CS458/CS558: Introduction to Computer Security

Email Security

Email

- Email is one of the most widely used network-based application.
- Every user is uniquely identified by an email address: user@domain
  - User: identifies the user of a domain
  - Domain: identifies the organization or a host machine
- Using a mailbox principle
  - A sender does not require the receiver to be online.
- Currently message contents are not secure
  - May be inspected either in transit or by privileged users on destination system

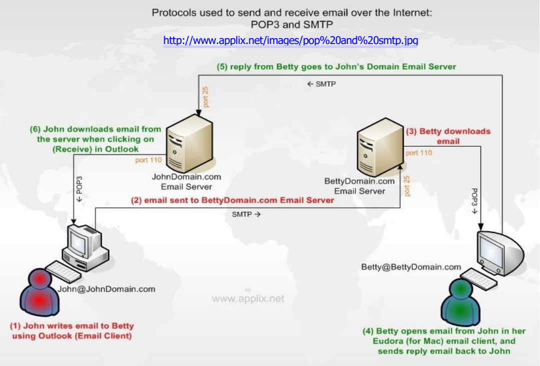
Simple Mail Transfer Protocol (SMTP)

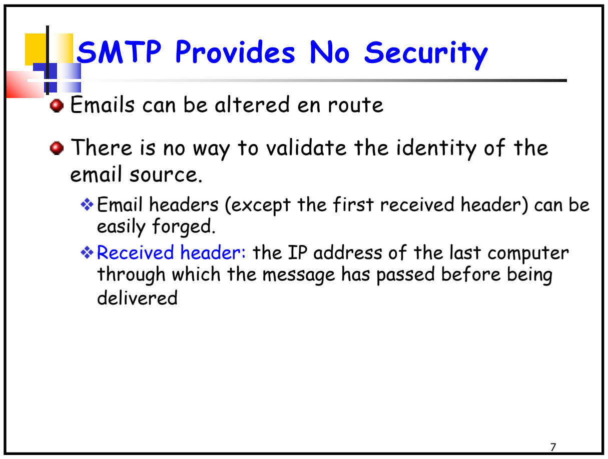
- SMTP: deliver email from the sender's email client to the recipient's email server.
  - Mails that cannot be delivered keep waiting in the spooling area
    - Client process will repeat its delivery attempts periodically
    - After several repetitions that mail will be removed from the spooling area.

POP3

- POP3 (Post Office Protocol version 3): handle email between Email Server and the recipient's local Email Client.
  - The email will stay on the recipient's email server until it is explicitly requested to be downloaded by the recipient's Email client (e.g. Outlook or Eudora) over, e.g. POP3 protocol.

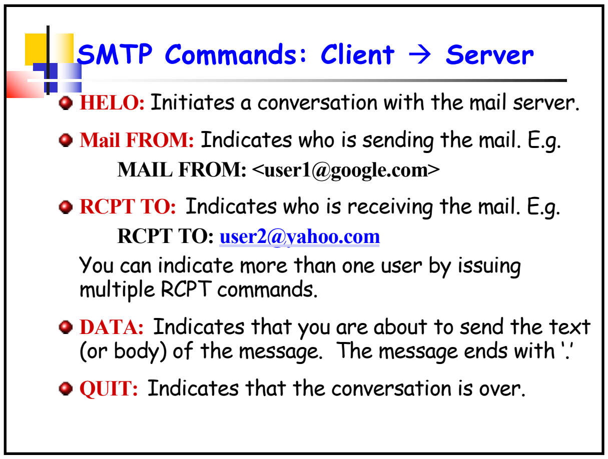
Example: SMTP and POP3


Protocols used to send and receive email over the Internet:
POP3 and SMTP
http://www.applix.net/images/pop%20and%20smtp.jpg
(5) reply from Betty goes to John's Domain Email Server
← SMTP
port 25
(6) John downloads email from the server when clicking on (Receive) in Outlook
port 110
JohnDomain.com Email Server
(3) Betty downloads email
port 110
BettyDomain.com Email Server
port 25
← POP3
POP3 →
(2) email sent to BettyDomain.com Email Server
SMTP →
John@JohnDomain.com
Betty@BettyDomain.com
by www.applix.net
(1) John writes email to Betty using Outlook (Email Client)
(4) Betty opens email from John in her Eudora (for Mac) email client, and sends reply email back to John



