1. PREETY GOOD PRIVACY

- **Explain Pretty Good Privacy in detail. (16 Marks) May/June'14,Nov/Dec'12**
- **Explain PGP message generation and reception.(16 Marks) Apr/May'11**
- **Illustrate the confidentiality service provided by PGP.(8 Marks) (May/June'2007)**
- **For what purpose Zimmerman developed PGP? Brief the various services provided by PGP. Discuss the threats faced by an e-mail and explain its security requirements to provide a secure e-mail service. (16 Marks) (Nov/Dec '14)**

Pretty Good Privacy

Definition of PGP: **(2 Marks Nov/Dec'2013)**

PGP provides confidentiality and authentication service that can be used for electronic mail and file storage applications.

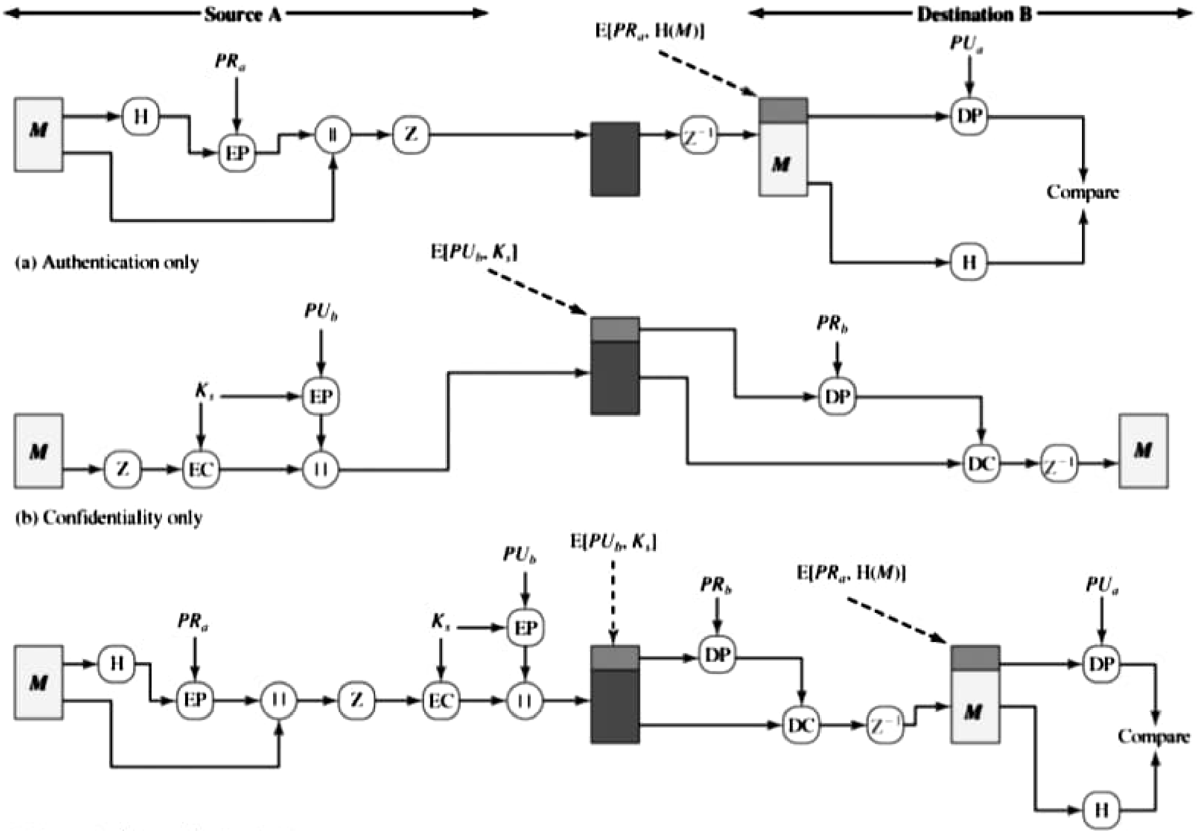
Pretty Good Privacy is an open-source freely available software package for e-mail security. It provides authentication through the use of digital signature; confidentiality through the use of symmetric block encryption; compression using the ZIP algorithm; e-mail compatibility using the radix-64 encoding scheme; and segmentation and reassembly to accommodate long e-mails.

