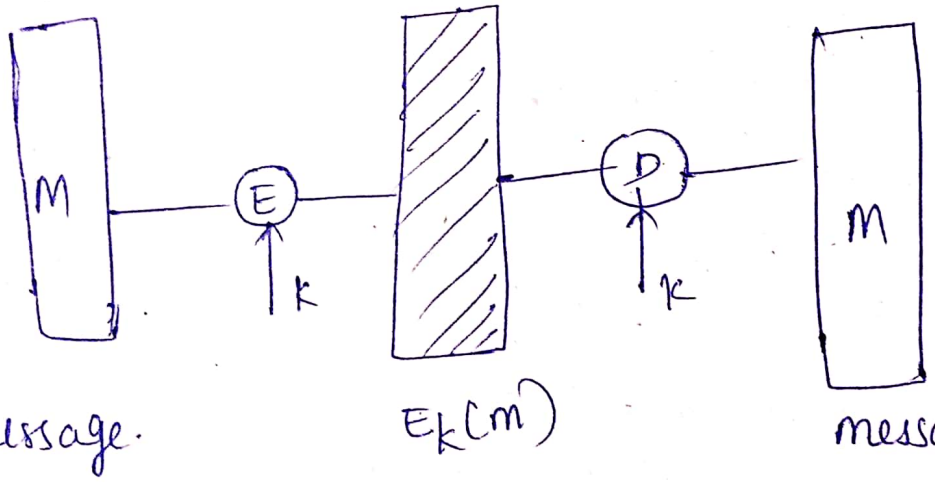
* Key

- Sender A generate the key & inform to Receiver
- Receiver may generate & inform to sender
- Trusted third party may generate a key & distribute them.
- Use Previous key

* Message Authentication * 26/08/2019

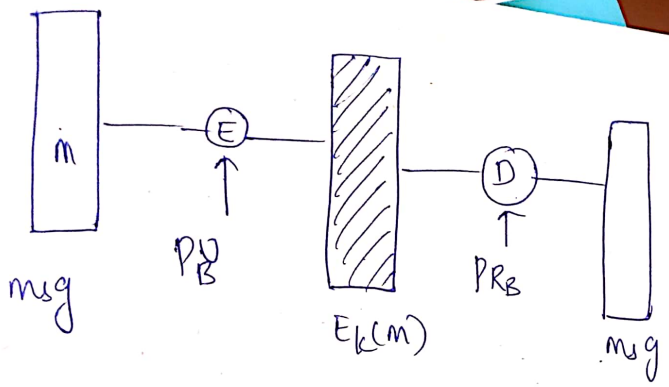
1) Private Key msg Authentication:-



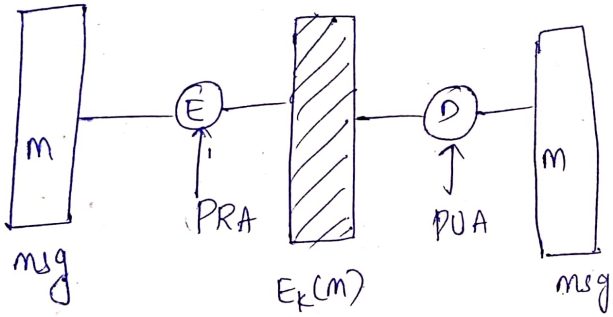
It Provides confidentiality services.

2) Public Key Encryption msg Authentification

Private key only known by concerned ends.

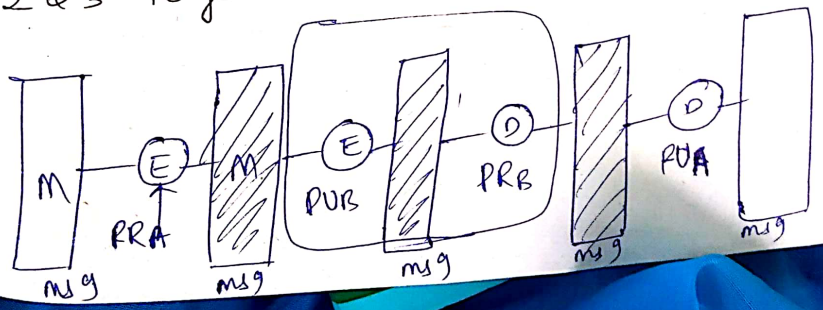


3) Authentication service:-



We have to prove only authorized Person can send the data. Its done by Using Private Key of A.

2 & 3 together:-



It Provides both Confidentiality & Authentication for transmittion data.

28/8/19

* SHA-1 :-

- Ilp msg $< 2^{64}$ bits
  Processed in 512 bit blocks
- olp 160 bit digest

It provides fixed length n.

	1 bit	2 bit	----	n bit
Block 1	⊕			
B_2	1 bit			
:	⊕			
Bm				
	1 bit			

Total n bits

* Advantages in One way Hash Function :-

→ Accepts variable size msg.

* msg
gene
Sha
- co

1) Ty

Public
into

1)
2)
3) -

* msg Authentication code:-

generate authentication code based on shared key & msg.

- common key is shared blw A & B.

1) Types of Attacks in secure hash fun?

Public key cryptographic algo is categorized into 3 types based on .ei

1) Encryption & Decryption
2) Digital signature
3) - key exchange.

