SNS COLLEGE OF ENGINEERING
Kurumbapalayam(Po), Coimbatore – 641 107
An Autonomous Institution
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 5: CYBER SECURITY SAFEGUARDS AND SECURITY SERVICES

Topic : PGP

THE PROBLEM

e-mail "security"

SMTP protocol

S: 220 smtp.example.com ESMTP Postfix C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPTTO:<alice@example.com> S: 250 Ok
C: RCPTTO:<theboss@example.com> S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF> C: Hello Alice.
C: Your friend, Bob C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye

SMTP protocol

PLAIN TEXT

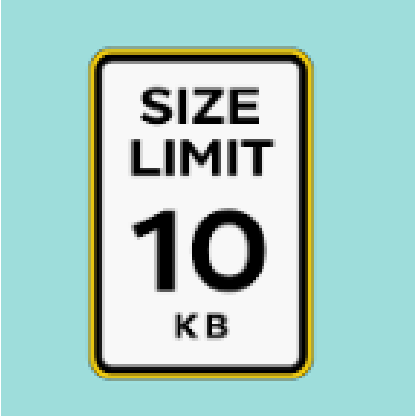
everyone on the way can read it

SMTP protocol

NO AUTHENTICATION

everyone can pose as anyone

SMTP protocol

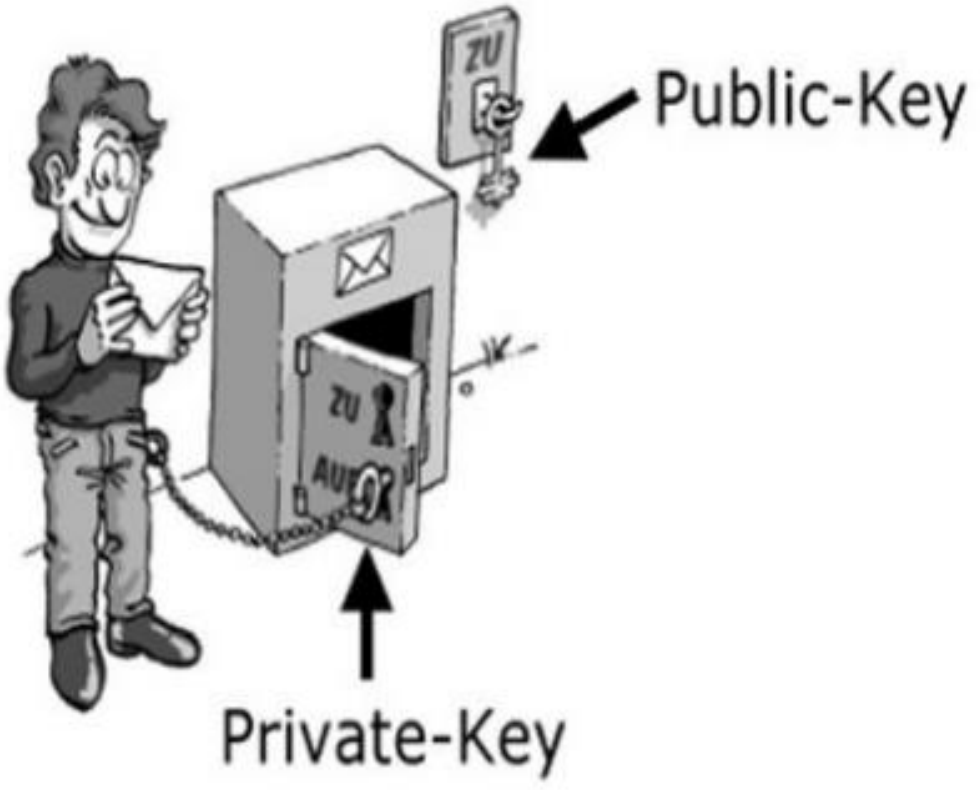


SIZE LIMIT

e-mails are limitedin size

THE SOLUTION

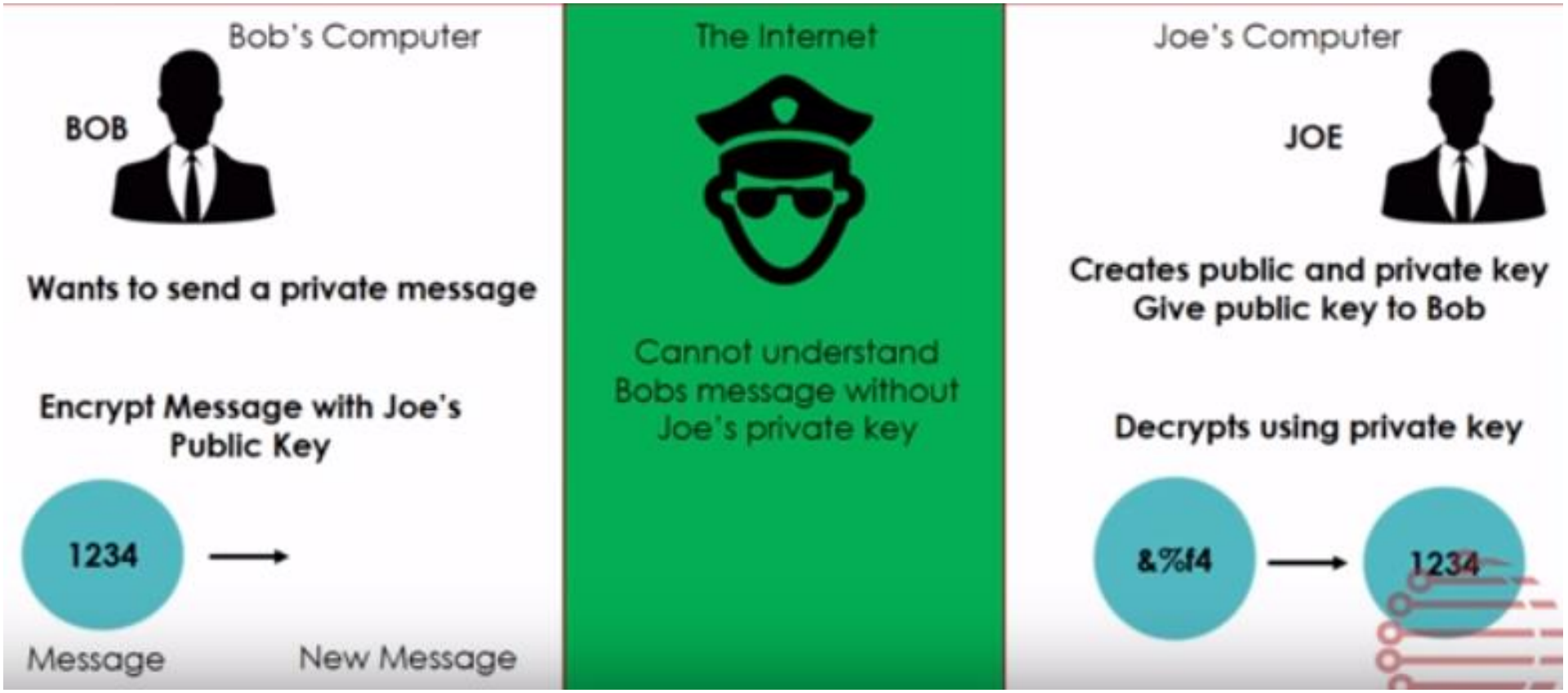
PGP - open solution to our problems



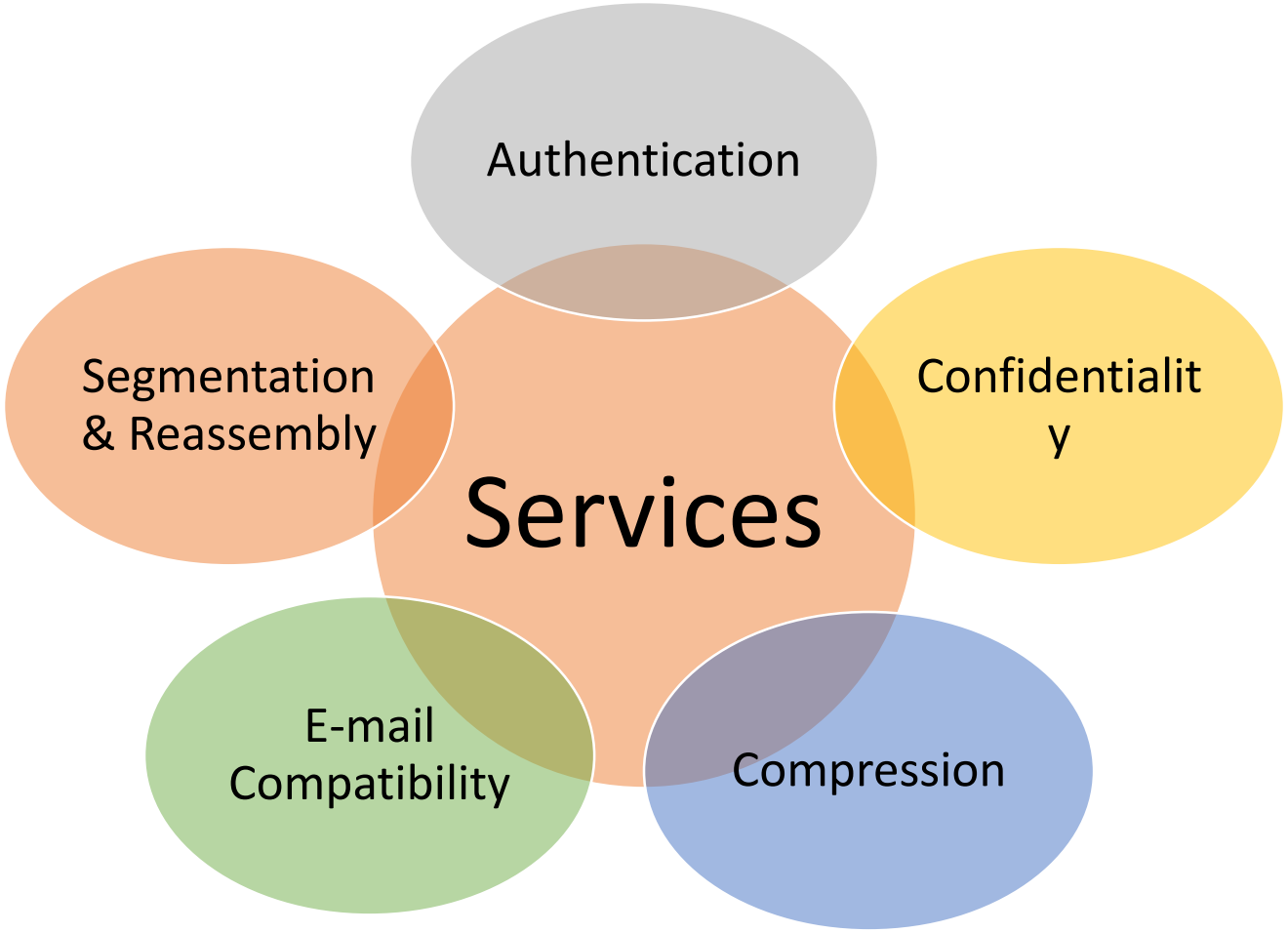
Pretty Good Privacy (PGP)