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

1. Selected the best available cryptographic algorithms as building blocks
2. Integrated these algorithms into a general-purpose application that is independent of operating system and processor and that is based on a small set of easy-to- use commands
3. Made the package and its documentation, including the source code, freely available via the Internet, bulletin boards, and commercial networks such as AOL (America On Line)

4. Entered into an agreement with a company (Viacrypt, now Network Associates) to provide a fully compatible, low-cost commercial version of PGP.

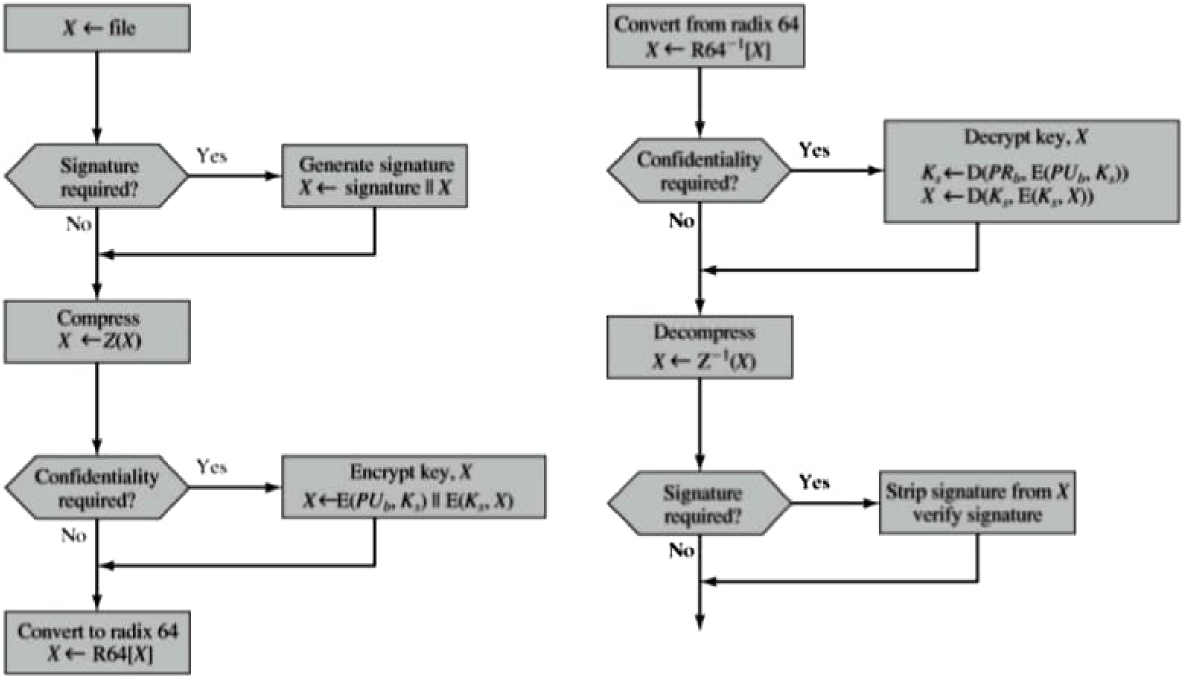
Confidentiality and Authentication



(a) Authentication only

(b) Confidentiality only

