CS 465

SECURE EMAIL

Slides by Kent Seamons and Tim van der Horst
Last Updated: Oct 8, 2012

Goals

- Be able to describe how secure email works to provide confidentiality, integrity, and authentication
- Understand the different in trust models between
  - PGP
  - S/MIME
- Gain experience using secure email

PGP Background

- Designed by Phil Zimmerman
  - Originally designed as a human rights tool
  - Published for free on the Internet in 1991
  - Phil was the target of a three year criminal investigation
- Where to get PGP?
  - http://www.philzimmermann.com/EN/findpgp/index.html
    - pgp.com
    - GnuPG (GPG)
- In the 1990's, one way to skirt federal export controls was to publish the source code in book form (this was allowed), ship the books to Europe, scan the source code using OCR technology to create the code. Laborious, but legal.
- Trust model – web of trust

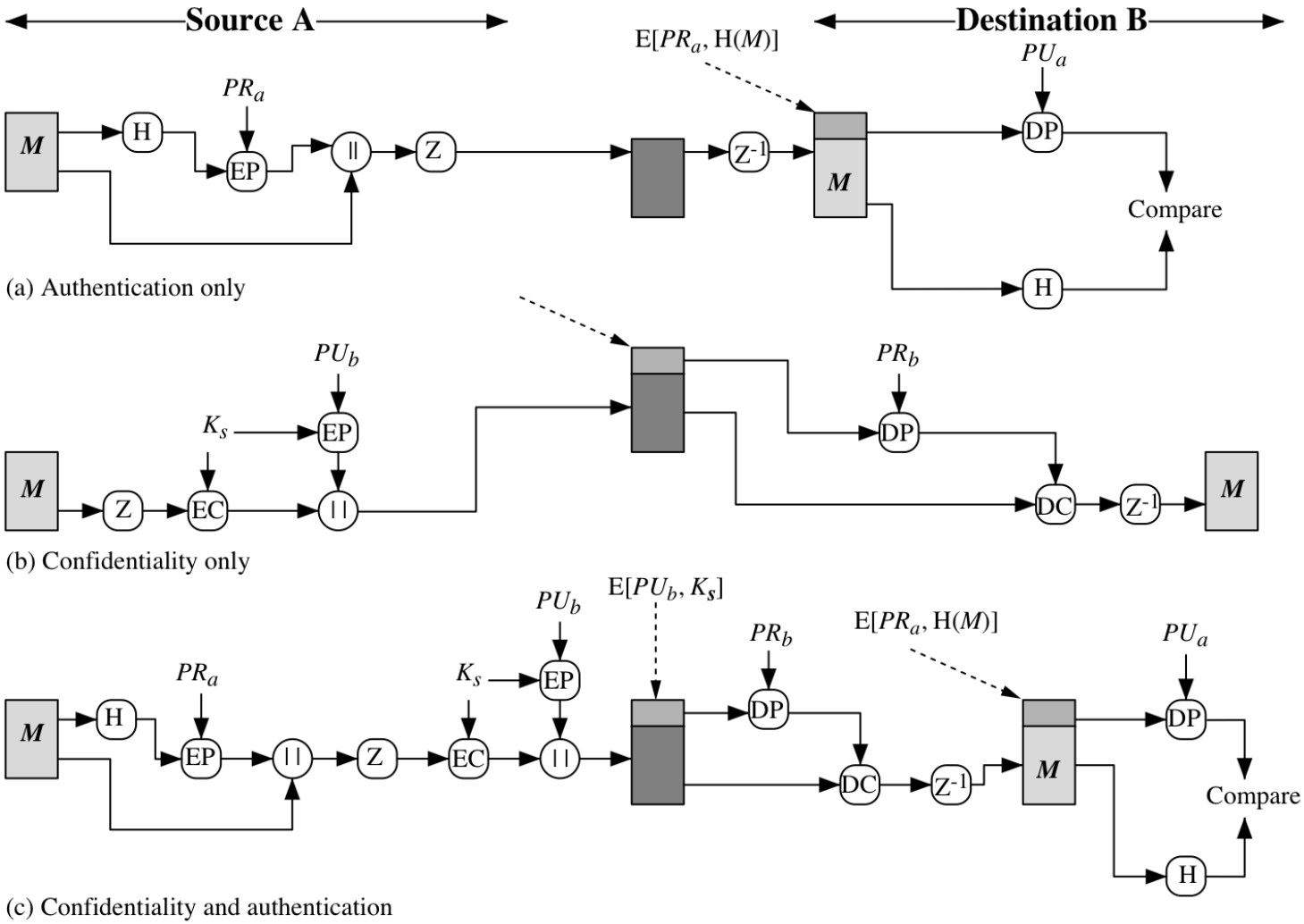
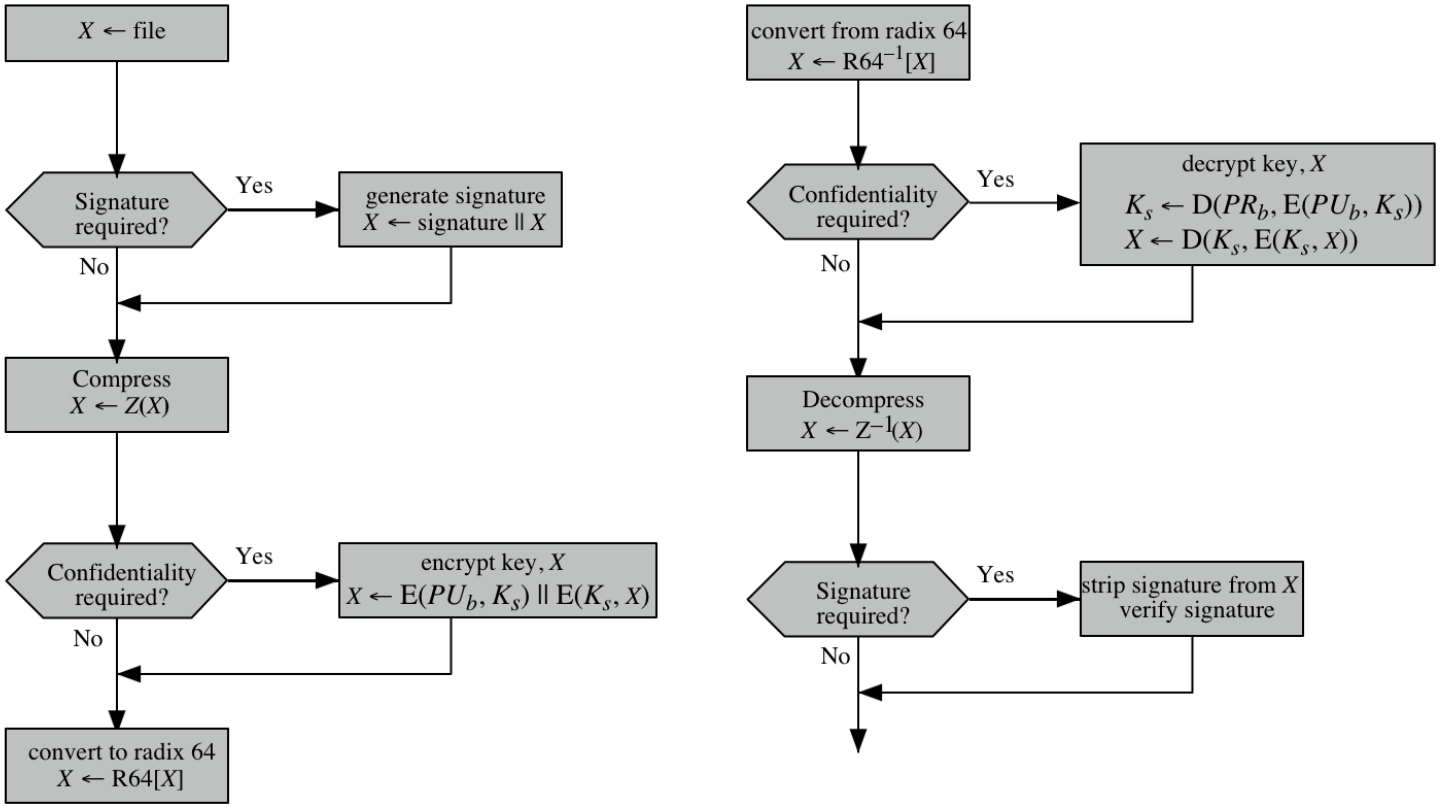


