

ECE 646 - Lecture 4

Key management

Pretty Good Privacy

1

Project, Next Steps

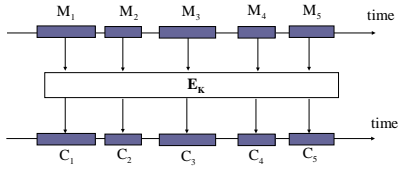
- Due Today: Initial project choice and reference list
- Sept 26: Group building finished and final project choice
- Discussions of groups with instructor
- Oct 3: Project specifications due

2

Key Management

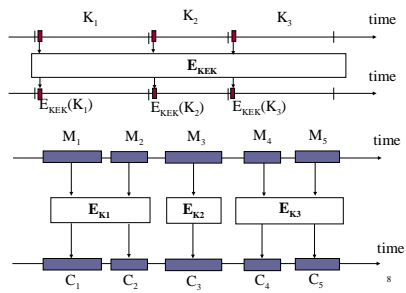
6

Using the same key for multiple messages



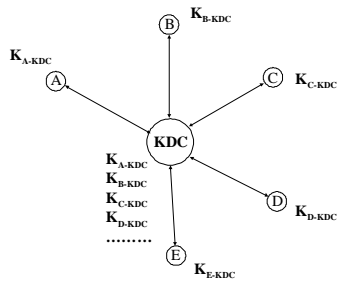
7

Using Session Keys & Key Encryption Keys

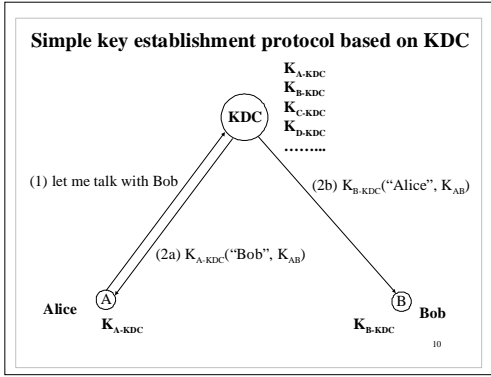


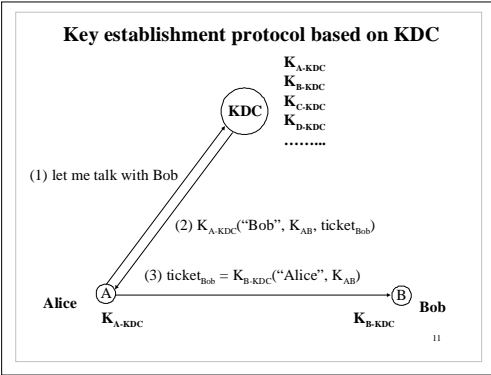
8

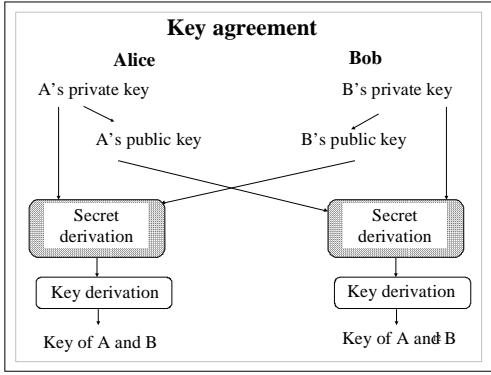
Key Distribution Center (KDC)

