SIIT CSS322

CSS322 - Quiz 3

Name:		
ID:	Mark:	(out of 10)
Question 1 [2.5 marks]		
Clearly show any calculations, assumptions an encryption and decryption are very fast (i.e. co = 1 Mbyte and 2^{30} bytes = 1 GByte.		
A symmetric block cipher called <i>S</i> operates in Assuming your computer can perform encryptisecond: a) How long would an average brute force	ion (or decryption) operation	
If the cipher is modified to be <i>Double-S</i> , so that performed (each with a different 32 bit key), the b) How long would an average meet-in-the plaintext/ciphertext pair)? [1 mark]	ien:	
c) Approximately how much memory wormiddle attack? [1 mark]	uld your computer neet to	perform the meet-in-the-

Quiz 3 15 Dec 2008 1

SIIT CSS322

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 X_0 .

True False

- b) RC4, DES in Output Feedback (OFB) Mode and AES in Cipher Feedback (CFB) Mode can all produce a stream-cipher output. True False
- c) 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 15 advisors, each with 30 advisees (students) within the School. What is the minimum number of keys needed in the system? [1 mark]

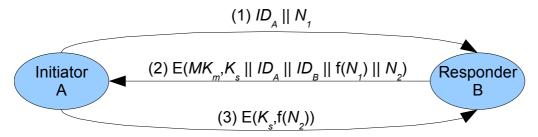
Assume the system is extended so that any student or advisor can confidentality communicate with any other student or advisor.

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]

SIIT CSS322

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 distribution 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]