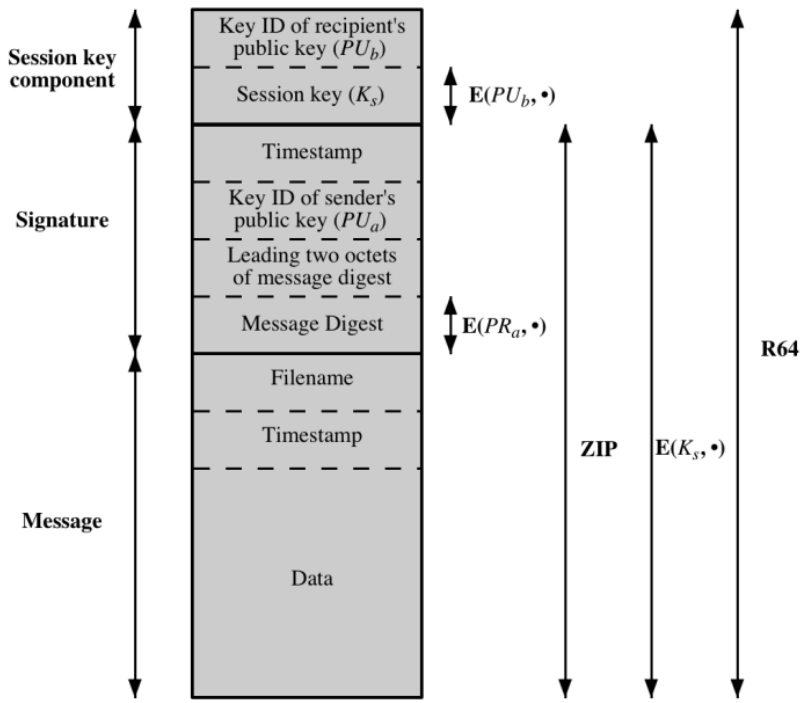
Figure 5.1 PGP Cryptographic Functions



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Figure 5.2 Transmission and Reception of PGP Messages



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 5.3 General Format of PGP Message (from A to B)