* RSA Algorithm :- (57)

→ Key Generation :-

Select p, q p & q both Prime

Clt $n = p \times q$

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

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

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

Publickey $KU = \{e, n\}$

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

→ Encryption :-

Plaintext : $m < n$

ciphertext : $C = m^e \pmod n$ is

→ Decryption :-

ciphertext : C

Plaintext : $m = C^d \pmod n$

29/08/2019

* Ex:- Key generation :-

Select P, Q

P = 17, Q = 11

Cl+ n = 187

$\phi(n) = 160$ // $\phi(n) = (P-1)(Q-1)$

Select e, gcd($\phi(n)$, e) = 1

gcd (160, 7) = 1

Cl+ d,

$de = 1 \bmod \phi(n)$

$d \times 7 = 1 \bmod 160$

$d = 23$

$KPu\ (Pubk) = \{e, n\} = (7, 187)$

$KR = (d, n) = (23, 187)$

Encryption :-

select m < n

m = 88

$c = m^e \bmod n$

$= 88^7 \bmod 187$

$= [(88 \bmod 187) \times (88^2 \bmod 187) \times (88^4 \bmod 187)] \bmod 187$

$= 88 \times 77 \times (88^2 \bmod 187 \times 88^2 \bmod 187) \bmod 187$

$= (88 \times 77 \times 132) \bmod 187$

$= \underline{11}$

77 × 4 = 308, 308 + 9 = 317, 317 + 9 = 326, 326 + 3 = 329

187) 894432 (4783
748
1464
1309
1553
1496
572
561
11

187) 21435888 (114630
187
2573
1870
8658
7480
11788
11220
5688
5610
781
748
33

3025 (

* Decryption:-

$C = 11$

$m = c^d \bmod n$

$= 11^{23} \bmod 187$

$(11 \bmod 187)(11^2 \bmod 187)(11^4 \bmod 187)$
$(11^8 \bmod 187)(11^{16} \bmod 187)$ ~~$(11 \bmod 187)$~~

33 · 121 · 55

15 16 23

3025 (187

Global
Prin
$\alpha < q$
Prin

User B
Select
$x_B <$ q
$Y_B \cdot$

3

$11 \times 121 \times (121 \times 121 \bmod 187)$

```
187) 14641 (78
     1309
     ----
      1551
      1496
      ----
        55
```

$11 \times 121 \times 55$

$= 88$

*

Global Public Element q

Prime Number α

$\alpha < q$ and α a

Primitive root of "q".

1

User A key generation select private X_A

$X_A < q$ clt Y_A

3

$Y_A = \alpha^{X_A} \bmod q$

$= 3$

2

User B key generation

Select Private X_B

$X_B < q$ clt Public

4

$Y_B \cdot Y_B = \alpha^{X_B} \bmod q$

1

3

Generation of secret key by User A

$K = (Y_B)^{X_A} \bmod q$

1

4

Generation of Secret Key by User B

1 $K = (Y_A)^{X_B} \bmod q$.

5

$a^i \bmod n$, $i = 1, 2, \ldots n-1$

$a^1 \bmod n =$

$a^2 \bmod n =$ } results are arranged in ascending order

$\vdots$

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

i.e; $\{1 \ldots\ldots n-1\}$

then we get sequence nbrs

$i=1$ is not a primitive root ~~$i=1$~~ $i=2$ is

Primitive root when $q=5$

$\alpha = 2, q = 5$

$\alpha < q$.

* Elleptic curve cryptography :- * 04/9/19

Step1 :- User A selects a random integer n_A which will become his/her private key & public key which is a point in $Ep(a,b)$ is c/t'd as follows

$$P_A = n_A \times G$$

where G is a generator point in $Ep(a,b)$

Step2 :- User B similarly selects a random integer n_B which will become his/her private key & Public key is given by $P_B = n_B \times G$

Step3 :- User A generates the secret key 'k' as follows: $K = n_A \times P_B$

Step4 :- User B generates the secret key 'k' as follows: $K = n_B \times P_A$

→ To encrypt a msg Pm User A chooses a random positive integer k and produces the cipher text Cm as follows. $Cm = \{kG, Pm + kP_B\}$

→ To decrypt the cipher text Bob uses the following calculations

Find $\Phi(n)$

Find $e^{-1} \pmod{\Phi(n)}$

Find m

* Arbitrated digital Signature:-

a) Conventional encryption, Arbiter sees message.

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

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

b) Conventional encryption, Arbiter does not see msg.

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

2) $A \rightarrow Y: E_{Kay}[ID_X \| E_{Kxy}[M] \| E_{Kxa}[ID_X \| H(E_{Kxy}[M])] \| T]$

c) Public key encryption, Arbiter does not see msg

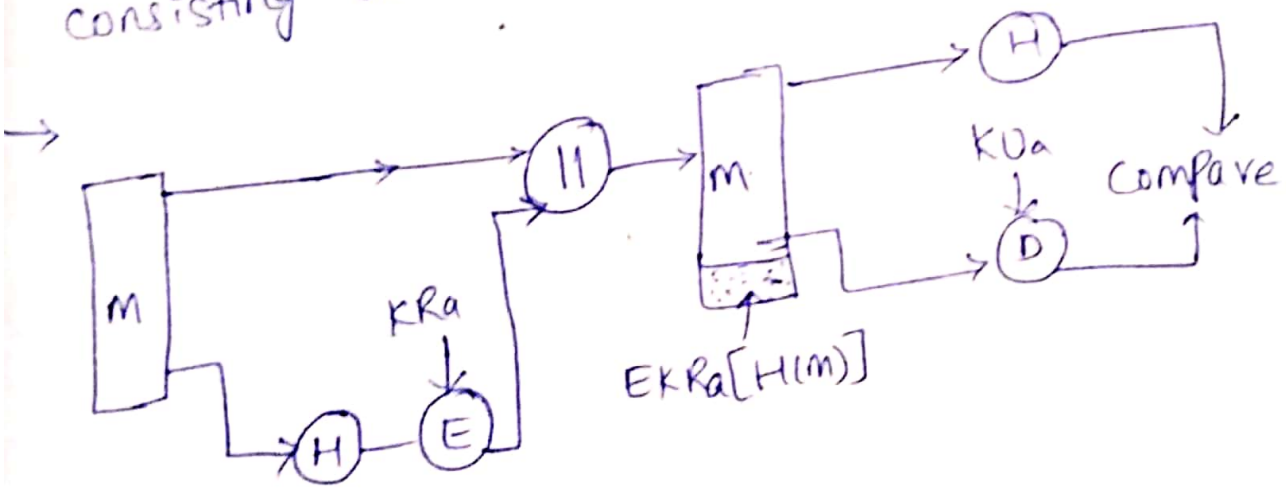
1) $X \rightarrow A: ID_X \| E_{KR_X}[ID_X \| E_{KU_Y}(E_{KR_X}[M])]$

