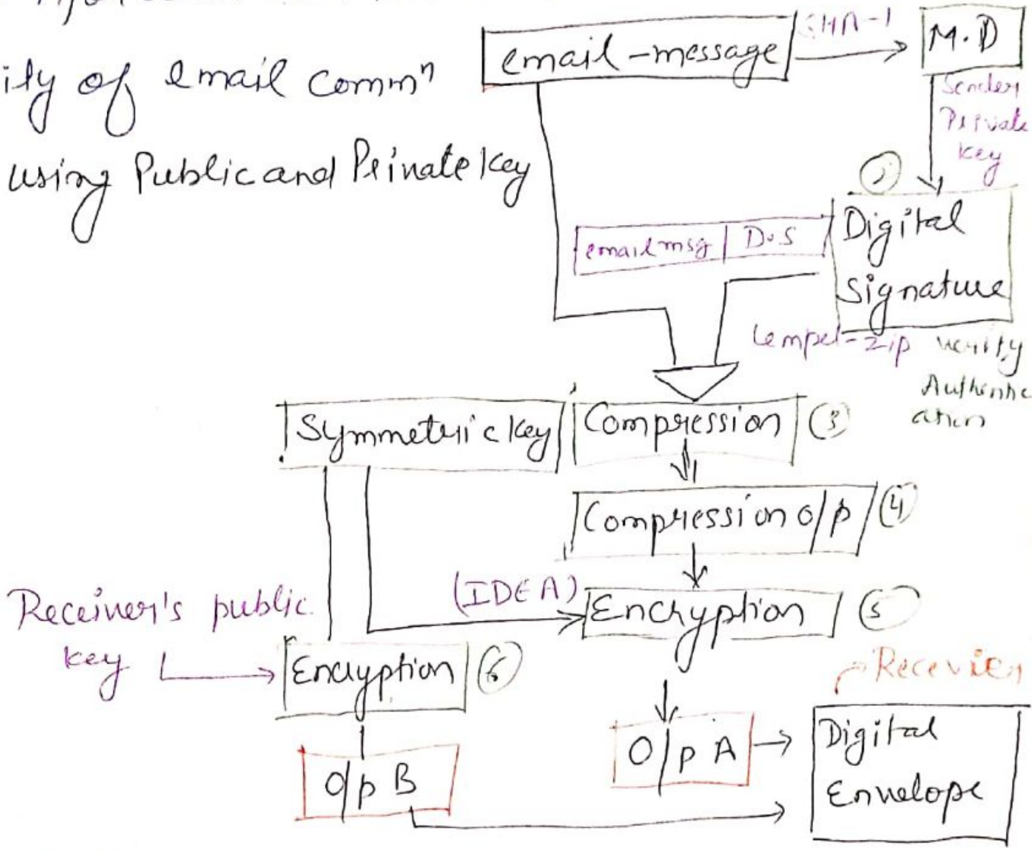
PRETTY Good ~~PRIVACY~~ PRIVACY (PGP) ↳ provides email security

father of PGP = Phill Zimmerman (1980)

It is an encryption Program that provides cryptographic privacy and authentication for data Communication.

↳ Increases Security of email commn

PGP WORKING: using Public and Private key Cryptography



Technique used in PGP

1. Hashing ↳ MD5, SHA

② Data Compression (Z)

