) $F - \{0\}$ (the set F without the additive identy 0) is an abelian group under X.

Good Write

Prime Numbers:

If N is a prime number then the division are 1 and N.

A prime number is a number greater than 1 with only two factors - itself and one.

Why we use prime Numbers in Cryptography

- Used by many encryption algo.
- Very fast multiplication
- Extremly computer-intensive to do reverse.
- factoring very large prime numbers is very hard i.e take computers a long time.

Relative Prime Number

Two prime numbers are said to be relatively prime, if they have no prime factor in common and their only common factor is 1.

if gcd (a, b) = 1

so, a, b are co-prime

DATE : __/__/____
PAGE : _____

Modular Arithematic

① Mod

$7 \bmod 4 = 3$

② $-x \bmod y = y - (x \bmod y)$

$-11 \bmod 7 = 7 - (11 \bmod 7)$

$= 7 - 4$

$= 3$

if $x \bmod y = 0$, then this formula fails.

* Congruent Modulo

Two integers a and b are said to be congruent modulo n if

$(a \bmod n) \equiv (b \bmod n)$

eg:- $73 \equiv (4 \bmod 23)$ means.

$73 \bmod 23 = 4 \bmod 23$

properties of congruency

(i) $a \equiv b \pmod n$ if $n/(a-b)$

(ii) $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

(iii) if $a \equiv b \pmod n$ & $b \equiv c \pmod n$

then $a \equiv c \pmod n$

Good Write

Modular arithmetic operations / properties

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

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

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

eg:- Let $a=11$, $b=15$, $n=8$

$(11 \times 15) \bmod 8 = (3 \times 7) \bmod 8$

$5 = 5$

Note

Exponentiation is performed by repeated multiplication, as in ordinary arithmetic

given

$11^7 \bmod 13$

to find it we will process ca-

DATE: __/__/____
PAGE: _____

$11^2 = 121 \equiv 4 \mod 13 = 4$

$11^4 = (11^2)^2 \equiv 4^2 \mod 13 = 3$

$= 3$

$11^7 = 11 \times 4 \times 3$

$= 132 \mod 13$

$= 2$

(4) if $x \equiv y \mod n$ $\quad a \equiv b \mod n$

$(x+a) \equiv (y+b) \mod n$

$17 \equiv 4 \mod 13$, $42 \equiv 3 \mod 13$

$59 \equiv 7 \mod 13$ which is true.

(5) if $x \equiv y \pmod n$ and $a \equiv b \mod n$ then

$(x-a) \equiv (y-b) \mod n$

Fermat's and Euler's theorem

Euler's theorem ($\phi(n)$)

Euler's toilient of n is defined as the no. of the integers less than n that are co-prime to n.

Now

when $n \rightarrow$ prime

$(\phi) = n-1$

Also,

$\phi(a*b) = \phi(a) * \phi(b)$ // a and b should be co-prime

eg $\phi(35) = \phi(7) * \phi(5)$

$= 6 \times 4 = 24$

Eulers theorem is also called as fermat-Eulers theorem or Euler's theorem

Euler's theorem state that if x and n are co-prime positive integers, then

$x^{\phi(n)} \equiv 1 \bmod n$ / $x^{\phi(n)} \bmod n = 1 \bmod$

where $\phi(n) \rightarrow$ eulers toilient function

DATE: __/__/____
PAGE: _____

* This is a generalized version of fermat's theorem.

Let $x = 11$, $n = 10$ both are co-prime

we can represent

$$11^{\phi(10)} = 1 \bmod 10$$

$$11^4 = 1 \bmod 10$$

$$\phi(10) = \phi(5) \times \phi(2)$$
$$= 4 \times 1$$
$$= 4$$

$14641 \equiv 1 \bmod 10$ which is true

~~$n \bmod 10 = 1 \bmod 10$~~

Note:

$$x^{\phi(n) \cdot a} = 1 \bmod n$$

a = any multiple of $\phi(n)$ it will give the same result.

Fermat's theorem

→ special case of euler's theorem.

If n is prime and n is a positive integer, not divisible.

$$x^{n-1} = 1 \bmod n$$

n → prime number
x → is not divisible by n

eg $x = 3, \quad n = 5$

$$x^{n-1} = 1 \bmod n$$

$$3^{5-1} = 1 \bmod 5$$

$$3^4 = 1 \bmod 5$$

$$81 = 1 \bmod 5$$

Another form of Fermat's theorem.

$$x^n = x \bmod n$$

$x = 3, \quad n = 5$

$$3^5 = 3 \bmod 5$$

$$243 \equiv 3$$

$$243 \bmod 5 = 3 \bmod 5$$

$$2 = 2$$

proved.