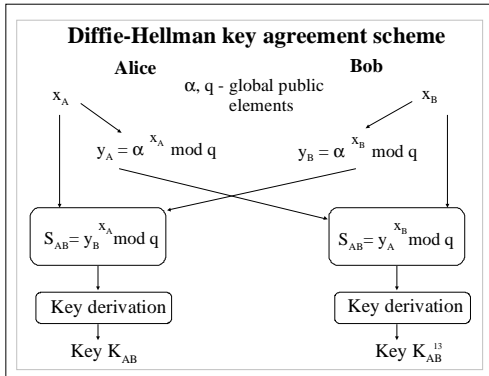


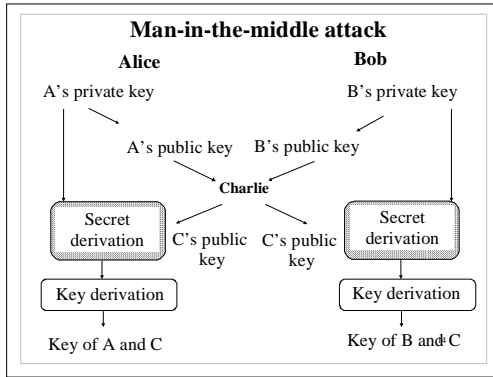
9

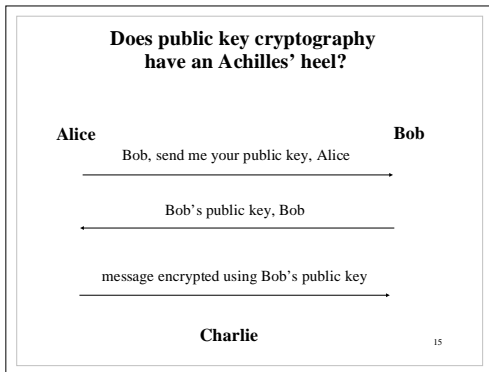


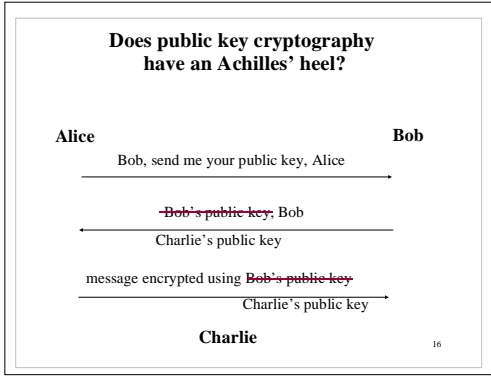


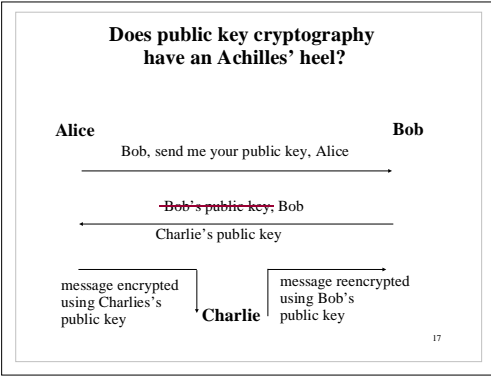


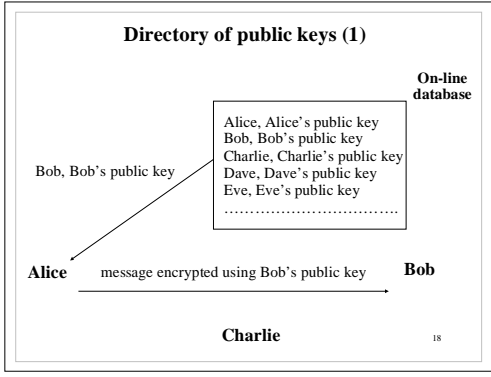


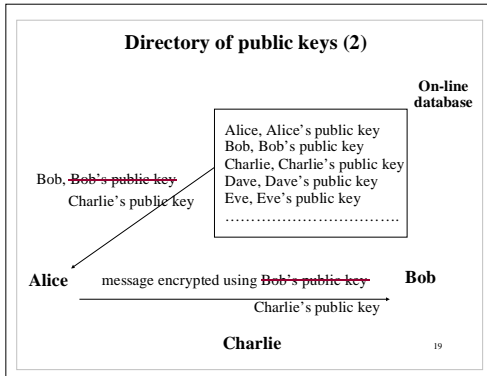


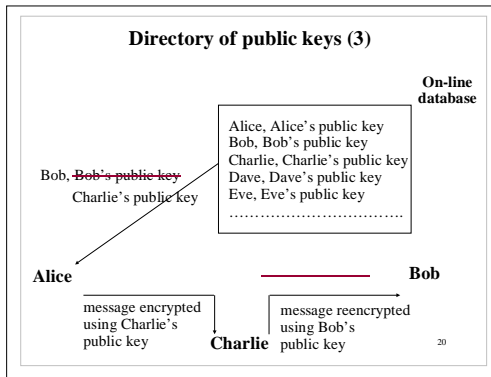


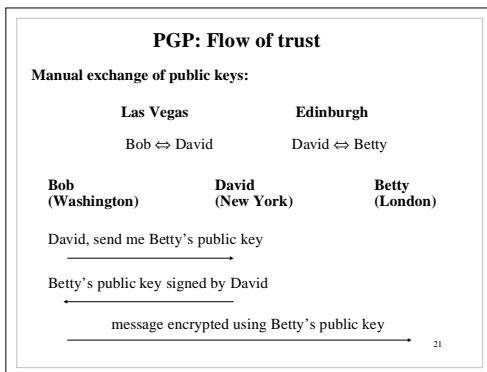


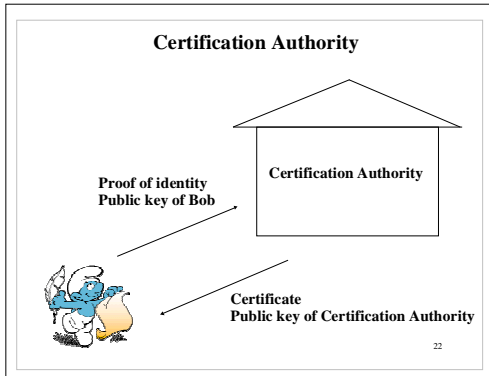


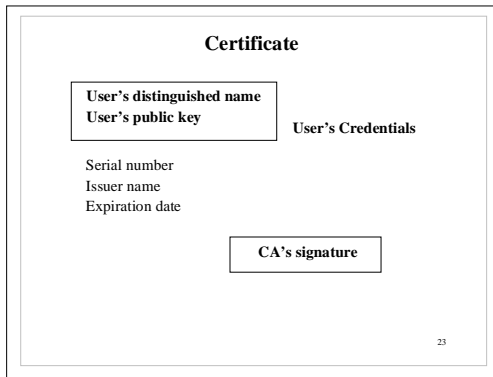


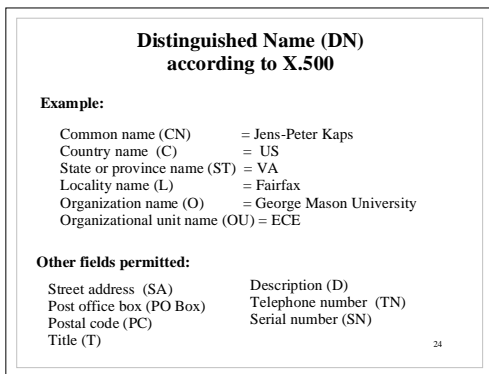


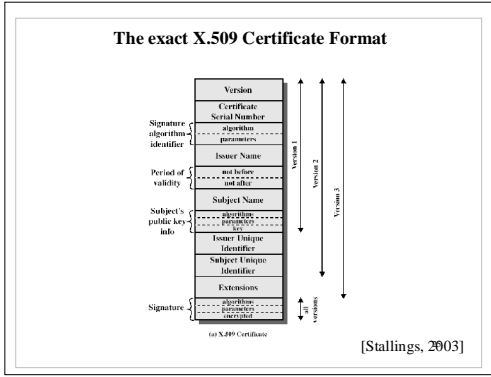


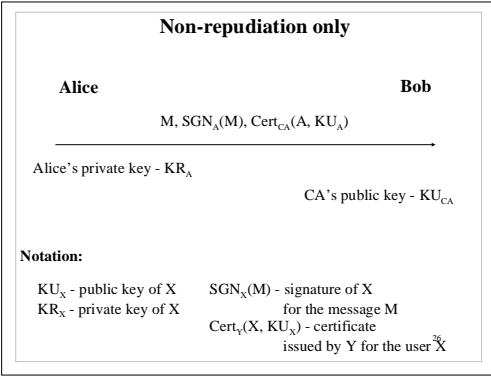


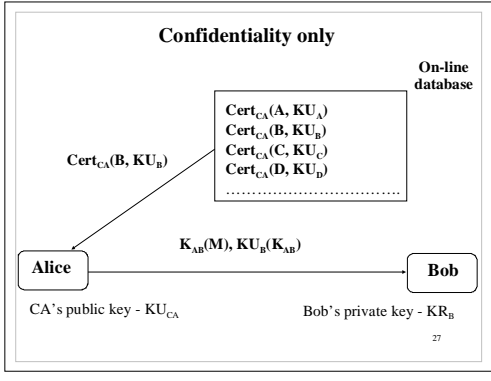


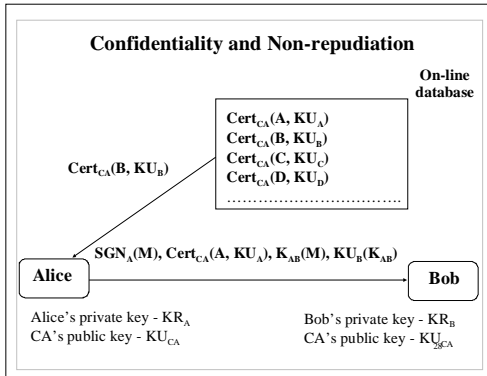


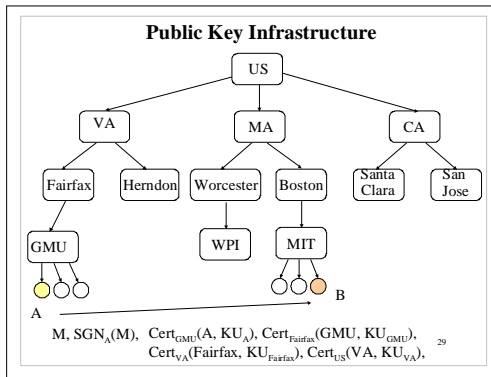












VeriSign Public-Key Certificate Classes

