

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^{22} per second:

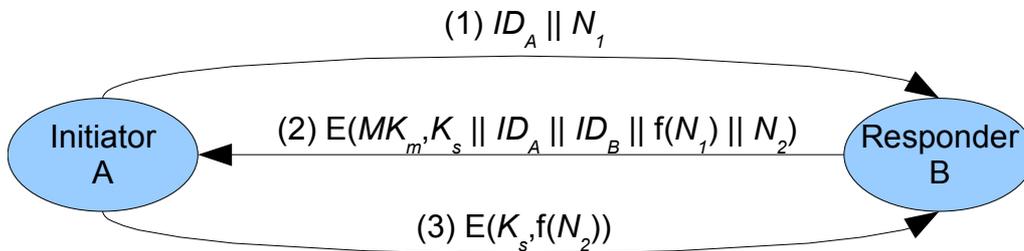
- a) How long would an average brute force attack take? [0.5 mark]

If the cipher is modified to be *Double-S*, so that for encryption two successive 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 need to perform the meet-in-the-middle attack? [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 successfully 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]