2) $A \rightarrow Y: E_{KR_A}[ID_X \| E_{KU_Y}[E_{KR_X}[M] \| T]]$

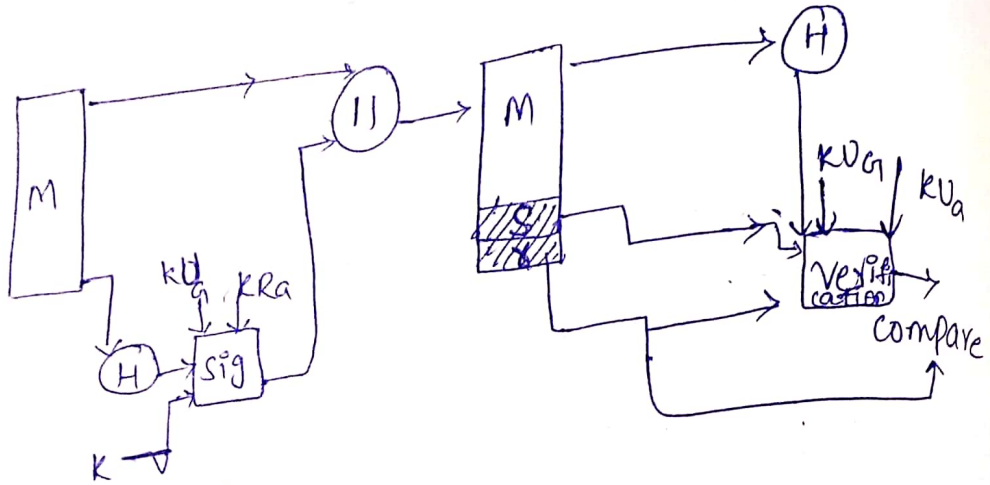
* Digital Signature Standard:-

The DSS approach also make us of hash function. The hash code is provided as i/p to a signature functions along with a random nbr k generated for this particular signature.

→ The signature function also depends on the sender's private key (KR_a) and set of parameters known to a group of communicating principals. So consider this set to constitute a global Public key KU_g. The result is a signature consisting of two components labled s & r.



RSA approach



DSS Approach

6/9/19

* Digital & Certificate:-

To obtain digital certificates an organization must apply to a certificate authority which is responsible for validating, ensuring the authenticity of requesting organization.

→ The certificate will identify the name of the organization a serial nbr, the validity date, the organization public key. where encryption to or from that organization is required.

→ A dc

a like to

authority

developers

→ A dc

entity it

Id card.

→ Dc form

framework

→ This fra

across nlw

it establi

those own

→ A DC is

→ It consists

- The

- The nan

certified

→ A dc is an id that is carried with a bike to validate a signature a certifying authority validates information about the sho developers & then issue them digital certificate.

→ A dc allows unique identification of an entity it is an essentially an electronic Id card. issued by trusted third party.

→ Dc forms part of the Iso Authentication framework also known as x.509 Protocol.

→ This frame work provide for authentication across nlw. A DC serves two purposes. it establishe owners identity & it maky thee owners Public key identity.

→ A DC is issued by a certificate authority.

⇒ It consists of

- The Pub key of a person being certified
- The name & address of the person being certified also known as distinguised name (dn)

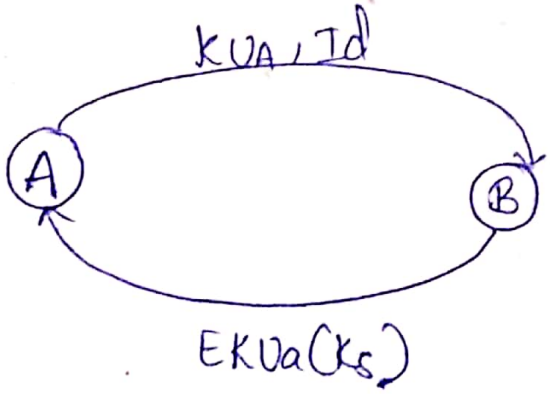
- The digital signature of the CA.
- The Issue date.
- Expiry date

* Public key distributions :- (61)

→ Public Announcement
→ Public Key Directory
→ Public key Authority
→ Certificate Authority.

* Distribution of secret keys using Public key Cryptography :- 6+

1) Simple key distribution :-

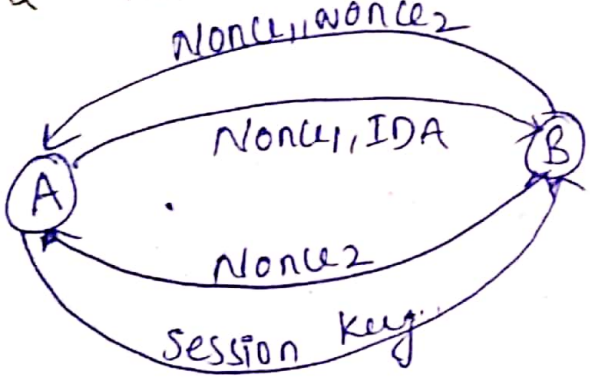


→ It is active attack.