| | Summary of Confirmation of Identity | IA Private Key Protection | Certificate Applicant and Subscriber Private Key Protection | Applications Implemented or Contemplated by Users |
|----------------|--|--|---|--|
| Class 1 | Automated unambiguous name and E-mail address search | PCA trust-worthy hardware; CA trust-worthy software or trust-worthy hardware | Encryption software (PIN protected) recommended but not required | Web-browsing and certain e-mail usage |
| Class 2 | Same as Class 1, plus automated enrollment information check plus automated address check | PCA and CA trust-worthy hardware | Encryption software (PIN protected) required | Individual and intra- and inter-company E-mail, online subscriptions, password replacement, and software validation |
| Class 3 | Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check. For individual (business records (or filings) for organizations) | PCA and CA trust-worthy hardware | Encryption software (PIN protected) required; hardware token recommended but not required | E-banking, corp. database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation; authentication of LERAs; and strong encryption for certain servers |

IA - Issuing Authority
CA - Certification Authority
PCA - VeriSign public primary certification authority
PIN - Personal Identification Number
LERAs - Local Registration Authority Administrator

[Stallings, 2003]

Certificate Revocation Lists (CRLs)

Issue time
Issuer (CA's) name
Serial numbers of revoked certificates

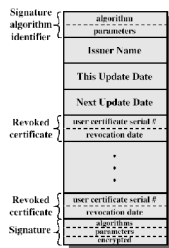
CA's signature

Certificate is valid if

- it has a valid signature of CA
- did not expire
- is not listed in the CA's most recent CRL

31

The exact X.509 CRL Format



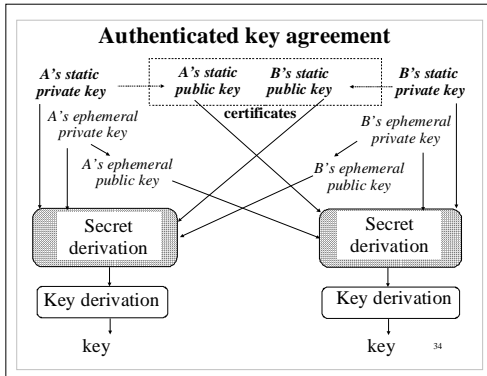
(a) Certificate Revocation List

[Stallings, 2003]

