1 a. What are the differences between message confidentiality and message integrity?

Message confidentiality means that the plaintext message being sent is only known by the sender and the recipient. Message integrity means the receiver can detect whether the message sent (whether encrypted or not) was altered in transmission.

b. Can you have confidentiality without integrity? Explain.

I can. Because an encrypted message altered in transmit may still be confidential, ie, the attacker cannot determine the original plaintext but will not have message integrity if there is undetected error.

c. Can you have integrity without confidentiality?

I can. Because the exchanged message could be public yet only end knows A hash knows the hash sum/hash function provides integrity without offering confidentiality could authenticate the message, ie, we share downloadable files and provide data integrity using md5 hash sums.

2 a. In what way does a cryptographic hash function provide a better message integrity check than a checksum (e.g., Internet checksum)?

A collision means there is more than one way to produce the same sum. Let say H() be a hash function. The two messages, x and y could get the same hash result. Let's say H(x) = H(y) then there is a collision which should be avoided. A Hash provides better message integrity because it has less collisions than checksum to better check whether the message has altered in transmission (the two different messages x and y are needed to be distinguishable).

b. Can you "decrypt" a cryptographic hash of a message to recover the original message? Explain your answer.

No. A hash may not be reversed, thus, it cannot be decrypted.

c. Should you ever use MD5 as a cryptographic hash function for any security-critical applications? Why or why not?

No. Because 1) MD5 is the one of the most vulnerable hashing algorithms because of collision vulnerability and 2) MD5 is fast hash that it is okay for an attacker tries millions of password per second.

d. Should you ever use SHA-1 as a cryptographic hash function for any security-critical applications? Why or why not?

No. Because 1) SHA-1 is also the one of the most vulnerable hashing algorithms because of collision vulnerability and 2) SHA-1 is also fast hash that it is okay for an attacker tries millions of password per second. 3) SHA-2 provides better encryption, algorithm and certificate.

3 a. What are the modulus N and Euler's totient Φ(N)?

n = pq = 55, z = (p-1)(q-1) = 40

[(a mod n) · (b mod n)] mod n = (a · b) mod n

For a positive integer n, two integers a and b are said to be congruent modulo n, as written: $a \equiv b\ (mod\ n)$

If their difference a − b is an integer multiple of n (or n divides a − b). The number n is called the modulus of the congruence, as for example 38-14 is 2*12 thus,
$38 \equiv 14\ (mod\ 12)$

Euler's Totient Φ(n) for an input n is count of numbers in {1, 2, 3, …, n} are relatively prime to n.

Φ(5) = 4
gcd(1, 5) is 1, gcd(2, 5) is 1,
gcd(3, 5) is 1 and gcd(4, 5) is 1

b. Let public exponent e = 3. Why is this an acceptable public exponent?

It is acceptable e = 3 is because it is less than n and it has no common factors with z

c. Find private exponent d such de = 1 mod Φ(N) and d < 160.

27

d. Encrypt the message m = 8 using public key (e, N) . Show the resulting cipher text

m = 8, me = 512, cipher text c= me mod n = 17

4 a. What is the purpose of the client and server random nonces in the SSL handshake?

The purpose of random nonces in the SSL handshake are
1. server authentication
2. client authentication
3. setup encryption algorithms
4. establish keys
5. defend against Playback Attack.

b. Suppose an SSL session employs a block cipher with cipher block chaining mode. Should the server send the initialization vector in the clear? Why or why not?

Yes, because it maintains the server key. In Cipher Block Chaining encryption, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol and the final ciphertext block is preserved.

c. Suppose Alice and Bob are communicating over an SSL session. Suppose an attacker, who does not have any of the shared keys, inserts a bogus TCP segment into a packet stream with correct TCP checksum and sequence numbers (and correct IP addresses and port numbers). Will SSL at the receiving side accept the bogus packet and pass the payload to the receiving application. Why or why not?

No, the bogus packet stream will not pass the integrity check.

5 a. Stateful packet filters maintain two data structures. Name them and briefly describe what they do.

Name: track connection setup (SYN), teardown (FIN)

Name: track connection setup
What they do: filter table and connection

Name: teardown
What they do: timeout inactive firewall connections or stop the packet admission

b. Why must an application gateway work in conjunction with a router filter to be effective?

The reason they combine essentially is for the increase in security level and flexibility than if either were used alone. Host runs proxy service an application gateway. Packet filtering routers do not allow TELNET and FTP connections

Packet filters	Application Gateway
Simple and least secure	Most secure approach
Many routers provide this functionality	Unique program for each application
Passes or rejects packets based on rules	good for authentication and logging
Hard to manage	Not always transparent to users
Easy to make mistakes	Used for email, FTP, TELNET, WWW

Source: http://www.rfwireless-world.com/Terminology/Application-Gateway-Vs-Circuit-Level-Gateway.html