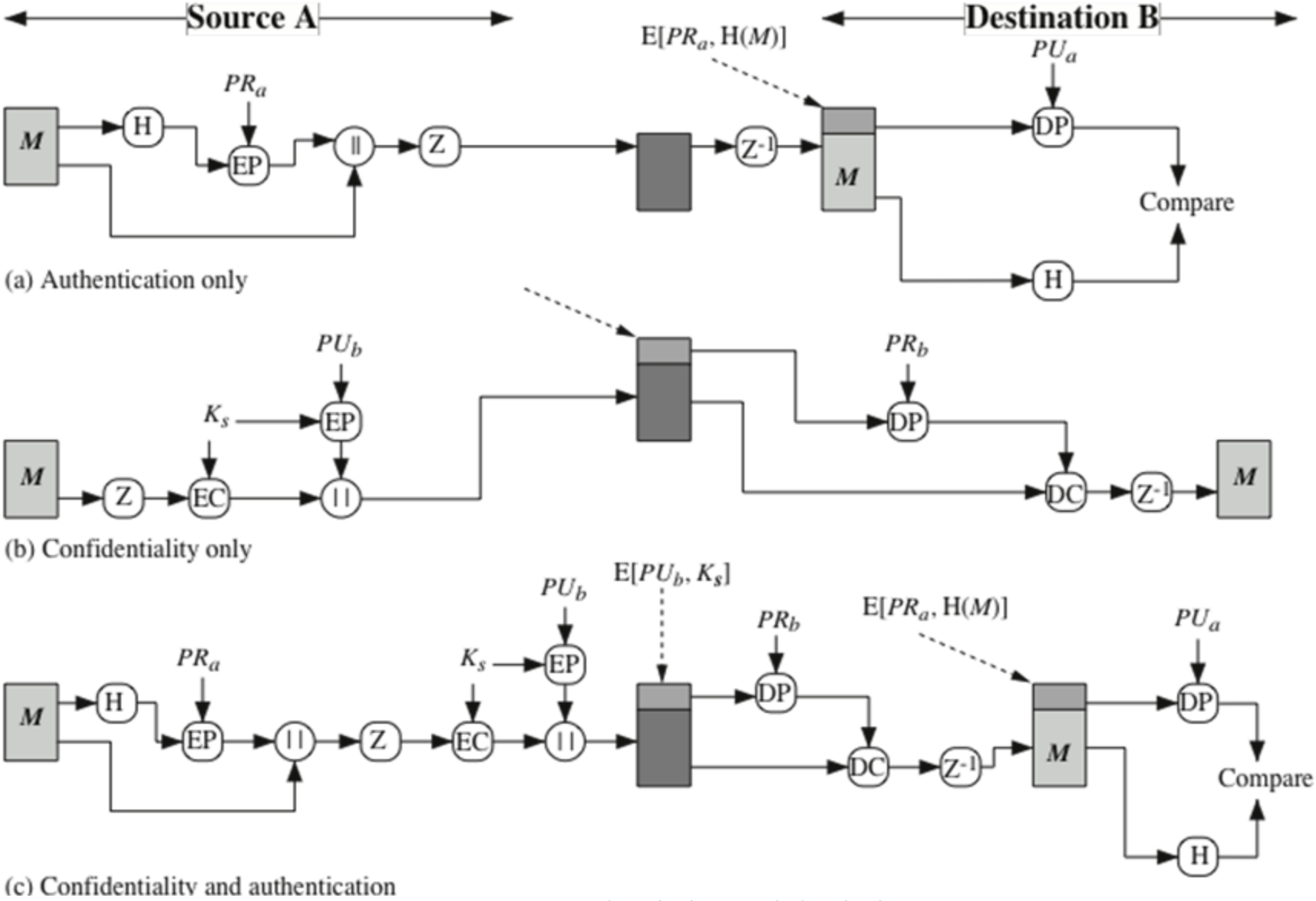
- widely used de facto secure email
- developed by Phil Zimmermann
- Best Available Cryptographic Algorithm
- Available on Unix, PC, Macintosh and Amiga systems
- originally free, now have commercial versions available also

How PGP Works?