(c) Confidentiality and authentication



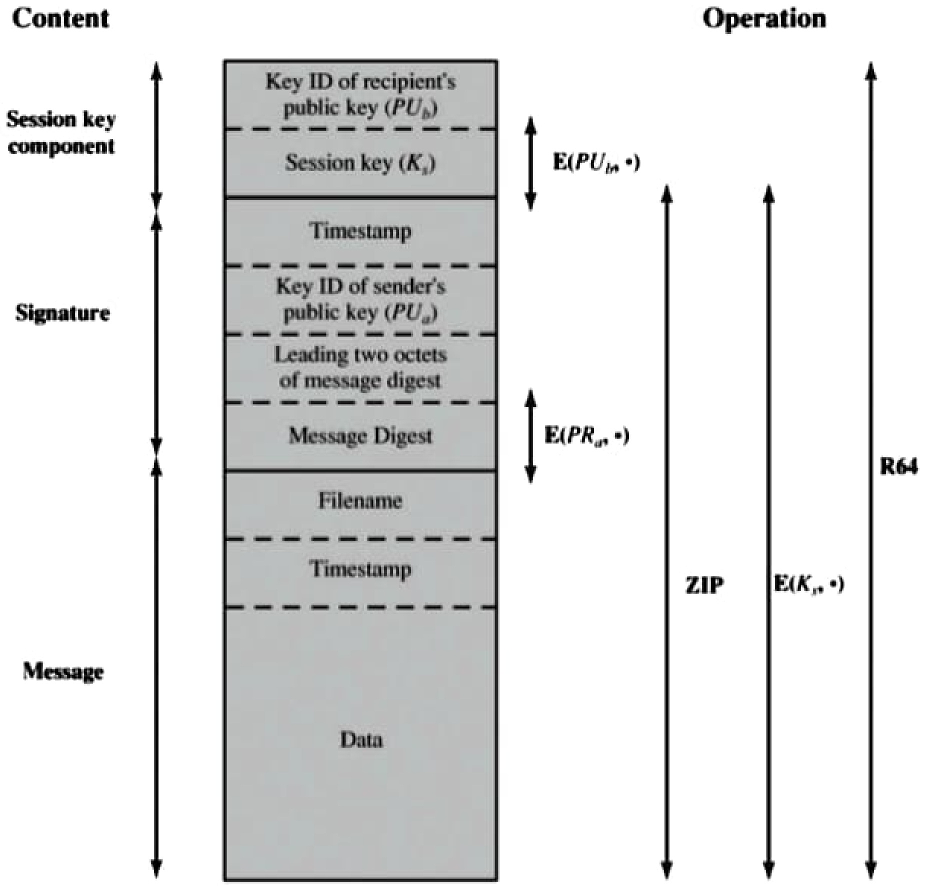
(a) Generic transmission diagram (from A)

(b) Generic reception diagram (to B)

Cryptographic Keys and Key Rings

1. A means of Type equation here. Type equation here. generating unpredictable session keys is needed.
2. We would like to allow a user to have multiple public-key/private-key pairs.
3. Each PGP entity must maintain a file of its own public/private key pairs as well as a file of public keys of correspondents.

General Format of PGP Message (from A to B)
Sketch the general format for PGP message. (2 Marks-Nov/Dec'2014)



Notation:
E(PU_b, •) = encryption with user b's public key
E(PR_a, •) = encryption with user a's private key
E(K_s, •) = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

