School of Digital Media and Infocomm Technology

### ST2504 Applied Cryptography

1. The PGP operation consists of 5 services / functions. State the 5 services

* **Digital Signature**
* **Message Encryption**
* **Compression**
* **E-mail Compatibility**
* **Segmentation and reassembly**

2. PGP email provides messages encryption. Name 3 ciphers supported by PGP

**Any 3**

* **CAST**
* **IDEA**
* **Three-key**
* **Triple DES with Diffie-Hellman**
* **RSA**

3. PGP email client uses Digital Signature to ensure non-repudiation. Describe the Signing process in PGP email client.

* **The sender creates a message**
* **PGP uses SHA-1 to generate a 160-bit hash code of the message**
* **The sender specifies the private key to be used for this operation and provides a passphrase, enabling PGP to decrypt the sender’s private key**
* **PGP encrypts the hash code with RSA using sender’s private key and the result is prepended to the message**
* **The receiver uses RSA with the sender’s public key to decrypt and recover the hash code**
* **The receiver generates new hash code. If the two matches, the message is accepted as authentic**

4. PGP email client could be used to ensure confidentiality. Assuming all keys have been generated and exchanged, describe how the message is exchanged securely.

* **The sender generates a message and a random 128-bit number to be used as a session key for this message only**
* **The message is encrypted, using CAST-128 (or IDEA or 3DEAS) with the session key**
* **The session key is encrypted with RSA, using the recipient’s public key, and is prepended to the message**
* **The receiver uses RSA with its private key to decrypt and recover the session key**
* **The session key is used to decrypt the message.**

5. Radix-64 is used by PGP application to convert binary (bytes) to printable ASCII characters. True / False

1. **The binary input is split into blocks of 24 bits (3 bytes)**
2. **Each 24 block is then split into four sets each of 6-bits**
3. **Each 6-bit set will then have a value between 0 and 2^6 – 1 (=63)**
4. **This value is encoded into a printable character**

6. Radix-64 is also known as Base64. True / False

**False – They have similar function, but they are not compatible.**

7. Order the following PGP operations (first = 1, last = 5)

1. Exchange public keys with others
2. Sign and encrypt your email and files
3. Decrypt and verify your email and files
4. Validate your keys
5. Create a private and public key pair

**e, a, d, b, c**