Good Write

DATE: __/__/____
PAGE: _____

Euclidean / Eludian Algorithm
used to find gcd of two positive integers (basically large numbers)

$$gcd(a,b) = gcd(b, a \bmod b)$$
$$gcd(a,0) = a$$

gcd(a, b)
a = 1025
b = 35

gcd(1025, 35)
= gcd(35, 1025 mod 35)
= gcd(35, 10)
= gcd(10, 35 mod 10)
= gcd(10, 5)
= gcd(5, 10 mod 5)
= gcd(5, 0)
= 5

Good Write

example 2:

$$\gcd(11,7) = \gcd(a,b)$$
$$= \gcd(7, 11 \bmod 7)$$
$$= \gcd(7, 4)$$
$$= \gcd(4, 7 \bmod 4)$$
$$= \gcd(4, 3)$$
$$= \gcd(3, 4 \bmod 3)$$
$$= \gcd(3, 1)$$
$$= \gcd(1, 3 \bmod 1)$$
$$= \gcd(1, 0)$$
$$= 1$$

Therefore they are co-prime, mutally relative or relative prime.

DATE: / /
PAGE:

Chinese Remainder Theorem

Chinese Reminder theorem states that there always exist an 'x' that satisfies the given convergence.

$x \equiv rem[0] \pmod{num[0]}$

$x \equiv rem[1] \pmod{num[1]}$

---and (num[0]; num[1] ---. num[m-1]) must be co-prime to one another

Algorithm

if $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

(i) $gcd(m_1, m_2) = gcd(m_2, m_3) = gcd(m_1, m_3) = 1$

(m_1 m_2 4m_3) All should be co-prime.

(ii) $x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 +$

$--- M_n X_n a_n) \bmod M$

$M = m_1 * m_2 * m_3 - --. m_n$

Good Write

$M_i = M/m_i$ eg:- $M_1 = M/m_1$

$= \frac{m_1 m_2 m_3}{m_1}$

$= m_2 m_3$

$M_1 = m_2 m_3$

$M_2 = m_1 m_3$

$M_3 = m_1 m_2$

To calculate x_i

$M_i x_i \equiv 1 \bmod m_i$

↳ multiplicative inverse of M_i

$\therefore M_1 x_1 \equiv 1 \bmod m_1$

example

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 3 \pmod{11}$

we can find the value of x as,

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$

Here, from question,

$a_1 = 1$ $\quad m_1 = 5$

$a_2 = 1$ $\quad m_2 = 7$ } co-primes

$a_3 = 3$ $\quad m_3 = 11$

Good Write

DATE: __/__/____
PAGE: _____

Using chines remainder theorem;

$M_1 = m_2 m_3$

$= 7 \times 11 = 77$

$M_2 = m_1 \times m_3$

$= 5 \times 11 = 55$

$M_3 = m_1 \times m_2$

$= 7 \times 5 = 35$

$M = m_1 \times m_2 \times m_3 = 7 \times 11 \times 5 = 385$

Now, we will calculate X_i value.

for X_1

$M_1 X_1 \equiv 1 \pmod{m_1}$

$77 X_1 = 1 \pmod 5$

or, $M_1 X_1 \pmod{m_1} = 1$

$77 X_1 \pmod 5 = 1$

$2 X_1 \pmod 5 = 1$

putting $X_1 = 3$

$6 \bmod 5 = 1$

$\therefore X_1 = 3$

Good Write

Similarly,

$M_2 X_2 \pmod{m_2} = 1$

$55 X_2 \pmod 7 = 1$

$6 X_2 \pmod 7 = 1$

When we put $X_2 = 6$

then,

$6 \times 6 \pmod 7 = 1$ true

$\therefore X_2 = 6$

Also,

$M_3 X_3 \pmod{m_3} = 1$

$35 X_3 \pmod{11} = 1$

$2 X_3 \pmod{11} = 1$

$X_3 = 6$

$\therefore 12 \pmod{11} = 1$

Now,

$x = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 9) \bmod 385$

$= 1191 \bmod 385$

$= 36$

Good Write

DATE: __/__/____
PAGE: _____

discrete logarithms

5^x Mod 17 = equally distributed.

If x is given then $5^x \bmod 17$ is easy to calculate but if

$5^x \bmod 17 = 12$ is given and we are asked to compute x, then its tough to do so.

Its easy on one way but difficult in reverse way.

if we are going to compute

$g^x \bmod p$

$2^x \bmod 7 = 4$, $x = 2, 5$ etc

here g is the primitive root of prime number p. and x can be any number

For smaller value of p is may be easy to find x

* If p is very large then find x will be hard.

* time & effort will be more to find it.

* Srength of one way ful & how much time it takes to break it.

Good Write

DATE: / /
PAGE:

Numerical

Solve $\log_2 9 \bmod 11$

Here $p = 11$, $g = 2$, $X = 9$

$\log_g X \equiv n \pmod p$

$X \equiv g^n \pmod p$

$9 \equiv 2^n \pmod{11}$

Try $n = 1, 2, 3, 3 \ldots$

when $n = 6$

then,

$9 \equiv n^6 \pmod{11}$ true.

$2^x \pmod 7 = 4$

$x = 2, 4$ then solved.

Good Write

DATE : __/__/____
PAGE : _____

* Principals of public key cryptosystem

The approach of public key cryptosystem derivative from an attempt to attacks two of the most complex problem related to symmetric encryption:

i) key distribution

The two basic principals of any crypto-system

I) confidentiality.

II) Authenticity.

problem associated with confidentiality problems associated with authentication.