Advantages of Certification Authorities over Key Distribution Centers

- CA does not need to be on-line
- CA is relatively easy to implement
- CA crash = no new users in the network but all old users operate normally
- certificates are not security sensitive, they can be stored in a public database, and transmitted over a public network
- compromised CA cannot decrypt messages (without first impersonating one of the users) only active attacks can be mounted using CA's private key

33



Pretty Good Privacy PGP

35

Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
 - may be inspected either in transit
 - or by suitably privileged users on destination system

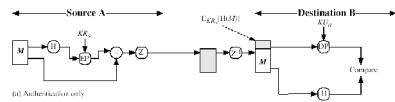
36

Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- selected best available crypto algs to use
- integrated into a single program
- available on Windows, Unix, Macintosh, and other systems
- originally free, now have commercial versions available also

37

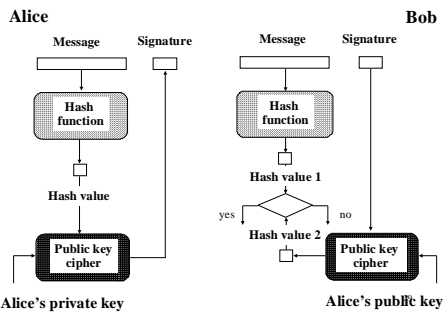
PGP – Authentication Only



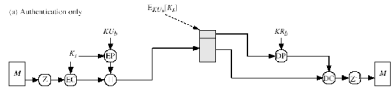
Notation: M - message
 H - hash function
 EP - public key encryption
 || - concatenation
 Z - compression using ZIP algorithm
 KR_A - private key of user A
 KU_A - public key of user A

38

Non-repudiation



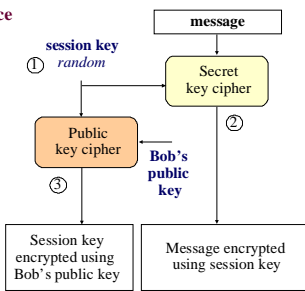
PGP – Confidentiality Only



Notation: M - message
 Z - compression using ZIP algorithm
 EC / DC - classical (secret-key) encryption / decryption
 EP / DP - public key encryption / decryption
 || - concatenation
 K_s - session key
 KR_a - private key of user B
 KU_a - public key of user B

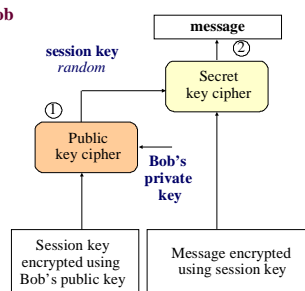
Hybrid Systems - Sender's Side (2)

Alice

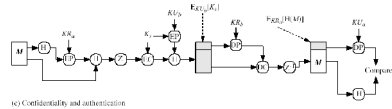


Hybrid Systems - Receiver's Side (2)

Bob

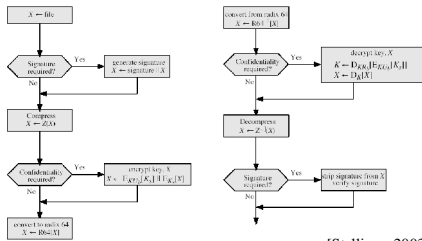


PGP – Confidentiality and Authentication



Notation: M - message
 H - hash function
 Z - compression using ZIP algorithm
 EP / DP - public key encryption / decryption
 || - concatenation
 EC / DC - classical (secret-key) encryption / decryption
 K_s - session key
 KR_a / KR_b - private key of user A / B
 KU_a / KU_b - public key of user A / B

Transmission and Reception of PGP Messages

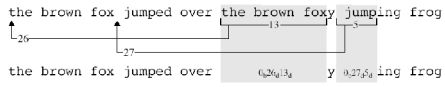


[Stallings, 2003]