SMTP Provides No Security

- Emails can be altered en route
- There is no way to validate the identity of the email source.
  - Email headers (except the first received header) can be easily forged.
  - Received header: the IP address of the last computer through which the message has passed before being delivered



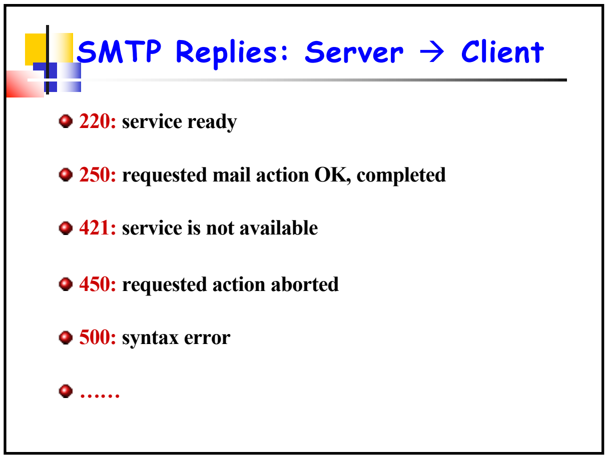
SMTP Commands: Client → Server

- **HELO:** Initiates a conversation with the mail server.
- **Mail FROM:** Indicates who is sending the mail. E.g.

  MAIL FROM: <user1@google.com>
- **RCPT TO:** Indicates who is receiving the mail. E.g.

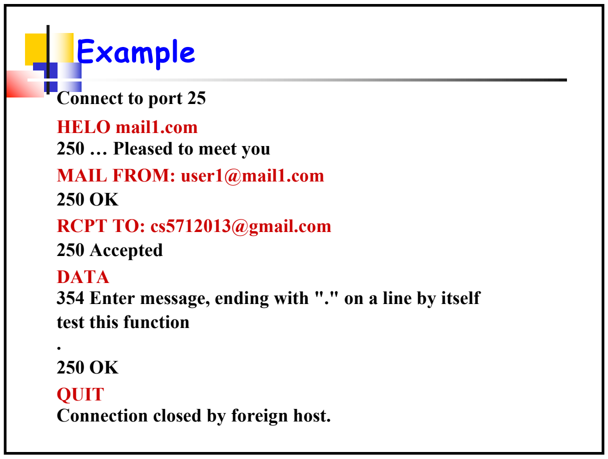
  RCPT TO: user2@yahoo.com

  You can indicate more than one user by issuing multiple RCPT commands.
- **DATA:** Indicates that you are about to send the text (or body) of the message. The message ends with '.'
- **QUIT:** Indicates that the conversation is over.



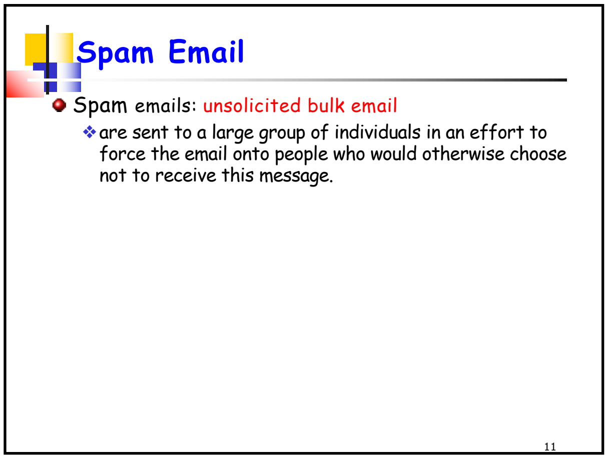
SMTP Replies: Server → Client

- **220:** **service ready**
- **250:** **requested mail action OK, completed**
- **421:** **service is not available**
- **450:** **requested action aborted**
- **500:** **syntax error**
- **……**



