CSS322 – Quiz 3

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} per second:

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

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]

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

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

c) 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

Question 3 [4.5 marks]

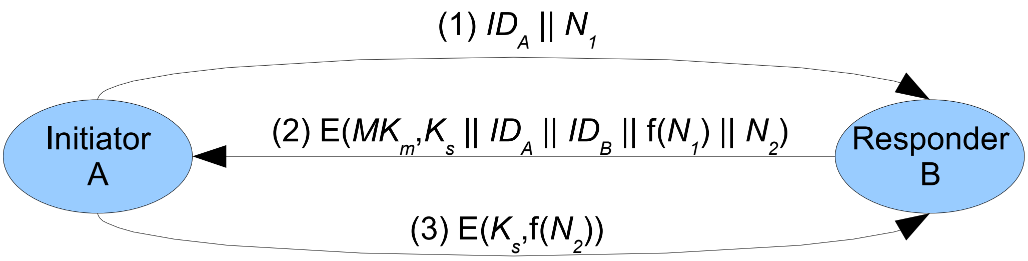
a) Assume symmetric key encryption will be used to provide confidentiality for electronic communications between a student and their academic advisor within the School of ICT. There are 20 advisors, each with 30 advisees (students) within the School. What is the minimum number of keys needed in the system?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

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]

c) If the system is full distributed (de-centralised), how many master keys are needed in the system? [1 mark]

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]