Daniel Meyer

0405182

CSIS 202-1008

**Week 16 Homework**

**Review Questions:**

**R1)** Message confidentiality ensures messages are kept from those not involved in the communication and that eavesdroppers are kept out. Message integrity on the other hand, involves the contents of the communication and that it remains unaltered. As such you cannot have integrity without confidentiality because if the message is altered then someone was able to see the message and modify it. You can however, have integrity without confidentiality if someone were to simply observe the communications, but not tamper them.

**R2)** Examples of Internet entities that would want secure communications include Chase Online Banking (keep bank accounts and money transfers secure), Skype (secure web communications, both audible, text, and visual), and Amazon (user purchases, addresses, credit cards).

**R3)** From a service’s perspective the key difference between public and symmetric key systems is how many of the keys are known to each user. In the case of public, does each user know of a common key and one the other does not, and in the case of symmetric, does each user know the same keys as one another.

**R4)** If an intruder had both the encrypted and decrypted versions of a message they could launch a known-plaintext attack.

**R5)** In an 8-block cipher there are 256 (2^8) possible inputs and 256! possible mappings and the same number of possible keys.

**R6)**

**R7)** (a \* b) mod *n* = 92

**R8)** 1010111 in decimal is 175

**R9)** Hash provides better integrity than a checksum because for one, a checksum can have multiple correct values allowing for a different message to still pass off as being correct.

**R10)** If you “decrypt” the hash of a message you will not get the original message. This is because the rehashed value can vary as it will often be a different size than the original text or produce an all-new hash value.

**R11)**  The (m, H(m) + s) variation isn’t flawed because the MAC now doesn’t include a hash of the secret, leaving the authentication key, s, vulnerable.

**R12)** A signed document is considered verifiable and non-forgeable because when it is signed, the signature is the private key that can only be used by the one who signed it (assuming the private key hasn’t been given away or stolen) and its verifiable because by applying the public key of the one who signed it to the signature will reveal the original message.

**R13)**

**R14)** True, the certified certificate for foo.com would contain the public key of certifier.com.

**R15)** In the situation where thousands will want to verify the integrity of a message, MAC would be more effective than a digital signature as each user doesn’t need to know where the message is coming from simply that it hasn’t been modified.

**R16)** A nonce is used in an end-to-end protocol to prevent playback attacks where a malicious user who copied a previous identification will try to copy it and send a false communication will be unable to because a nonce is a onetime use number, that if received again will prevent the communication.

**R17)** Nonce being a one in a lifetime value means that it will never be used again by that protocol while it is in use.

**R18)** The message integrity scheme based on HMAC is indeed still susceptible to playback attacks because the MAC can be copied along with the message, however by adding a nonce to the message could prevent this by adding a second layer of protection preventing a second message with identical credentials from passing.

**R19)** In PGP, a messages source is verified by each user certifying that each key belongs to one another by signing the others public key with their own private key. It does not use MAC for message integrity.

**R20)** False, in the SSL record there is no field for sequence numbers, but they are instead handled during MAC calculation.

**R21)** During the SSL handshake nonces are sent by the client and server to prevent a connection replay attack where multiple identical messages can be sent and still receive replies if it were not for the nonces.

**R22)** False, the block cipher will prevent the IV.

**R23)** During step 3 of the handshake is when Bob will discover he is not actually communicating to Alice because the certificate will be verified and an old nonce will be found.

**R24)** False, once an SA is created it is held for the duration of the communication.

**R25)** False, when retransmitting the ESP header will be reassembled with a new sequence number each time.

**R26)** An IKE and IPsec SA aren’t similar because an IPsec SA in unidirectional whereas an IKE SA is bi-directional.

**R27)** The resulting ciphertext of the data 10101100 and the keystream 1111000 is 1110111010100.

**R28)** False, because there are only 2^24 unique keys that WEP can use.

**R29)** Stateful Packet filters monitor TCP connections and connection tables. It monitors the beginning and end of connections by observing the three-way handshake when a connection is established and searches for the FIN packet when a connection is ended. When monitoring connection tables, it can observe ongoing connections and block packets that aren’t a part of a current connection.

**R30)** True, traditional packet filters can filter packets based on their TCP flag bits.

**R31)** False, a traditional packet filter doesn’t allow for each interface to have its own access control list.

**R32)** In order for an application gateway to be effective, it needs to be paired with a router filter because the application gateway needs to check the router filter to see if a user has permission to do what they are try to do and if so, allow the packet to pass through the gateway, if not, it will block it.

**R33)** False, signature-based IDSs and IPSs inspect the payloads of the entire packet.