## [3413ICT Network Security](file:///C:\Documents%20and%20Settings\s995689\My%20Documents\Teaching\Courses_2013\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 4A**

**Part 1 – Review the lecture notes and test book, answer the following questions**

|  |
| --- |
| 1. What are the five principal services provided by PGP?   1. Confidentiality: is provided using the session key that is encrypted with the public key. 2. Authentication: is provided by signing the message with a hash that is encrypted with a private key.  3. Data Compression: Zipping data after signing it and before encryption  4. E-mail compatibility  5. Segmentation |
| 1. What is the utility of a detached signature in email application?    Includes the signature and certificate without the signed data. An advantage is a message can be sent separately from the signature. |
| 1. Why does PGP generate a signature before applying compression? |
| (a) It is preferable to sign an uncompressed message so it is free of the need for a compression algorithm for later veriﬁcation.  (b) Different version of PGP produces different compressed forms. Applying the hash function and signature after compression would constrain all PGP implementation to the same version of the compression algorithm. |
| 1. Why is the segmentation and reassembly function in PGP needed? |
| This functionality is used when an e-mail exceed the maximum octet length of 50,000. When the message exceeds the maximum octet length it is split up into multiple messages and sent separately. |
| 1. What is MIME?   Originally, e-mail messages were sent over SMTP (Simple Mail Transfer Protocol) in plain text. MIME (Multipurpose Internet Mail Extensions) extended this basic functionality of sending messages and included the following features: -Text in character sets other than ASCII -Non text attachments -Multi part message bodies |
| 1. What is S/MIME?   S/MIME (Secure Multipurpose Internet Mail Extensions) adds security to MIME. It operates in a similar way that PGP works. |

1. Clearly explain, with the aid of a diagram, how the session key is exchanged in PGP.

[A] Generates and encrypts message with a session key.  
[A] Encrypts session key with public key and attaches it to message  
[A] Ships message to [B]  
[B] Decrypts session key with private key  
[B] Decrypts message with session key

1. Why key IDs are critical to the operation of PGP.

Key IDs identify which public key to use. When dealing with multiple users using different public keys it is important to identify which key to use by the least significant 64 bits in a key.

1. What are the five entries used in the private-key ring for each pair of keys.  
   Time Stamp  
   Key ID  
   Public Key  
   Encrypted Private Key  
   User ID
2. Clearly explain, with the aid of diagrams, the steps involved in the PGP message generation and PGP reception.

**Generation:**Message goes through a hash that is encrypted with a private key  
Message is joined with hash  
Message is compressed  
Session key is generated and encrypts message  
Session key is encrypted with public key  
Encrypted session key is joined with encrypted message **Reception:**Private key is used to decrypt session key  
Session key is used to decrypt message

Message goes through a hash  
Message digest is checked against message hash for Authentication

1. Explain 4 different approaches used for Public-key management in email systems.

Enveloped Data: Encrypted content of any type and encrypted content encryption keys for one or more recipients.  
Signed Data: digital signature by taking the message digest of the content and encrypting it with the private key of the signer. Content and signature are encoded using base64 encoding. A signed data message can only be viewed by a recipient of S/MIME capability.  
Clear + Signed Data: digital signature by taking message digest of the content and encrypting it with private key of the signer. Signature is signed with base64 encoding allowing non S/MIME capable can view message content. Cannot verify signature.  
Signed + Enveloped Data: Signed only and encrypted only entities may be nested so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

|  |
| --- |
| 1. What is R64 conversion? Why is R64 conversion useful for an e-mail application?   Radix 64 conversions take a stream of 24 bits and separate them into 6 bit binary groupings. Binary groups are then converted to printable ascii characters. |
|  |

**Part 2 – Challenge Exercises (Home work & presentation in the class)**

Going through the literature, identify a real world major security incident, which had happened by exploiting vulnerabilities in email systems.

In your own words (about 300 – 400 words), clearly describe the security incident, provide the reference, and explain what was the vulnerability, how it was exploited, what were the consequences, and what countermeasures were recommended.

To the class, you should be able to explain the summary in about 3 minutes.   
  
http://malware.wikia.com/wiki/Nimda

**Part 3 Additional Exercises**

Consider radix-64 conversion as a form of encryption. In this case there is no key. But suppose an opponent knew only that some form of substitution algorithm was being used to encrypt English text. How effective would this algorithm be against cryptanalysis? Explain in detail.

Using radix-64 as a form of encryption is better than a straight substitution cipher. The bit stream of the message is essentially going through substitution by breaking the original ascii letter into 6 bit chunks and then using a lookup table in radix 64 format.   
  
This cipher substitution is susceptible to brute force because the process is reversible. However it is good because it implements both confusion and diffusion and cannot be broken with letter number frequency attacks.