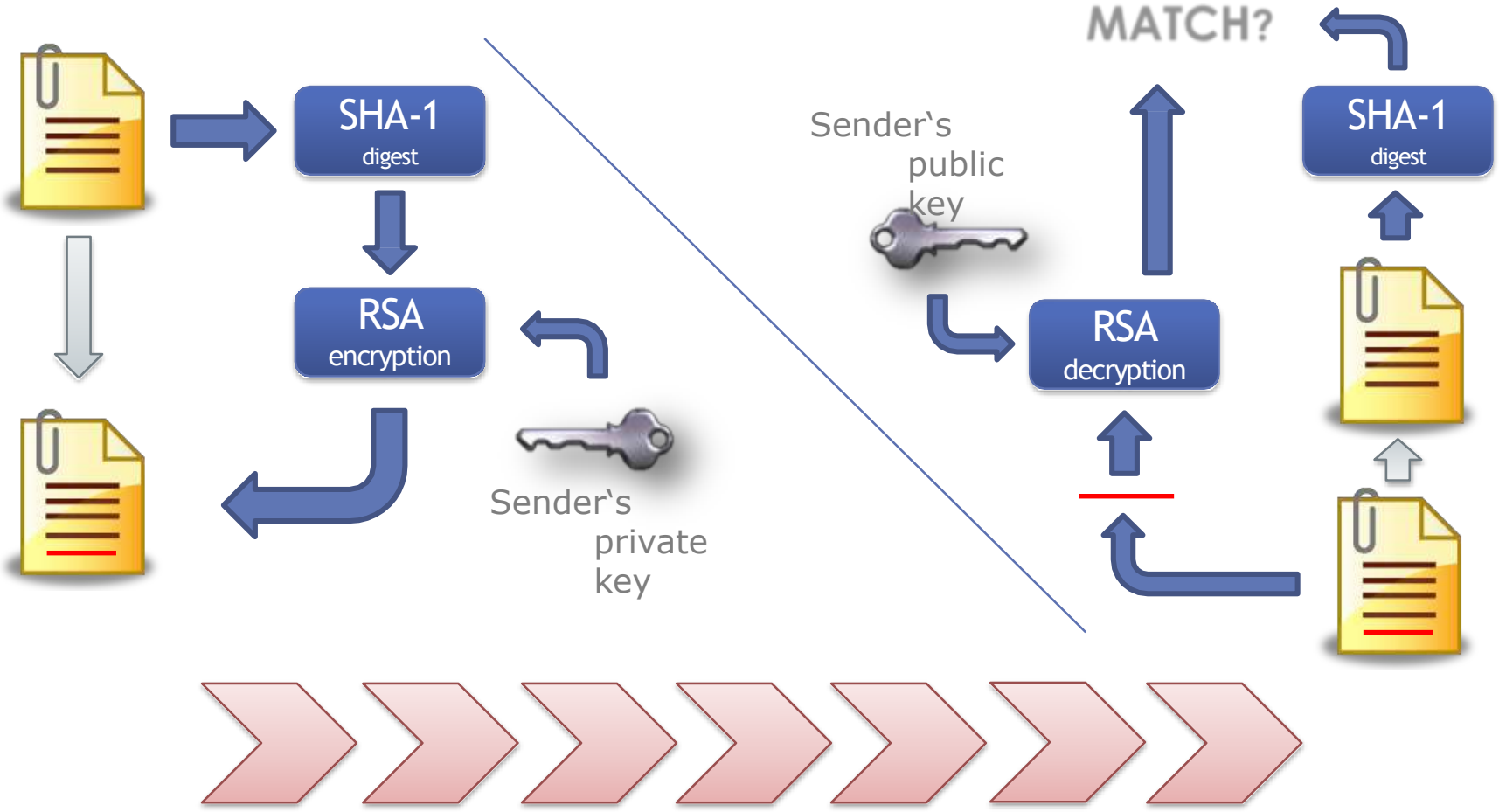


PGP Services




Source A
Destination B
$E[PR_a, H(M)]$
PU_a
PR_a
M
H
EP
||
Z
Z^{-1}
DP
Compare
(a) Authentication only
PU_b
PR_b
K_s
EC
DC
(b) Confidentiality only
$E[PU_b, K_s]$
(c) Confidentiality and authentication