→ While sending KUA, Id other/third party can modify it & send other key its own.

1) A generate temp pair of key
2) Send those to receiver with identity.
3) B Receiver generates the secret key & Encrypt the data
4) Send secret key to A/sender.
5) A encrypt the data.

2) Secret key distribution with confidentiality & Authentication.



1) Encrypt the msg by using Public key of B
i.e, EKUB(Nonce1, IDA) so that it Provides confidentiality.

2) Decrypt the msg only by Receiver
EKUA (Nonce1, Nonce2) = confidentiality.

3) EKUB(Nonce2)

4) $E_{KUB}(E_{KRA}(K_s))$. We provide the authentic by using Private key of A & then provid the confidentiality by using Public key of

5) Decryption at done at B side ie,

$D_{KUA}(O_{KRB}(K_s))$ by using Public key of B and private key of A.

* KERBEROS :- (14) 9/9/19

11/9/19

* More Secure authentication dialouge:-

a) Authentication Servic exchang: to Obtain ticket - granting ticket.

1) $C \rightarrow AS$: Optain $||ID_c||$ Real mc $||ID_{tgs}||$ Timy $||N_1$

2) $AS \rightarrow C$: Real mc $||ID_c||$ Ticket $_{tgs}||E_{Kc}[K_{c,tgs}||$ Times $||$ Nonce $||$ Real mc $||ID_{tgs}]$

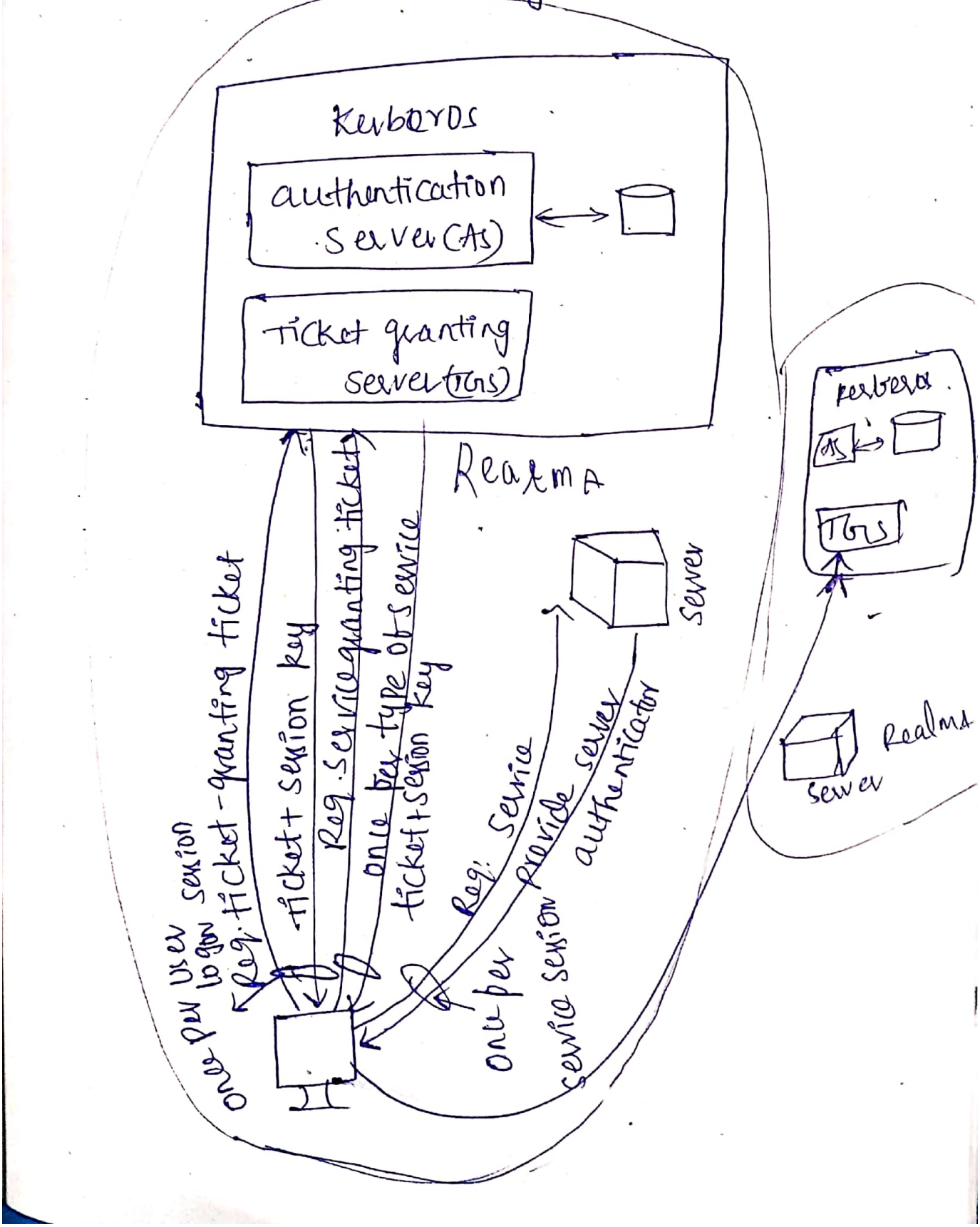
Ticket $= E_{Ktgs}[$ Flags $||K_{c,tgs}||$ Real mc $||ID_c||$ ADc $||$ Times $]$

c) Client | server Authentication Exchange:

to obtain service

1) C → TGS: options || Ticket v || Authenticator c.

