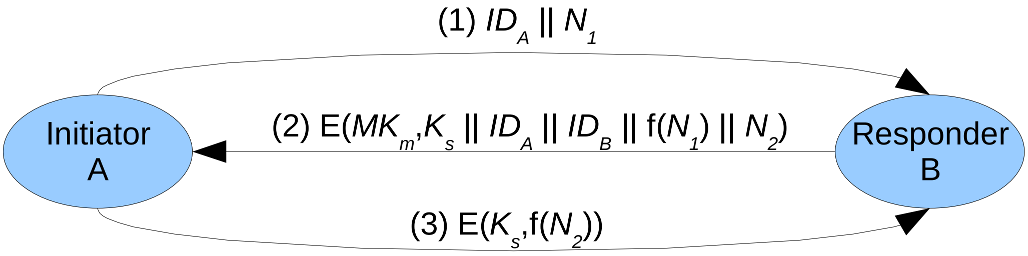
CSS322 – Quiz 3 Answers

Name: ______________________________________

ID: _________________________ Mark: ________ (out of 10)

Question 1 [5 marks]

Below is an example de-centralised key distribution protocol that may be used. MK_m is the master key shared between two nodes A and B (this sharing must be done manually/physically), and K_s is the session key.



a) How many master keys are needed in a network using this key distribution protocol if there are 10/20/11/21 nodes in the network? [2 marks]

Answer
With de-centralised scheme, each node must share a Master key with every other node:
10 nodes: 10x9/2 = 45 Master keys
20 nodes: 20x19/2 = 190 Master keys
11 nodes: 11x10/2 = 55 Master keys
21 nodes: 21x20/2 = 210 Master keys

b) If a KDC (using the protocol covered in the lecture) was used instead of the above de-centralised protocol, how many master keys would be needed in the network? [1.5 marks]

Answer
With a KDC each node must share a Master key with the KDC:
10 nodes: 10 Master keys
20 nodes: 20 Master keys
11 nodes: 11 Master keys
21 nodes: 21 Master keys

c) What is the benefit of using the de-centralised protocol compared to simply using the physically exchanged master keys for encrypting the session data? [1.5 marks]

Answer

By regularly exchanging session keys and using them for encryption, the Master key is not used for encryption. The advantage is that the attacker has less opportunity to determine the key from analysis (since the key is changing regularly).

Question 2 [3.5 marks]

Calculate the following (write answer in space provided, show any calculations below, you cannot use a calculator):

a) $\Phi(21)$ Answer: _________

b) $\Phi(18)$ Answer: _________

c) $\Phi(24)$ Answer: _________

d) $\Phi(22)$ Answer: _________

e) $\Phi(23)$ Answer: _________

f) $\Phi(37)$ Answer: _________

g) $\Phi(31)$ Answer: _________

h) $\Phi(29)$ Answer: _________

i) 3^{24} mod 25 Answer: _________

Answers

$\Phi(21)$: factors are 1, 3, 7, 21. Numbers relatively prime are: 1, 2, 4, 6, 8, 10, 11, 13, 16, 17, 19, 20. Therefore totient is: 12.

$\Phi(18)$: factors are 1, 2, 3, 6, 9, 18. Numbers relatively prime are: 1, 5, 7, 11, 13, 17. Therefore totient is: 6.

$\Phi(24)$: factors are 1, 2, 3, 4, 6, 8, 12, 24. Numbers relatively prime are: 1, 5, 7, 11, 13, 17, 19, 23. Therefore totient is: 8.

$\Phi(22)$: factors are 1, 2, 11, 22. Numbers relatively prime are: 1, 3, 5, 7, 9, 13, 15, 17, 19, 21. Therefore totient is: 10.

23, 37, 31, and 29 are prime numbers. Therefore there totients are: 22, 36, 30 and 28, respectively.

3^{24} mod 25 $= (3^3)^8$ mod 25

$= (27 \bmod 25)^8$ mod 25

$= 2^8 \bmod 25$

$= 256 \bmod 25$

$= 6$

Question 3 [1.5 marks]

Consider the following algorithms/concepts: RC4, Nonce, Linear Congruential Generator, DES, KDC, AES, Eulers Totient. Which *cannot* be used to generate random numbers? If more than one cannot be used, you must write both; if all of them can be used, then write “all appropriate”.

Answer

KDC, Eulers Totient, Nonce