Authentication - *confirming the sender's identity*



Confidentiality- *message is known to the intended person*

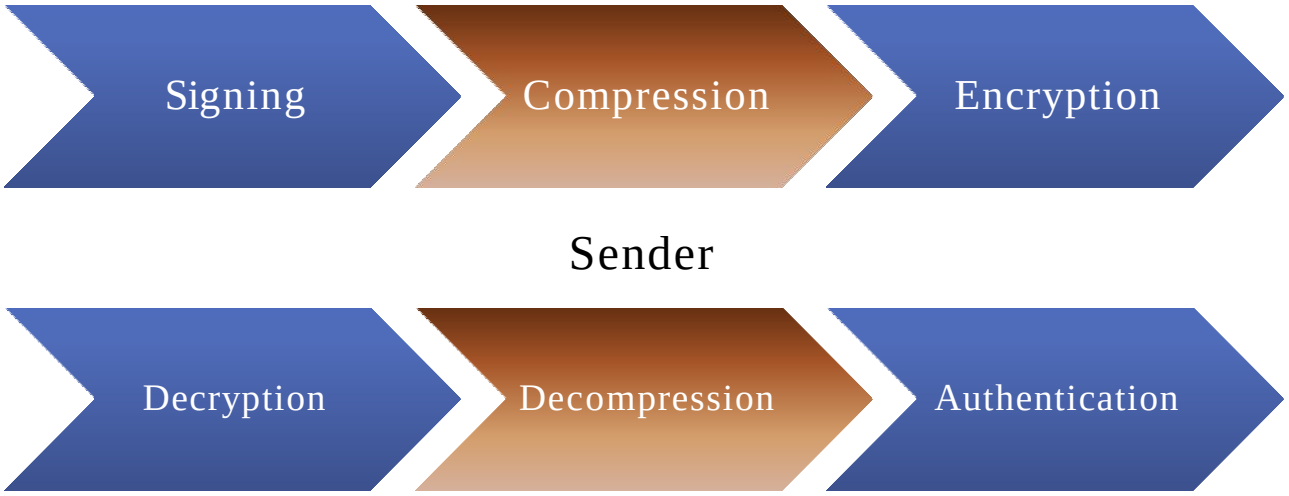
- Sender generates message and random 128-bit number to be used as session key for this message only
- Message is encrypted, using CAST-128 / IDEA/3DES with session key
- Session key is encrypted using RSA with recipient's public key, then attached to message
- Receiver uses RSA with its private key to decrypt and recover session key
- Session key is used to decrypt message

Confidentiality & Authentication

- uses both services on same message
  - create signature & attach to message
  - encrypt both message & signature
  - attach RSA encrypted session key

Compression

- After signing but before encrypting
  - One can store uncompressed message & signature for later verification
  - compression is non deterministic
- uses ZIP compression algorithm