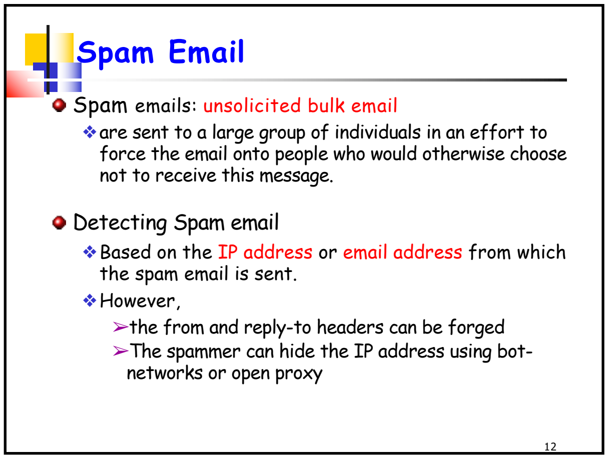
Example

```
Connect to port 25
HELO mail1.com
250 … Pleased to meet you
MAIL FROM: user1@mail1.com
250 OK
RCPT TO: cs5712013@gmail.com
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
test this function
.
250 OK
QUIT
Connection closed by foreign host.
```



Spam Email

- Spam emails: unsolicited bulk email
  - are sent to a large group of individuals in an effort to force the email onto people who would otherwise choose not to receive this message.



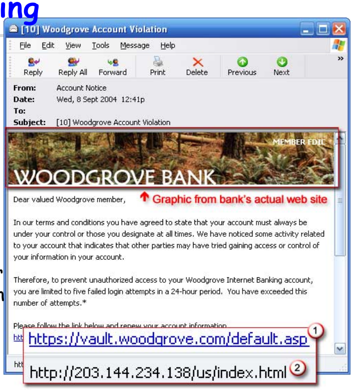
Spam Email

- Spam emails: unsolicited bulk email
  - are sent to a large group of individuals in an effort to force the email onto people who would otherwise choose not to receive this message.
- Detecting Spam email
  - Based on the IP address or email address from which the spam email is sent.
  - However,
    - ➢the from and reply-to headers can be forged
    - ➢The spammer can hide the IP address using bot-networks or open proxy

Email Phishing

Email Phishing

- Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.
- Often include official-looking logos and other identifying information taken directly from legitimate Web sites



From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation

Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

https://vault.woodgrove.com/default.asp

http://203.144.234.138/us/index.html

http://www.microsoft.com/athome/security/email/phishing.mspx?ifs=0

How to Tell If an Email is a Phishing Email

- Verify your account
  - Businesses should not ask you to send passwords, login names, SSNs, or other personal information through e-mail.
- If you don't respond within 48 hours, your account will be closed or your response is required because your account might have been compromised.
  - These messages convey a sense of urgency so that you'll respond immediately without thinking.
- Dear Valued Customer
  - Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.
- Click the link below to gain access to your account.
  - The link you see does not take you to that address but somewhere different, usually a phony Web site.

PGP (Pretty Good Privacy)

Notation

K_s = session key used in symmetric encryption scheme

PR_a = private key of user A, used in public-key encryption scheme

PU_a = public key of user A, used in public-key encryption scheme

EP = public-key encryption

DP = public-key decryption

EC = symmetric encryption

DC = symmetric decryption

H = hash function

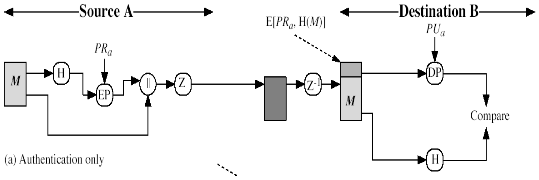
|| = concatenation

Z = compression using ZIP algorithm

R64 = conversion to radix 64 ASCII format

PGP Operation – Authentication

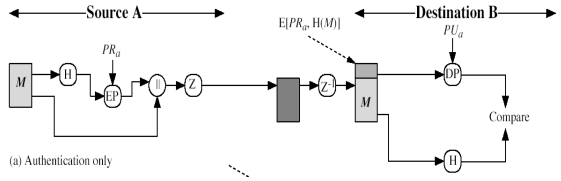
1. Sender creates message
2. Use SHA-1 to generate 160-bit hash of message
3. Signed hash with RSA using sender's private key, and is attached to message.



