CNS QUIZ 2.2 DES

Points: 4/10

1. When the key is 10-bits long, how many decryptions do the brute-force attacker try in the worst case (this is the worst case in the Alice-Bob perspective and corresponds to the case when the attacker gets lucky)? *
(1/1 Points)

1024 ✓

2. When the key is 64-bits long, how long does it take in days for an attacker to brute-force search/attack for the key on average? The attacker can perform 10 trillion (10^13) decryptions per second, given the attacker processor and the encryption/decryption algorithm. *
(0/1 Points)

(2^63)/(10^13*3600*24)

Correct answers: 2^63/10^13/3600/24=10.67519911, 10.6751991 days, 10.675

3. Triple-DES or 3-DES encryption can be characterized by the following: C=Enc(K3,Dec(K2,Enc(K1,P))). Each keys, K1, K2, K3 are 56-bits-long and are independent to each other (the three-key version). The DES block size is 64 bits.

The attacker now does not have known plaintext-ciphertext pair that it can use for her cryptanalysis. Using the big O notation, which of the following best describe the attacker's encryption/decryption computational effort? *
(0/1 Points)

● O(2^56)

○ O(2^128)

○ O(2^112)

○ O(2^168) ✓

4. Quadruple-DES or 4-DES encryption can be characterized by the following: C=Enc(K4,Enc(K3,Enc(K2,Enc(K1,P)))). Each keys, K1, K2, K3, K4, are 56-bits-long and are independent to each other. The DES block size is 64 bits.

The attacker now does not have known plaintext-ciphertext pair that it can use for her cryptanalysis. Using the big O notation, which of the following best describe the attacker's encryption/decryption computational effort? *
(0/1 Points)

○ O(2^56)

○ O(2^128)

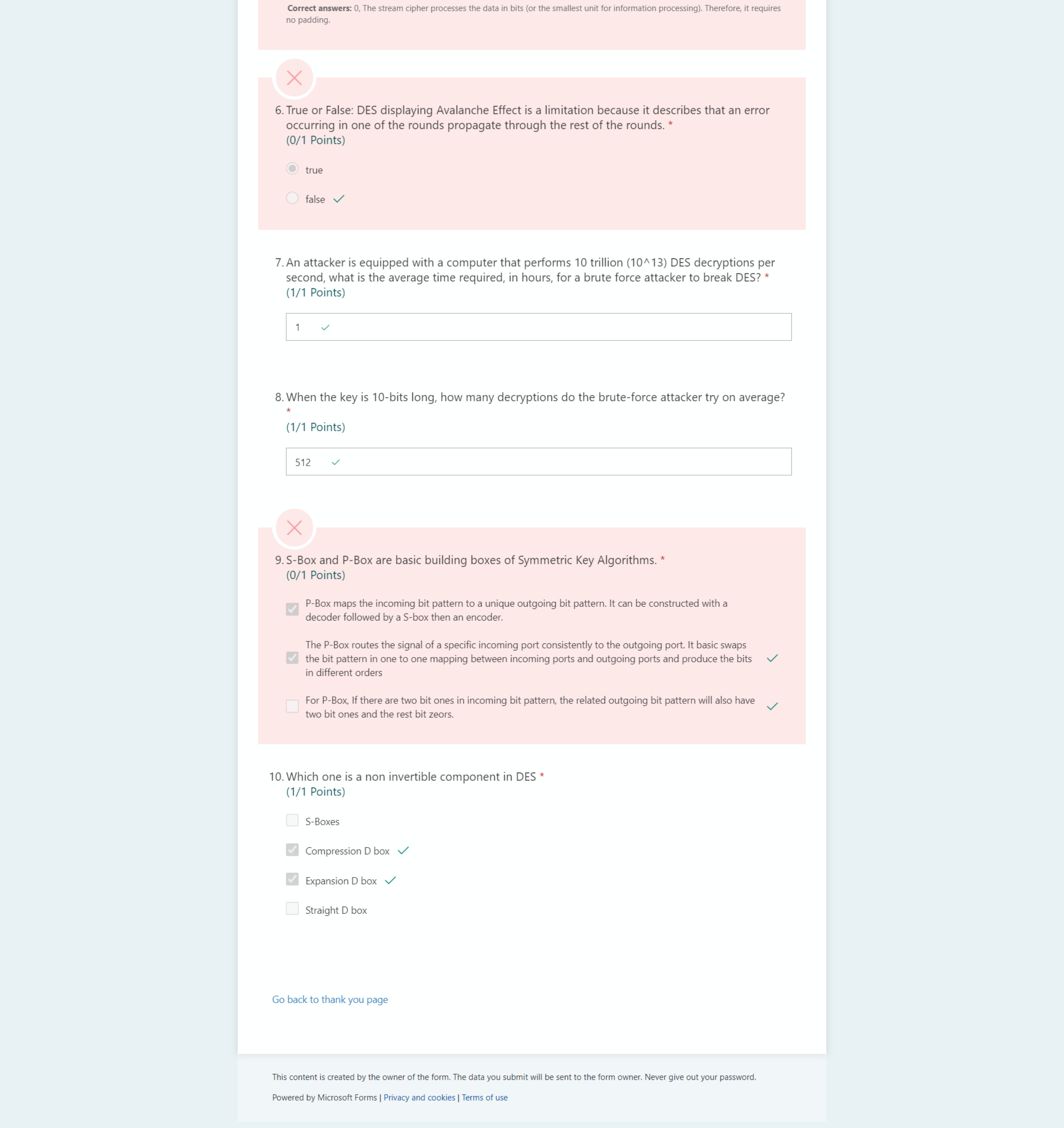
○ O(2^58)

● O(2^112)

○ O(2^224) ✓

5. You are given a stream cipher and a block cipher with a block size of 64 bits. The data input is 32 bits. How many bits do you need to pad before processing the data input using a stream cipher? *
(0/1 Points)

1024



Correct answers: 0, The stream cipher processes the data in bits (or the smallest unit for information processing). Therefore, it requires no padding.

✗

6. True or False: DES displaying Avalanche Effect is a limitation because it describes that an error occurring in one of the rounds propagate through the rest of the rounds. *
(0/1 Points)

● true

○ false ✓

7. An attacker is equipped with a computer that performs 10 trillion (10^13) DES decryptions per second, what is the average time required, in hours, for a brute force attacker to break DES? *
(1/1 Points)

1 ✓

8. When the key is 10-bits long, how many decryptions do the brute-force attacker try on average? *
(1/1 Points)

512 ✓

✗

9. S-Box and P-Box are basic building boxes of Symmetric Key Algorithms. *
(0/1 Points)

☑ P-Box maps the incoming bit pattern to a unique outgoing bit pattern. It can be constructed with a decoder followed by a S-box then an encoder.

☑ The P-Box routes the signal of a specific incoming port consistently to the outgoing port. It basic swaps the bit pattern in one to one mapping between incoming ports and outgoing ports and produce the bits in different orders ✓

□ For P-Box, If there are two bit ones in incoming bit pattern, the related outgoing bit pattern will also have two bit ones and the rest bit zeors. ✓

10. Which one is a non invertible component in DES *
(1/1 Points)

□ S-Boxes

☑ Compression D box ✓

☑ Expansion D box ✓

□ Straight D box

Go back to thank you page