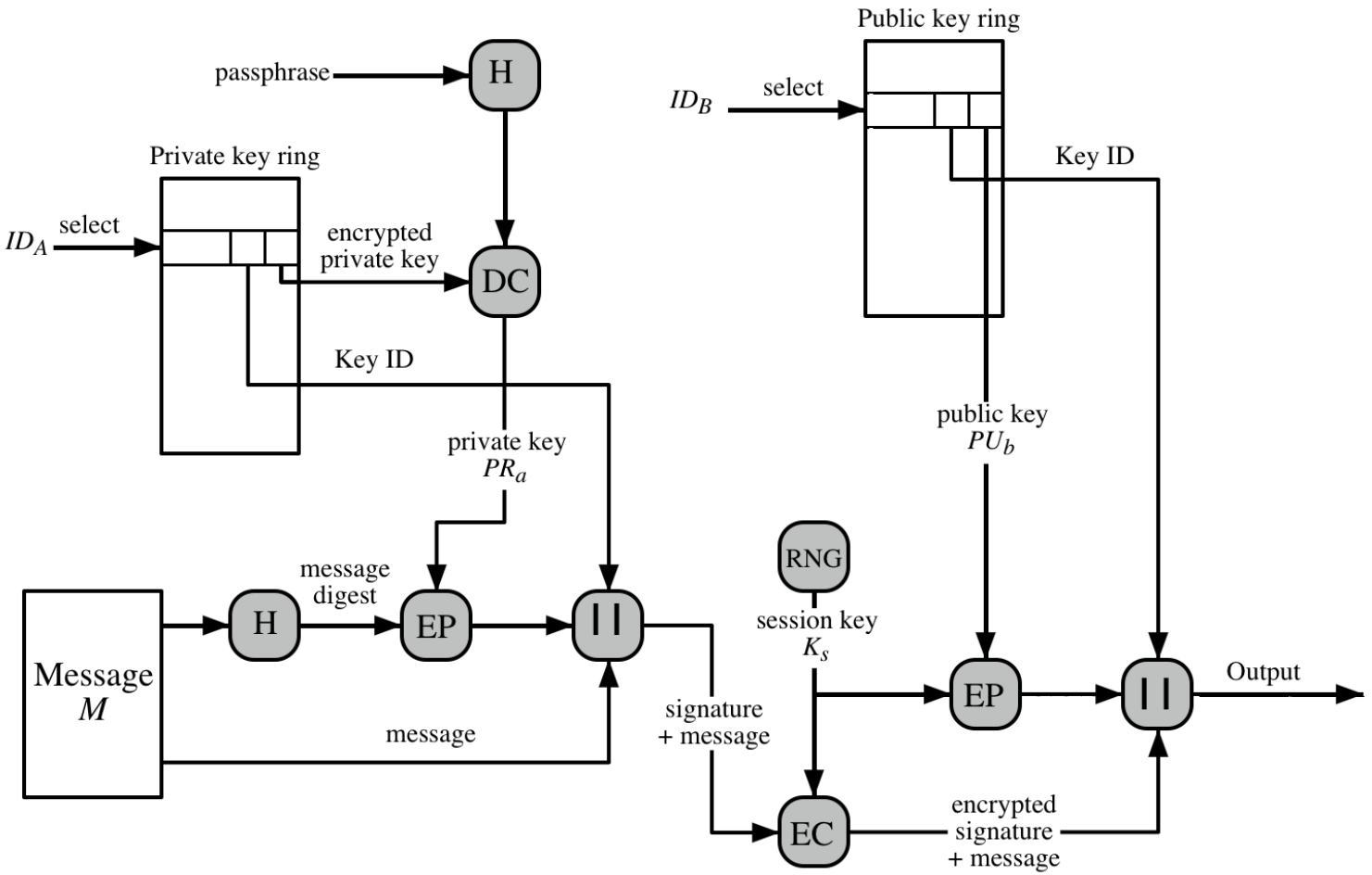


Figure 5.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

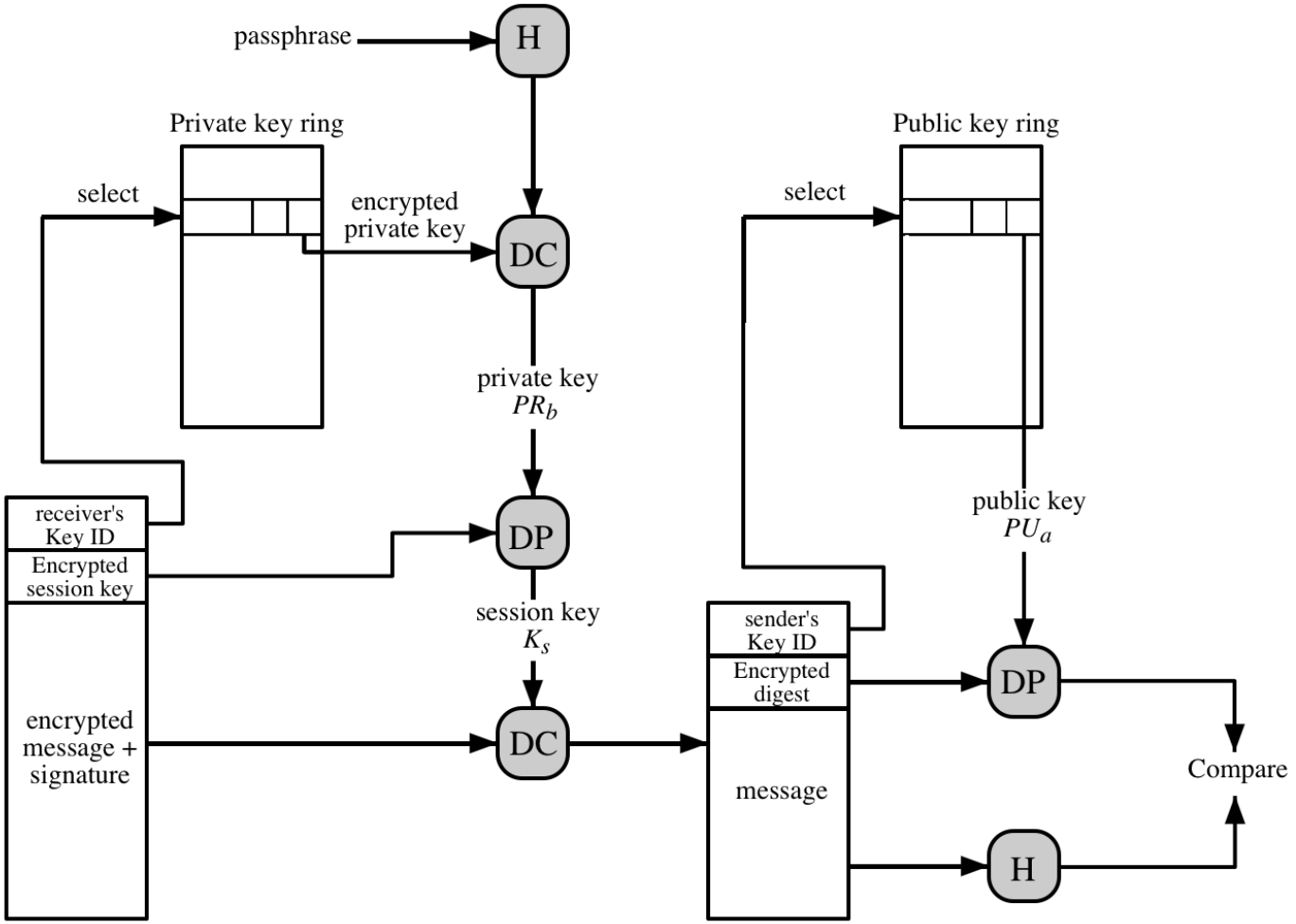


Figure 5.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

S/MIME

- Secure Multipurpose Internet Mail Extension
- Security extension to the MIME Internet email format
- What is the trust model?
  - Hierarchical, top-down
  - X.509 certificates