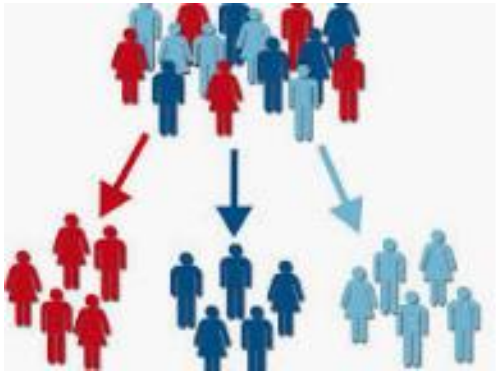
Email Compatibility

- traveling across platforms avoiding maximum size limit

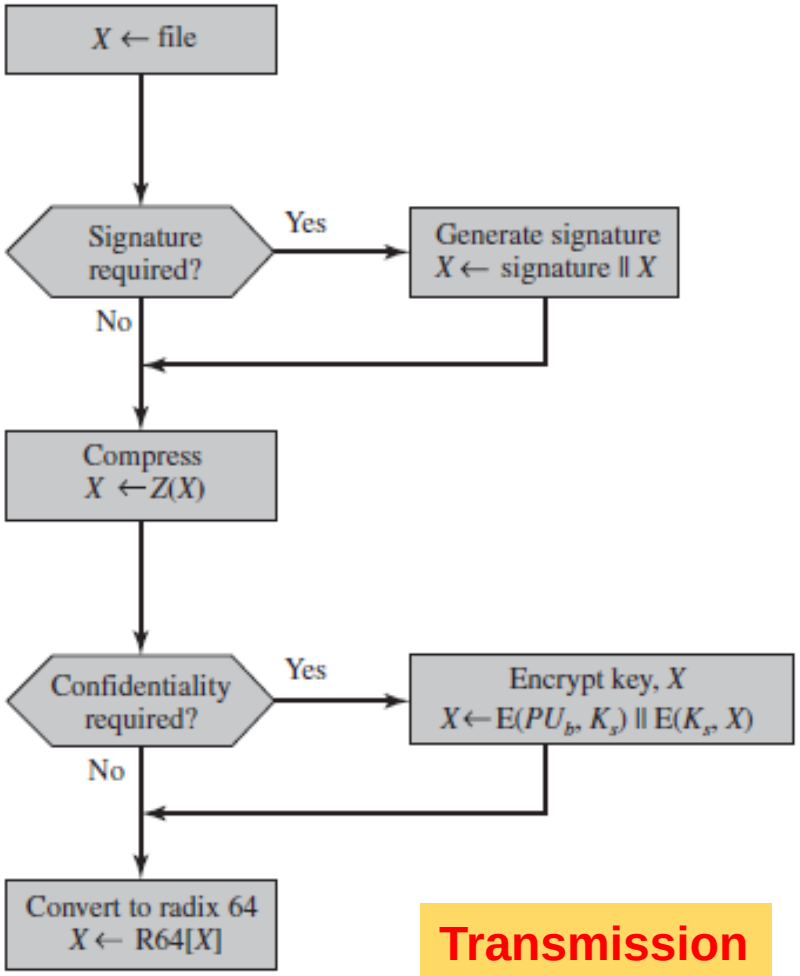
binary data → radix-64

Segmentation & Reassembly

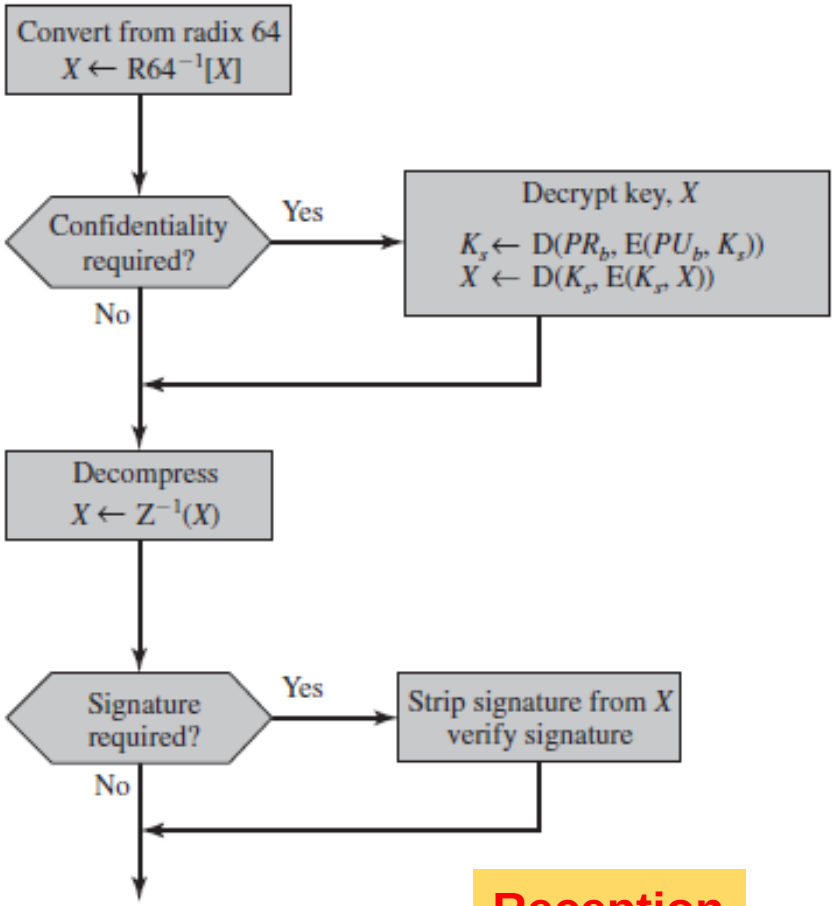
automatic segmentation and reassembly of long messages



PGP Operations



Transmission



Reception

Thank You