CSS322 – Quiz 3 Answers

Name: _____

ID: _____ Mark: _____ (out of 10)

Question 1 [2.5 marks]

Clearly show any calculations, assumptions and/or explanations. Assume operations other than encryption and decryption are very fast (i.e. consume 0 time). Assume 2^{10} bytes = 1 Kbyte, 2^{20} bytes = 1 Mbyte and 2^{30} bytes = 1 GByte.

A symmetric block cipher called *S* operates in a block size of 48 bits and a key size of 32 bits. Assuming your computer can perform encryption (or decryption) operations at a rate of 2^{20} [or 2^{22}] per second:

a) How long would an average brute force attack take? [0.5 mark]

Answer
On average, with a brute force attack on the key we need to try half of the possible keys. With 2^{32} possible keys that means 2^{31} attempts (decryptions). At a rate of 2^{20} decryptions per second, then the average brute force attack would take 2^{11} seconds = 2048 seconds (about 34 minutes).
[Alternate answer (2^{22}): 512 seconds]

If the cipher is modified to be *Double-S*, so that for encryption two succesive encryptions with S are performed (each with a different 32 bit key), then:

b) How long would an average meet-in-the-middle attack take (assuming the attacker has a plaintext/ciphertext pair)? [1 mark]

Answer
Although the actual key size has doubled (64 bits), a meet-in-the-middle attack means the attacker tries all possible keys on the known plaintext and then attempts the keys for the known ciphertext. The average number of operations is: 2^{32} (all decryptions) + 2^{31} (half encryptions). This would take: $2^{12} + 2^{11}$ = 6144 seconds.
[Alternate answer (2^{22}): 768 seconds]

c) Approximately how much memory would your computer neet to perform the meet-in-the-middle attack? [1 mark]

Answer
The problem with meet-in-the-middle attack is at least all 2^{32} possible ciphertexts must be stored in memory for comparative purposes. Each ciphertext is 6 bytes, therefore at least 6 x 2^{32} bytes = 6 x 4 Gbytes = 24 GBytes of memory is needed.
[Alternate answer (2^{22}): 24 GBytes]

Question 2 [3 marks]

True or false:

a) A practical way of increasing the length of the sequence of unique pseudo-random numbers generated by the Linear Congruential Generator $X_{n+1}=(aX_n+c)mod(m)$ is increasing the value of *m*. **True** False

b) A practical way of increasing the length of the sequence of unique pseudo-random numbers generated by the Linear Congruential Generator $X_{n+1}=(aX_n+c)mod(m)$ is increasing the value of X_0. True **False**

c) RC4, DES in Output Feedback (OFB) Mode and AES in Counter (CTR) Mode can all produce a stream-cipher output. True **False**

d) RC4, DES in Output Feedback (OFB) Mode and AES in Cipher Feedback (CFB) Mode can all produce a stream-cipher output. **True** False

e) If link-level encryption is applied in every link in a path from source to destination, it is practically impossible for an attacker, who has physcially access to one of the routers in the path, to obtain the plaintext message. True **False**

f) If end-to-end encryption is applied between source to destination, it is practically impossible for an attacker, who has physcially access to one of the routers in the path, to obtain the plaintext message. **True** False

Question 3 [4.5 marks]

a) Assume symmetric key encryption will be used to provide confidentiality for electronic communications between a student and their academic advisor within the School of ICT. There are 20 [or 15] advisors, each with 30 advisees (students) within the School. What is the minimum number of keys needed in the system? [1 mark]

Answer
Each advisor needs a unique key for each student. Hence each advisor has 30 keys, meaning a total of 20 x 30 = 600 keys. Or in other words, since every student only needs a single key (for their advisor), the number of keys equals the number of students (600).
[Alternate answer (15 advisors, 30 students): 450 keys]

Assume the system is extended so that any student or advisor can confidentality communicate with any other student or advisor.

b) If the system used a Key Distribution Centre, how many master keys are needed in the system? [1 mark]

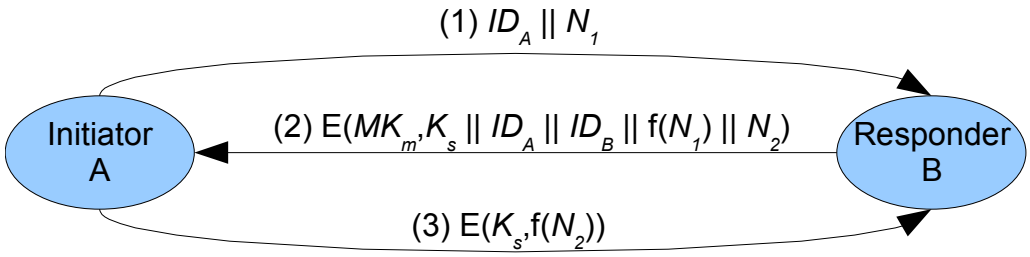
Answer
Now there are effectively 620 users. With a centralised KDC, a single master key is shared by the KDC and each user, meaning 620 master keys.
[Alternate answer (15 advisors, 30 students): 465 keys]

c) If the system is full distributed (de-centralised), how many master keys are needed in the

system? [1 mark]

Answer
With 620 users in a distributed system, a total of 620x619/2 master keys are needed. 191,890 keys
[Alternate answer (15 advisors, 30 students): 107,880 keys]

Below is an example de-centralised key distribution protocol that may be used. MK_m is the master key shared between A and B, and K_s is the session key to be used for encryption only during this session.



Assume A and B successful completed the key distibution one hour ago. However the attacker intercepted all three messages. Now A initiates a new session using the key distribution protocol (sending message (1)).

d) If an attacker C intercepts message (1) and replays message (2) to A, explain how the attacker can be detected. Note that, with C intercepting the messages, B does not receive any messages. [1.5 marks]

Answer
In the first (successful) interaction with B, A should have chosen a random nonce N_1. When A sent the second initial message (1) it should choose a different nonce, say N_1'. Therefore, when A receives the replayed message (2) and successfully decrypts the message, then A will notice that $f(N_1)$ which is included in the message does not match the expected $f(N_1')$. Hence A detects a replay attack.

It is possible that if A receives message (2) and detects the same session key as previous, then it assumes a replay attack. This assumes B will not re-use the same session key, which may not be realisitc in some scenarios (i.e. sometimes, B may want to use the same session key).