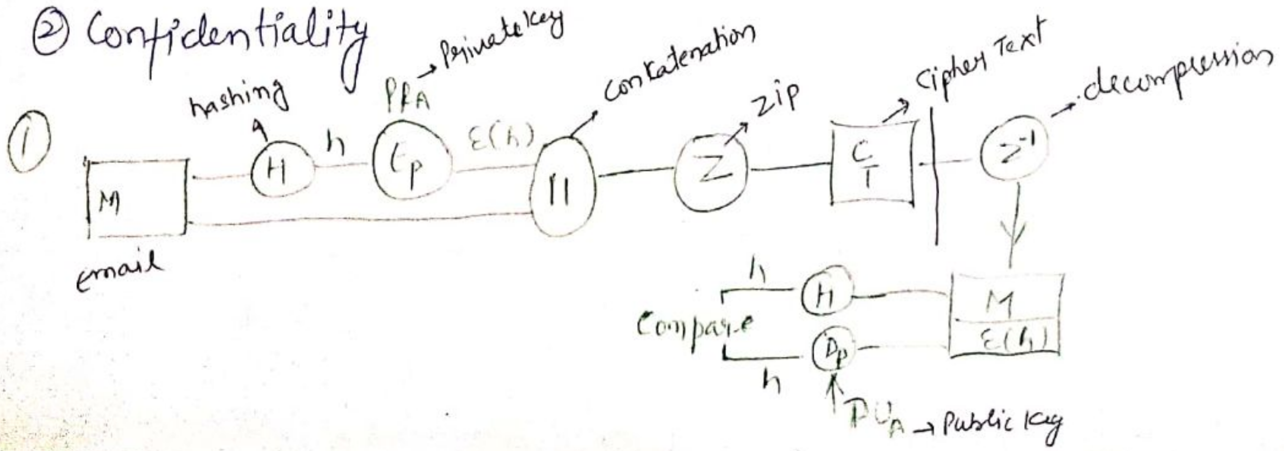
③ Symmetric key cryptography

④ Asymmetric key cryptography

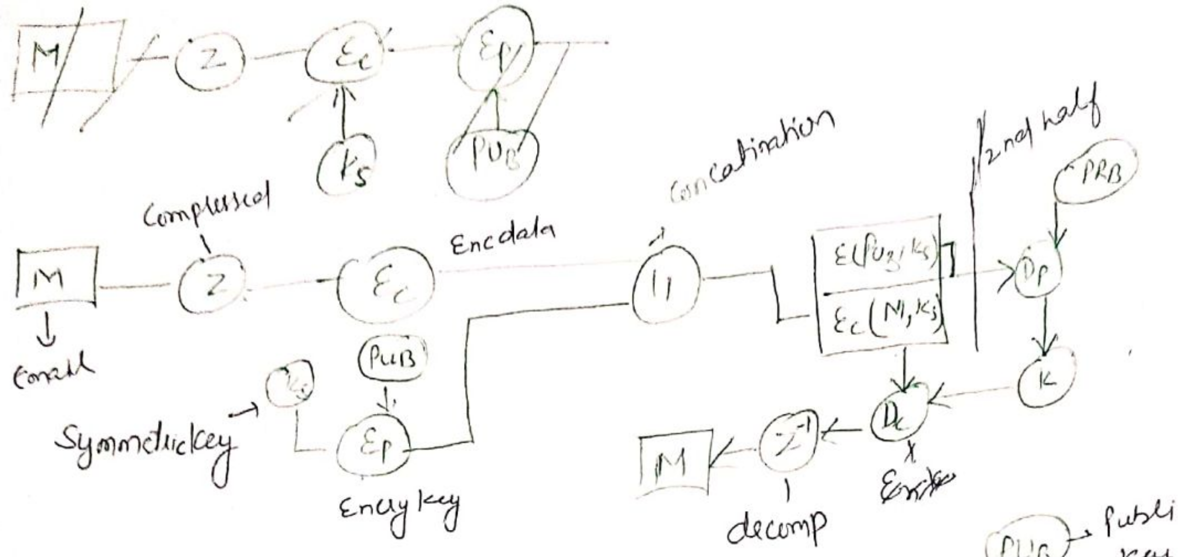
Services of PGP

① Authentication

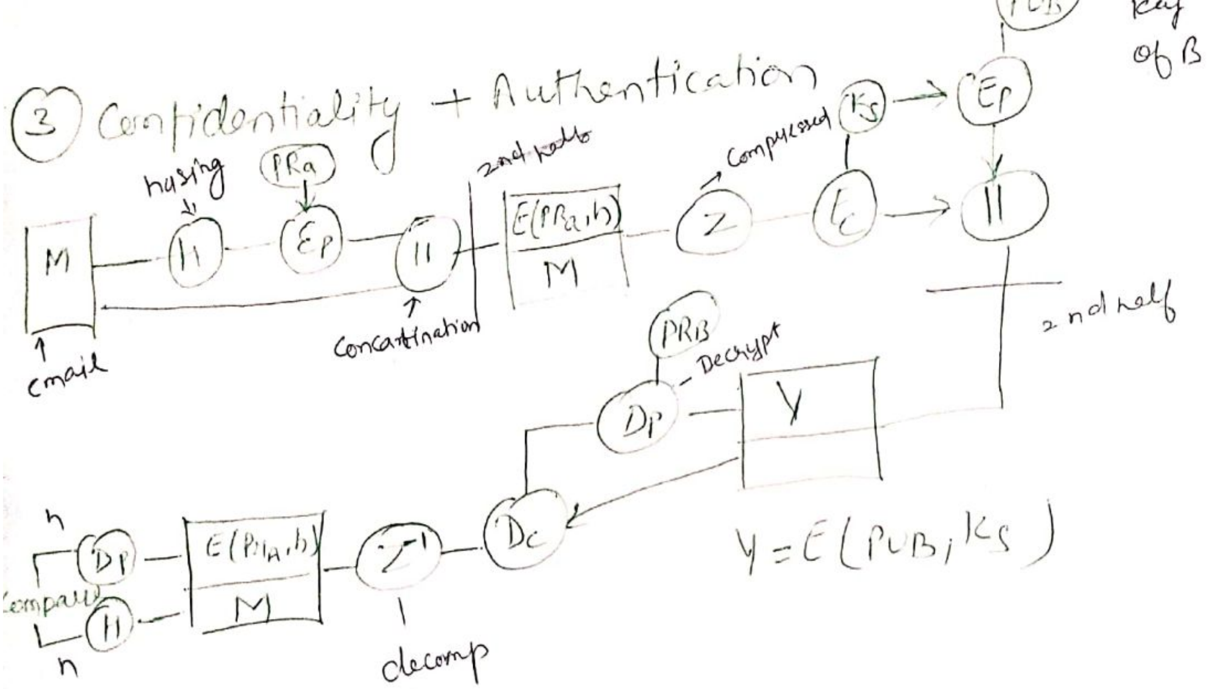
② Confidentiality



② only confidentiality

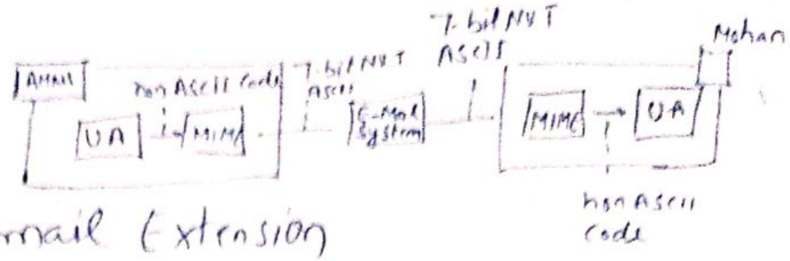


③ Confidentiality + Authentication



S/MIME PROTOCOL :-

— MIME Protocol:



Multipurpose Internet mail Extension

previously, emails could be sent only in NVT 7bit A.SCII format

(i.e. audio/video/Images etc could not be sent)

∴ MIME is Introduced

addon which allows us to Transfer non ASCII data over mail
(other types of data)

S/MIME Protocol:

Secure/MIME,

↳ encrypts emails and provide security

↳ Allows us to digitally sign on our email

↳ uses asymmetric key cryptography

functions of S/MIME:

1. Authentication
2. Message Integrity
3. Non-Repudation
4. Privacy
5. Data Security

~~Sett~~ Services of S/MIME :-

1. Digital Signature
2. Message Encryption

7

Difference b/w PGP and S/MIME

PGP	S/MIME
1. It is designed for processing the plain text	1. While it is designed to process email as well as many multimedia files
2. PGP is less costly as compared to S/MIME	2. While S/MIME is comparatively expesive
3. PGP is good for personal as well as office use.	3. It is good for industrial use.
4. PGP is less efficient than S/MIME	4. It is more efficient than PGP
5. It depends on user key exchange.	5. Whereas it relies on a hierarchically vaild certificate for key exchange.
6. PGP is comparatively less convenient	6. While it is more convenient than PGP due to the secure transformation of all the applications.
7. PGP contains 4096 public keys	7. While it contains only 1024 public keys
8. PGP is the standard for strong encryption	8. While it is also the standard for strong encryption but has some drawbacks
9. PGP is also be used in VPNs.	9. While it is not used in VPNs, it is only used in e-mail services.
10. PGP uses Diffie Hellman digital signature.	10. While it uses Elgamal digital signature.