**• In the ACS Code of Ethics, which among the following has the highest priority:**

Confidentiality

Integrity

**The public interest**

Competence

**• In the ACS Code of Ethics, which among the following has the lowest priority:**

Confidentiality

Integrity

Competence

**The image of the profession and the society**

**• An example of a *passive* attack is:**

**Traffic analysis**

Replay

Denial of service

**• An example of an asymmetric key algorithm is:**

**RSA**

AES

DES

**• How many bits are in a DES block?**

64

**56**

128

**• When encrypting a signed message to ensure confidentiality, which key is used?**

sender’s public key

sender’s private key

receiver’s public key

**receiver’s private key**

**• Hashing a message provides the following service:**

confidentiality

**integrity**

authentication

**• An example of a symmetric key algorithm is:**

MD5

**DES**

SHA1

**• When signing a message using RSA, which key is used?**

sender’s public key

sender’s private key

receiver’s public key

**receiver’s private key**

**• Digital signature using RSA provides the following service:**

Confidentiality

Integrity

**Authentication**

**• How many keys are used in a symmetric key algorithm?**

**One** secret key for encrypting the message. Then use the secret key for decrypting the ciphertext.

**• Why are hash functions used to generate digital signatures?**

Without using hash functions, signatures could get very **long according to the length of messages**

**• How will a receiver verify a message signed using RSA, when no hash function is used in generating the signature?**

Decrypt the signature with the **sender’s public key** and compare it with the received message if they are identical.

**• How will a sender sign a message using RSA, when a hash function is used in generating the signature?**

**• Why are session keys usually symmetric keys?**

**• Name one issue with symmetric key cryptosystems.**

Need a secure channel for secret key exchange

Too many keys to keep track

Origin and authenticity of message cannot be guaranteed.

**• Name one issue with asymmetric key cryptosystems.**

Encryption/decryption much slower (higher computational cost) than symmetric cryptosystems.

When used for signing, both encrypted message and original message required for signature verification.

**• In the ACS Code of Ethics, which among the following has the highest priority?**

Confidentiality

**Integrity**

Competence

Promoting information technology

**• When decrypting a signed message using RSA, which key is used?**

**sender’s public key**

sender’s private key

receiver’s public key

receiver’s private key

**• An example of a symmetric key algorithm is:**

RSA

**AES**

El Gamal

**• How many bits are in a DES key?**

64

**56**

128

**• Why are public keys normally used to encrypt session keys?**

To overcome the key distribution problem associated with the distribution of symmetric keys (session keys are normally symmetric keys). This approach allows a sender to securely transmit a session key encrypted with the receiver's public key, to the receiver.

**• Encryption using AES provides the following service:**

**confidentiality**

integrity

authentication

**• How will a receiver verify a message signed using RSA, when a hash function is used in generating the signature?**

When a hash function is used to generated the signature, the receiver will (should) receive a signed hash plus the original message. The receiver will use the sender's public key to decrypt the signed hash, thus obtaining the actual hash, say H(m). The receiver will then run the same hash algorithm that the sender used over the original message to get its hash, say H(m)'. If the two hashes are the same (H(m) equals H(m)'), then the signature is verified.