(a) Authentication only

PGP Operation – Authentication

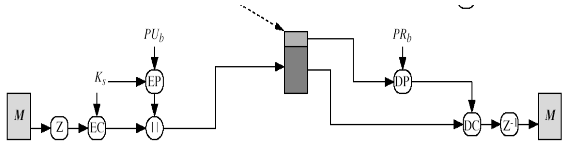
4. Receiver uses RSA with sender's public key to decrypt and recover hash code
5. Receiver verifies received message using hash of it and compares with decrypted hash code



(a) Authentication only

PGP Operation – Confidentiality

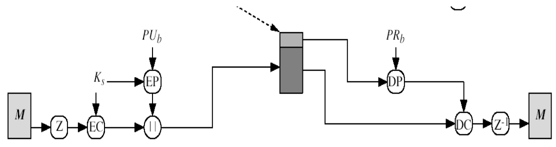
1. Sender generates message and 128-bit random number as session key for it
2. Encrypt message using Three-key Triple DES with a one-time session key generated by the sender



(b) Confidentiality only

PGP Operation – Confidentiality

3. The session key is encrypted using RSA with recipient's public key, & attached to message
4. Receiver uses RSA with private key to decrypt and recover session key
5. Session key is used to decrypt message



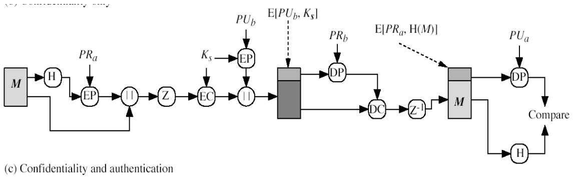
(b) Confidentiality only

Some Observations

- To reduce encryption time the combination of symmetric and public-key encryption is used in preference to simply using RSA to encrypt the message
- The use of the public-key algorithm solves the session key distribution problem.
  - Only the receiver is able to recover the session key that is bound to the message.
  - We do not need a session key exchange protocol

PGP Operation – Confidentiality & Authentication

- Can use both services on same message
  - Create signature & attach to message
  - Encrypt both message and signature
  - Attach RSA encrypted session key



(c) Confidentiality and authentication

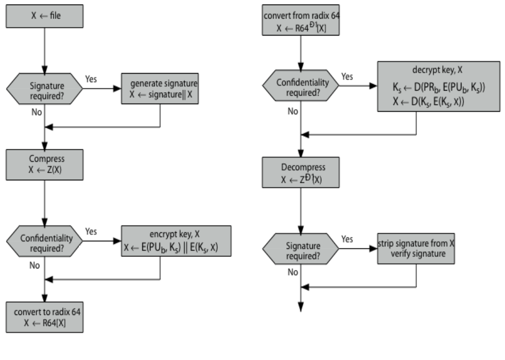
PGP Compression

- The signature is generated before compression:
  - Can store uncompressed signature for later verification
- Compression is done before encryption.
  - To speed up the process (less data to encrypt)
  - Also improves security
    - Compressed messages are more difficult to cryptanalyze.

PGP Operation – Email Compatibility

- After the above security operations, the resulting message will contain some arbitrary octets.
- However email was designed only for ASCII text
- Hence PGP must convert raw binary data into printable ASCII characters - uses radix-64 algorithm

PGP Operation – Summary



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

PGP Public & Private Keys

- A user may have multiple public/private key pairs
  - To interact with different groups of correspondents
  - Enhance security by limiting the amount of material encrypted with any one key
- Need to identify which public-key is actually used to encrypt session key in a message

PGP Public & Private Keys

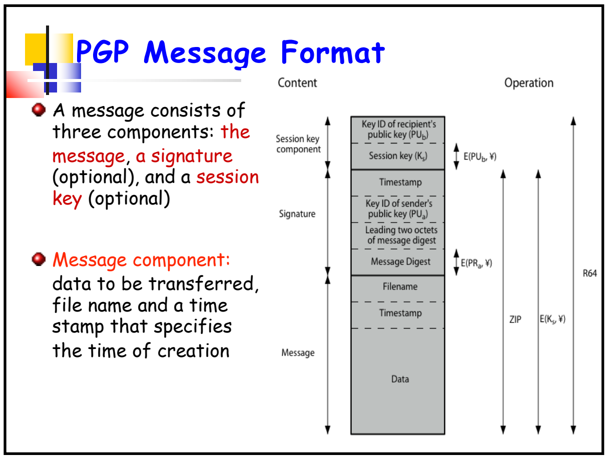
- A user may have multiple public/private key pairs
  - To interact with different groups of correspondents
  - Enhance security by limiting the amount of material encrypted with any one key
- Need to identify which public-key is actually used to encrypt session key in a message
  - Could send full public-key with every message, but this is inefficient – an RSA public key may be hundreds of decimal digits in length