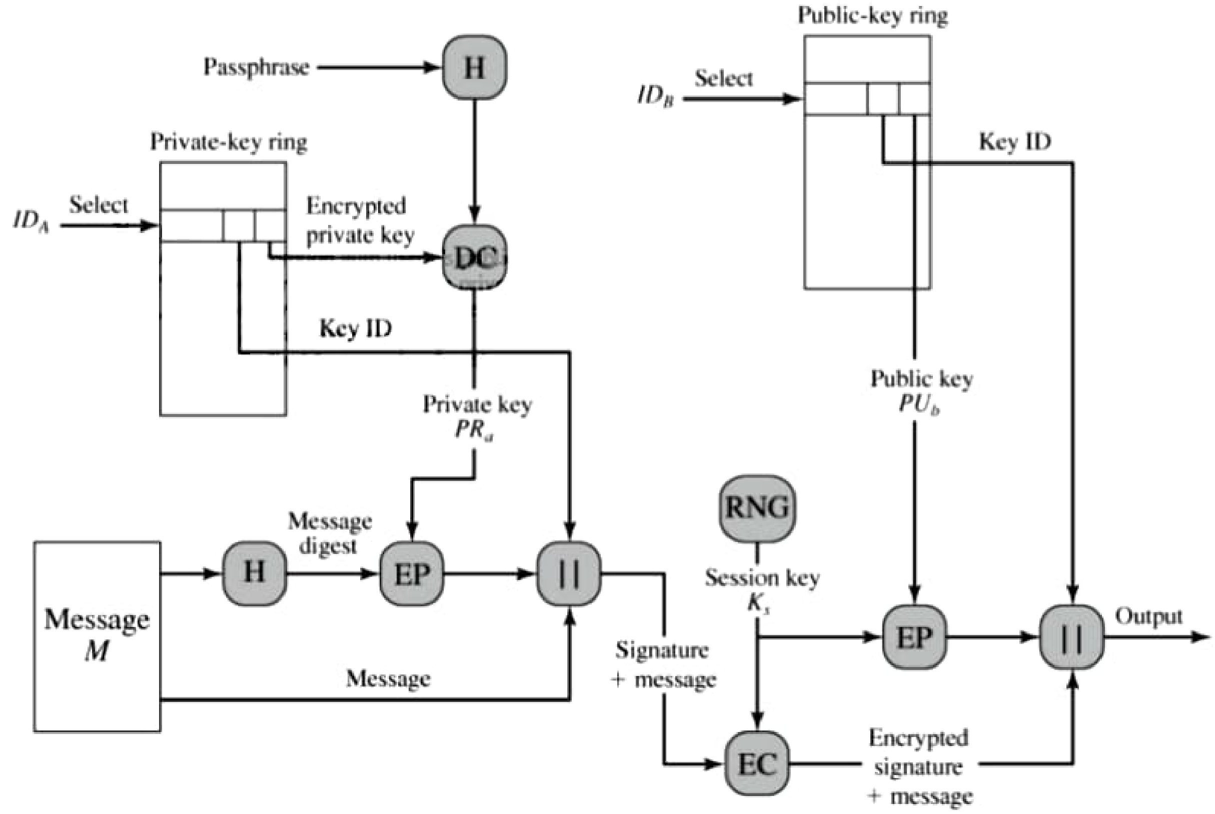


Figure: PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

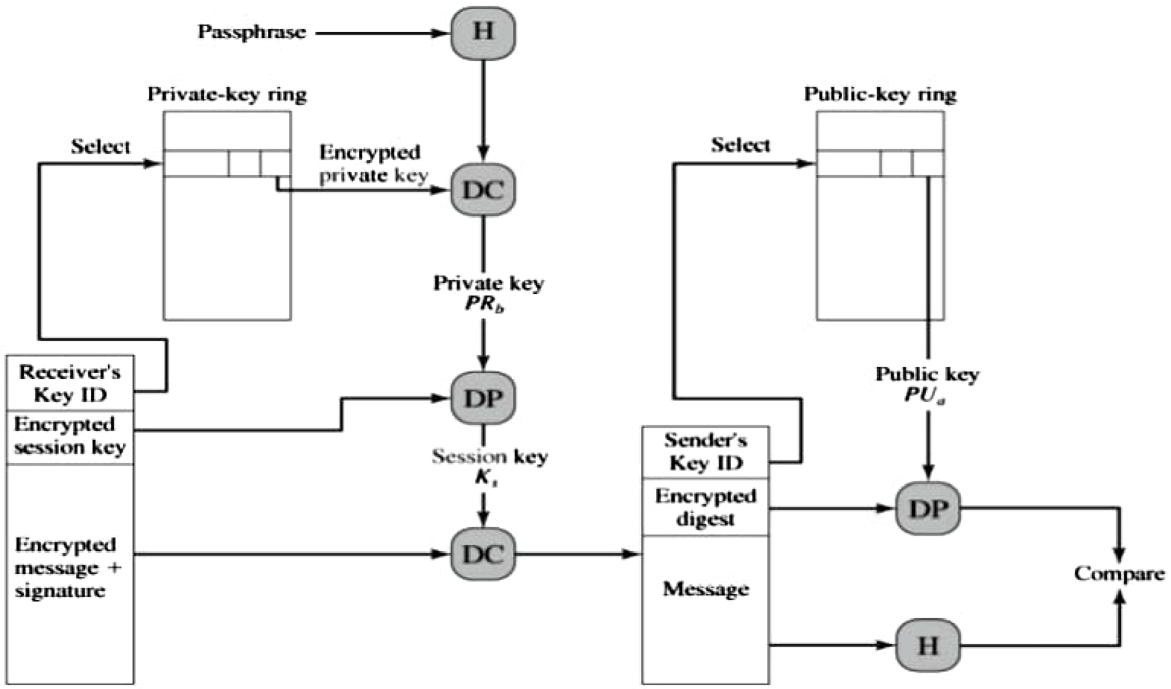
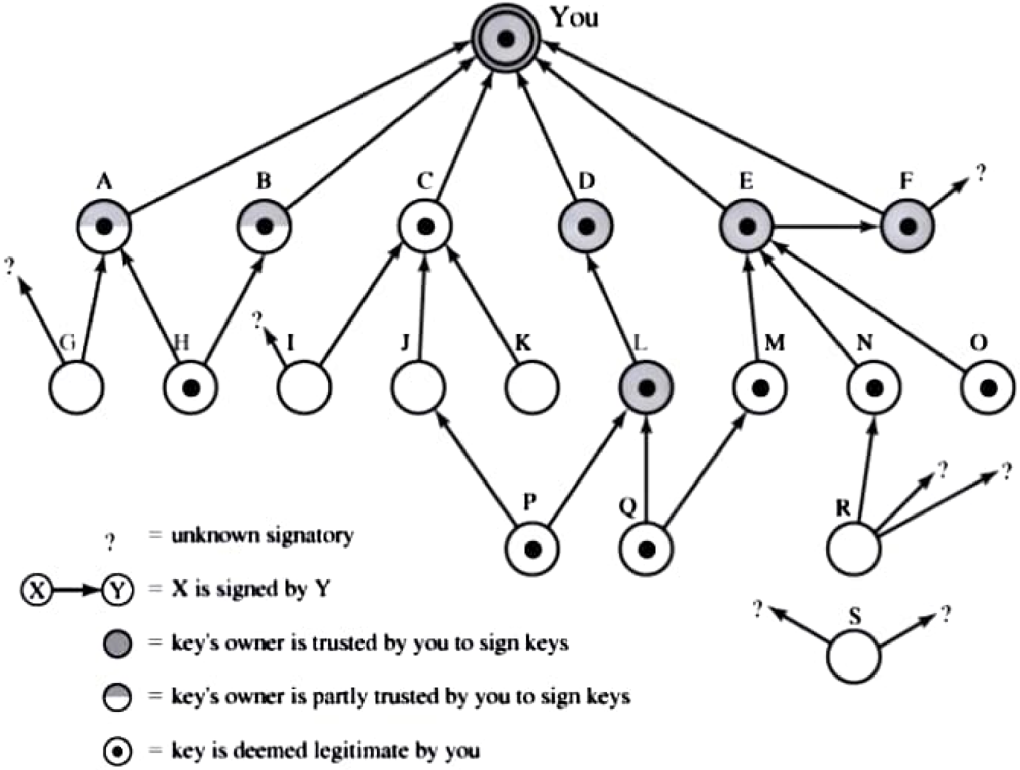


Figure: PGP Trust Model Example


You
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
?
? = unknown signatory
X Y = X is signed by Y
● = key's owner is trusted by you to sign keys
◒ = key's owner is partly trusted by you to sign keys
⊙ = key is deemed legitimate by you