2) TGS → C: $E_{K_{c,v}}$[T_{s2} || subkey || seq #]



12/9/19

* X.509:-

It is a part of X.500.

The information includes a mapping from user name to network edges as well as other attributes and info about the user.

→ It is used in IP security SSL, set, TLS.

→ X.509 uses public key cryptography and digital signature, the standard does not dictate they used to any but recommended to used RSA.

→ The ds scheme is assumed the use of a hash function.

* Certificate Format:-

1) Version:- There are 3 versions. V1, V2, V3 and default version is V1.

Signature algo. identifier

Period of validity

Subject public key information

Signature

2) Serial

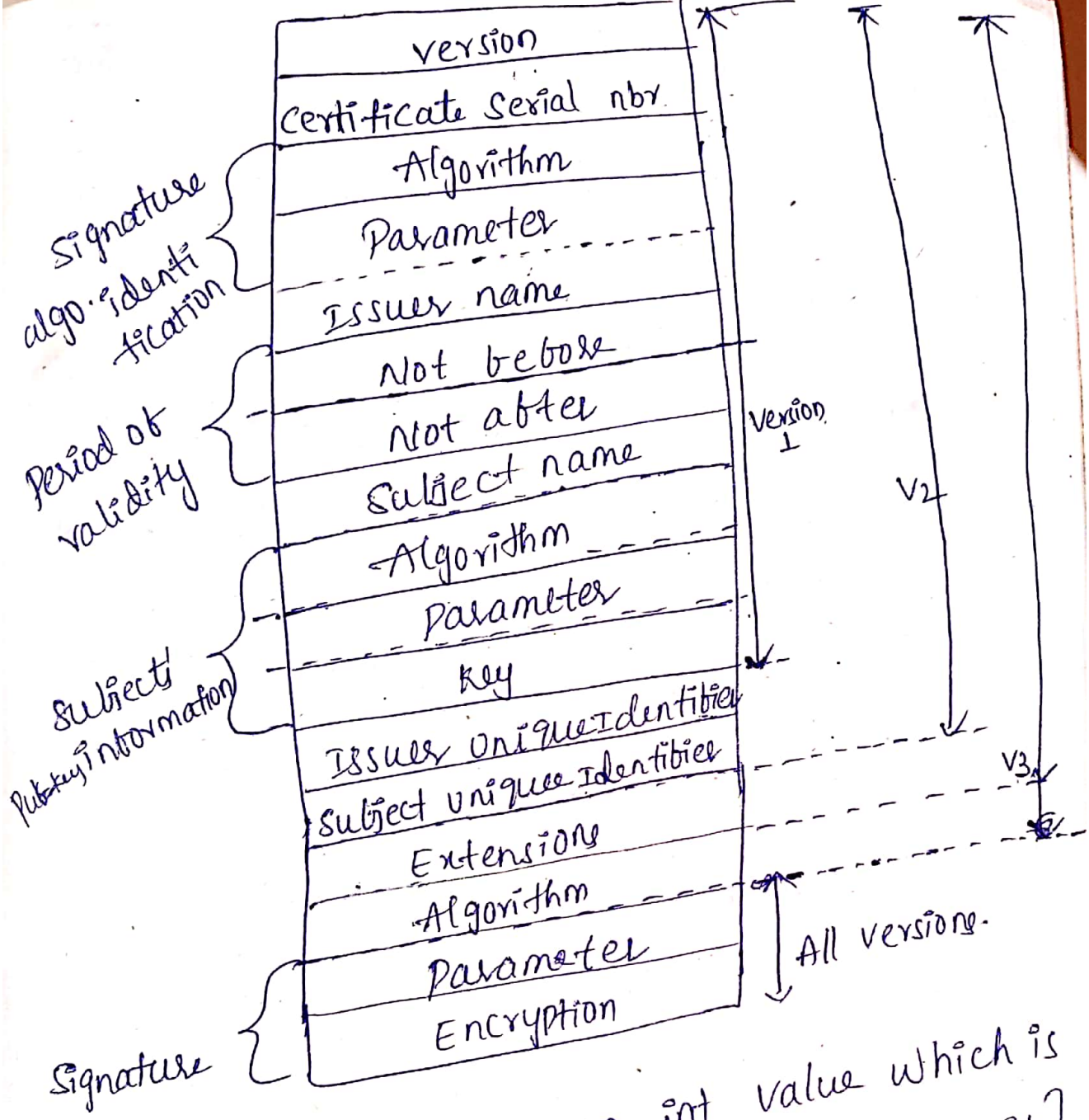
Unique

ie. which

3) signature

used to

any



2) Serial nbr: It is an int value which is Unique with in the CA [certificate Authority] issuing. ie. which is associated with this

3) Signature Algorithm Identifier: The algo is used to sign the certificate together with any associated Parameter.

4) Issuer Name:- Name of the certificate Authority that created & signed on this certificate

5) Period of validity:-

It consists the dates that is the first and last in which the certificate is valid.

6) Subject Name:- The name of the user to whom this certificate refers.

7) subject public key info:-

The public key of the subject plus an identifier of the algorithm for which this key is to be used.

8) Issuer Unique Identifier:-

An optional stream field used to identi uniquely the issuing field in the event the x.500 name has been used for a diff en

9) Subject Unique Identifier:-

An optional bit string field used to ide the subject in the event x.500 name ha

been re-used for distnt entities.

10) Extensions:-

A set of one or more Extension fields

11) signature:-

This covers all of the other fields of certificate it contains the hash code of the other fields encrypted with the CA's private key. Thus ~~field~~ have signature algorithm identifier.