PGP Public & Private Keys

- Solution: Associate an identifier with each public-key – the combination of user ID and key ID would be sufficient to identify a key uniquely.
  - Key IDs must be assigned and stored so that both sender and receiver can map from Key ID to public key
  - PGP: The key ID associated with each public-key consists of its least significant 64 bits (PU mod 2^{64}).
    - Very likely be unique

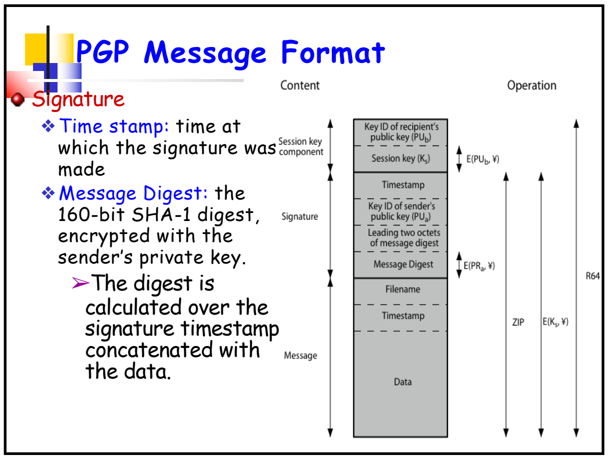
Key ID

- Key ID is also required for the PGP digital signature.
  - Sender may use one of a number of private keys to encrypt the message digest
  - Receiver must know which public key is intended for use.
  - The digital signature of a message includes the 64-bit key ID of the required public key.
  - When the message is received, the recipient verifies that the key ID is for a public key that he/she knows for that sender.



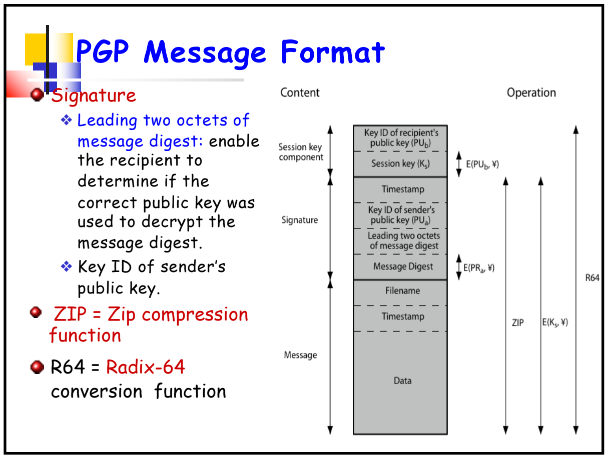
PGP Message Format

- A message consists of three components: the message, a signature (optional), and a session key (optional)
- Message component: data to be transferred, file name and a time stamp that specifies the time of creation



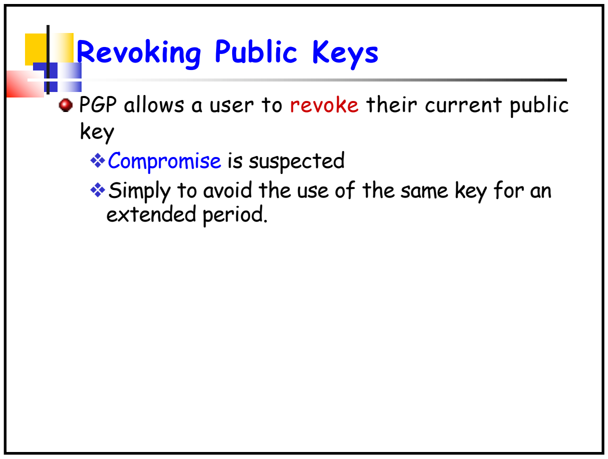
PGP Message Format

- Signature
  - Time stamp: time at which the signature was made
  - Message Digest: the 160-bit SHA-1 digest, encrypted with the sender's private key.
    - The digest is calculated over the signature timestamp concatenated with the data.



PGP Message Format

- Signature
  - Leading two octets of message digest: enable the recipient to determine if the correct public key was used to decrypt the message digest.
  - Key ID of sender's public key.
- ZIP = Zip compression function
- R64 = Radix-64 conversion function



Revoking Public Keys

- PGP allows a user to revoke their current public key
  - Compromise is suspected
  - Simply to avoid the use of the same key for an extended period.