PGP Operation – Compression

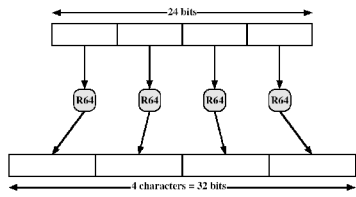
- by default PGP compresses message after signing but before encrypting
 - so can store uncompressed message & signature for later verification
 - & because compression is non deterministic
- uses ZIP compression algorithm

Major idea behind ZIP compression



[Stallings, 2003]

Radix-64 Conversion



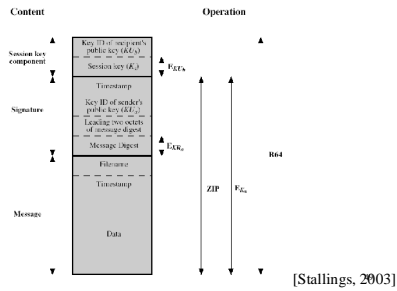
[Stallings, 2003]

Radix-64 Encoding

| 6-bit value | character encoding | 6-bit value | character encoding | 6-bit value | character encoding | 6-bit value | character encoding |
|-------------|--------------------|-------------|--------------------|-------------|--------------------|-------------|--------------------|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |
| 12 | M | 28 | c | 44 | s | 60 | 8 |
| 13 | N | 29 | d | 45 | t | 61 | 9 |
| 14 | O | 30 | e | 46 | u | 62 | + |
| 15 | P | 31 | f | 47 | v | 63 | / |
| | | | | | (pad) | 64 | = |

[Stallings, 2003]

General Format of PGP Message



Summary of PGP functions

| Function | Algorithms Used | Description |
|---------------------|--|--|
| Digital signature | DSS/SHA or RSA/SHA | A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message. |
| Message encryption | CAST or IDEA or Thalesage, Triple DES with Diffie-Hellman or RSA | A message is encrypted using CAST-128 or IDEA or IDEA with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message. |
| Compression | ZIP | A message may be compressed, for storage or transmission, using ZIP. |
| Email compatibility | Radix 64 conversion | To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion. |
| Segmentation | | To accommodate maximum message size limitations, PGP performs segmentation and reassembly. |

[Stallings, 2003]

Private Key Ring

Private Key Ring

| Timestamp | Key ID ^a | Public Key | Encrypted Private Key | User ID ^b |
|-----------|----------------------------|------------|-----------------------|----------------------|
| * | * | * | * | * |
| * | * | * | * | * |
| * | * | * | * | * |
| t_i | $KU_i \text{ mod } 2^{24}$ | KU_i | $E_{KU_i}(PK_i)$ | User i |
| * | * | * | * | * |
| * | * | * | * | * |
| * | * | * | * | * |

[Stallings, 2003]

Public Key Ring

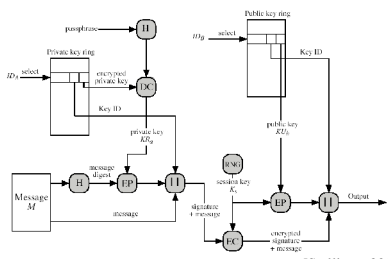
Public Key Ring

| Timestamp | Key ID* | Public Key | Owner Trust | User ID* | Key Legitimacy | Signature | Signature Trust(s) |
|----------------|-------------|------------|-------------|----------|----------------|-----------|--------------------|
| . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . |
| T ₁ | K1, user 2* | key | trust_Bug | User 1 | trust_Bug | . | . |
| . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . |

* = field used to index table

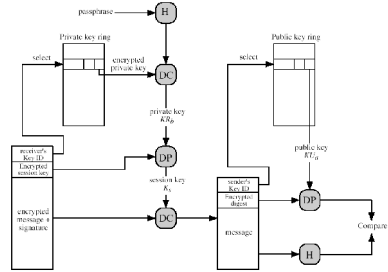
[Stallings, 2003]

PGP Message Generation (without compression or radix-64 conversion)



[Stallings, 2003]

PGP Message Reception (without compression or radix-64 conversion)



[Stallings, 2003]