→ The standard users the following notations to define a certificate

$$CA\langle\langle A \rangle\rangle = CA\{V, SN, AI, CA, TA, A, AP\}$$

where [CA = certificate Authority.]

$Y\langle\langle X \rangle\rangle$ means that

- The certificate of user X issued by certification Authority Y.

→ $Y\{I\}$ = The signing of I by Y. It consists of I with an encrypted hash code

→ The CA signed the certificate with its secret keys & the corresponding public key is known to user. then that user can verify that certificate signed by the CA is valid.

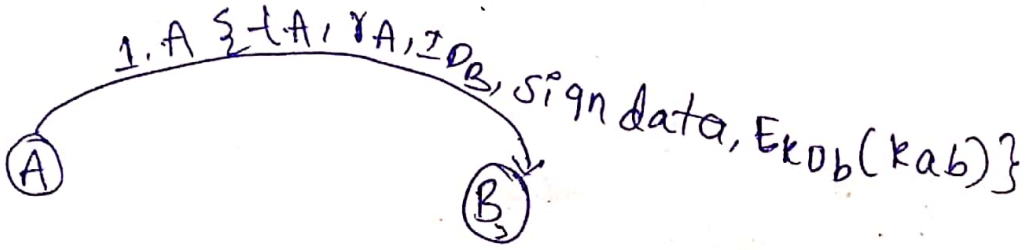
13/09/19

* Authentication process in X.509:-

3 Procedures

1) one-way authentication
2) Two-way authentication
3) Three-way authentication.

1) one-way authentication:-



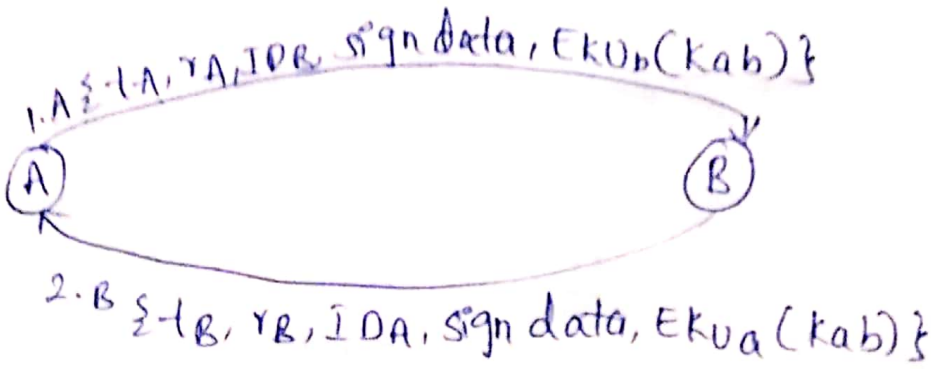
rA = random nbr / Nonce

IDB = Identification of B

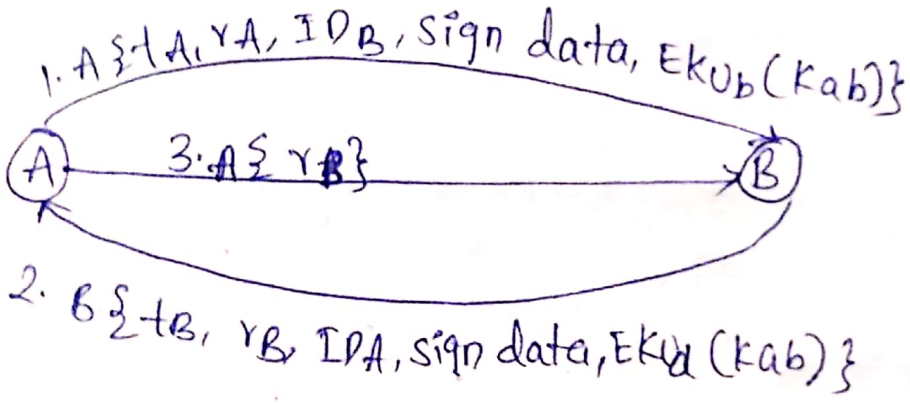
EkUb(kab) = session key encrypted

Only A can send the data.

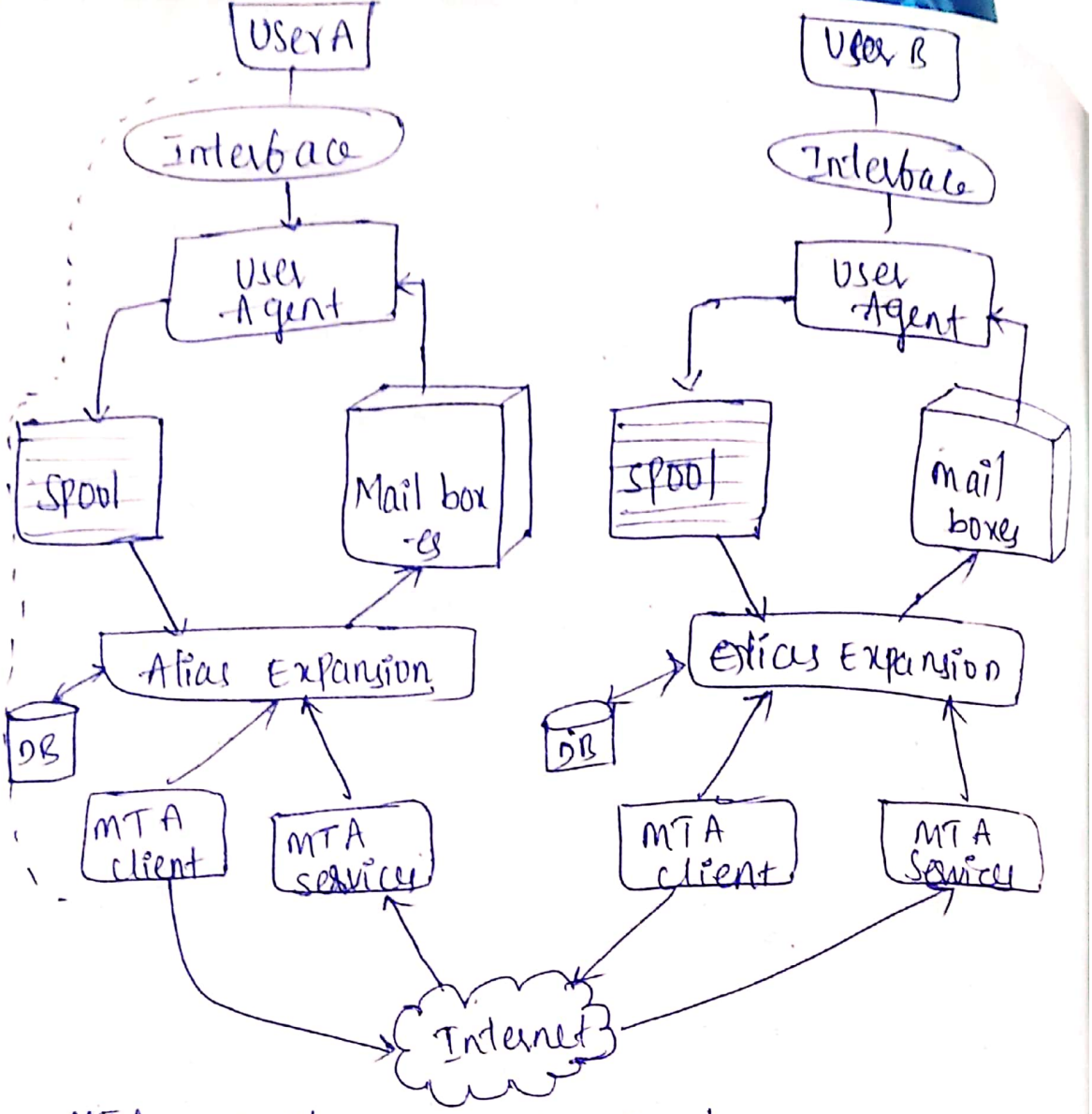
2) Two- way Authentication:-



3) Three- way Authentication:-



* Complete Email System:- (85)



MTA = Mail Transpevent Agent

POP = Post office Protocol

IMAP = Internet mail Access protocol

These two protocols are used in mixing.

But now these replaced by HTTP protocol for more reliability.

These leads to move vulnerability so that we go for Email security.

* Email - Security:-

Some of the security services for Email is

1) Confidentiality
2) Authentication
3) Integrity
4) Non-Repetation
5) Proof of submission of mail
6) Proof of delivery of mail
7) Confidentiality of msg
8) security from self distruct
9) Auditing & accounting
10) Integrity regarding msg sequence

→ Secure email standards provide two important concepts to overcome threats.

1) PGP = pritty good Privacy
2) S/MIME

→ Provides confidentiality

radix$_{64}$ is a process to provide compatability in emails by PGP process.

→ compression decreases the size of data and by that increase the speed of sending data.

→ Authentication we use Private key of Receiver Based on digest value/key Receiver know the Sender information.

1) PGP (66)

High security s/w application. It is used to encrypt and apply di email along with confidentiality and Intigrity.

→ PGP was developed by zimmerman in 1991 and first version way released on internet in 1991 bcz of legal issue for usage of RSA it was purchased by via crypt and RSA Liecensed company. in 1993. and released again 1994.

→ Afo 1998 it was purchased by NIW. Associates. There are nbr of reasons that make the PGP to use widely. Some of them are 1) PGP is free bere but also commercial versions available

2) Operating system independent. and independent from Processor.

3) Used Popular & std algo's like RSA, DSS IDEE.

4) It has wide range of applications. one of the major reason is it was not controlled by any governamental and std. organizations.

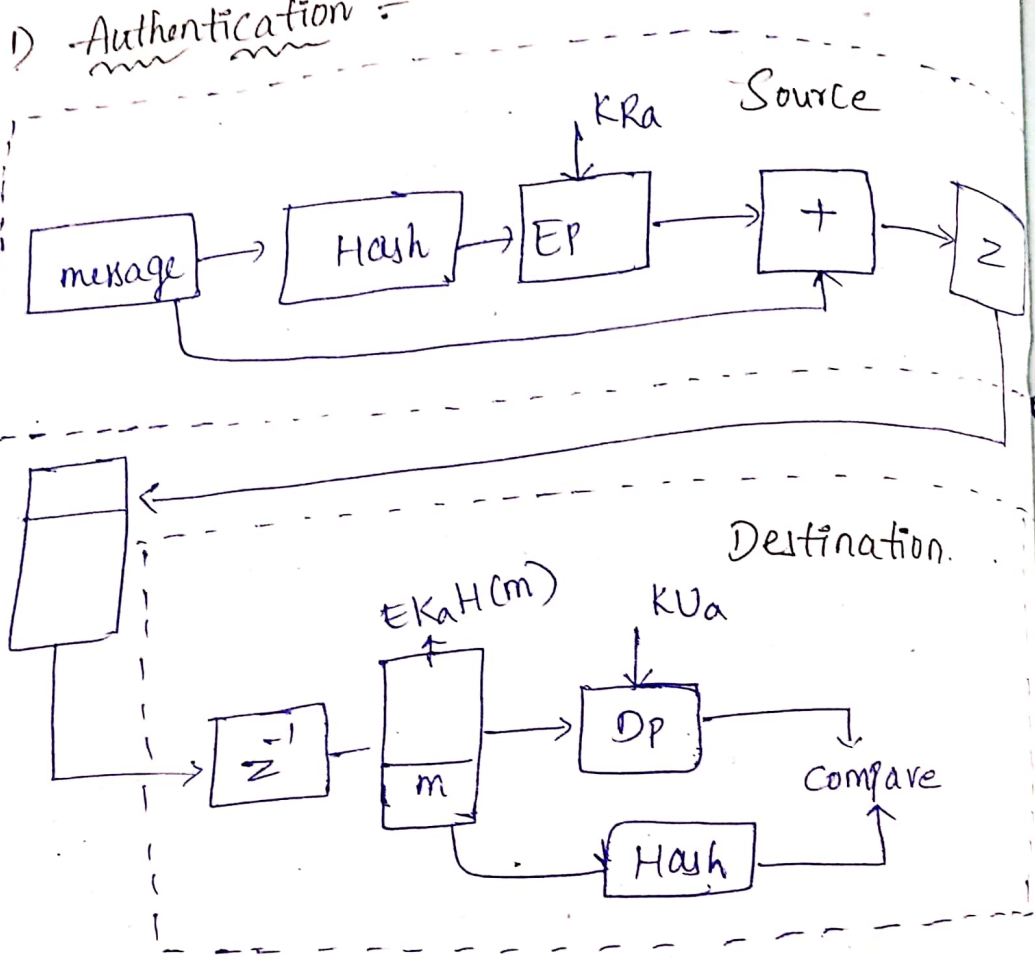
* Pritty good Privacy Operations :—

Service	Function	Algorithm used
Authentication	Digital signature	DSS/SHA or RSA/SHA
Confidentiality	msg encryption	CAST or IDEA or Triple DES along with or RSA
Speed	Compression	zip
Transmission	E-mail Compatability	Radix 64 Conversion

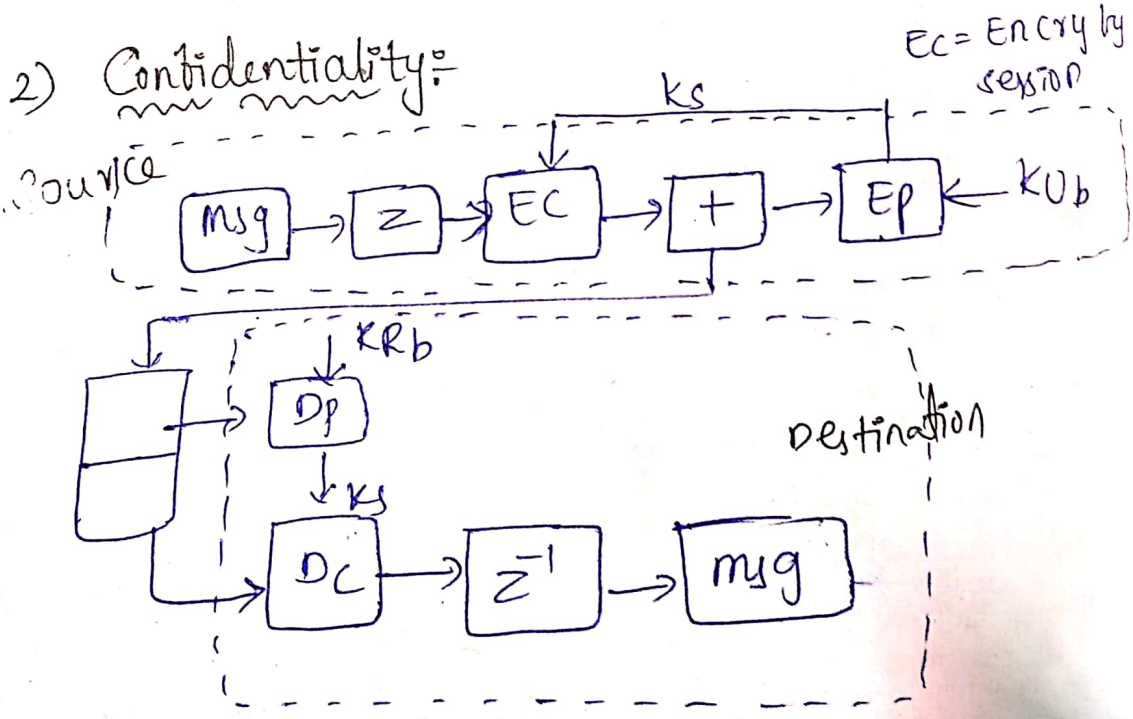
Limitation

Segmentation

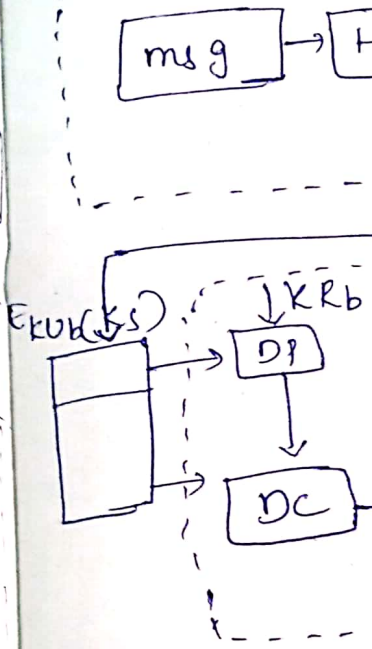
1) Authentication :



2) Confidentiality:



1 & 2 Combine:



1 & 2 combine: