Started on	Thursday, 9 September 2021, 11:05 AM
State	Finished
Completed on	Thursday, 9 September 2021, 11:40 AM
Time taken	34 mins 35 secs
Marks	16.00/20.00
Grade	**8.00** out of 10.00 (**80**%)

Question 1

Correct

Mark 2.00 out of 2.00

Flag question

Assume the alphabet set as described here: {A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, R, S, T, W, X}. The plaintext, ciphertext, and keyspace are same as the described in the set. Now, consider the concept of Affine Cipher and decrypt the ciphertext "KH" by using the key k = (7, 3).

[Hint: Consider A = 1, B = 2, and so on.]

Select one:

- a. DO ✓
- b. HE
- c. ME
- d. Decryption is not possible

Your answer is correct.

The correct answer is: DO

Question 2

Correct

Mark 2.00 out of 2.00

Flag question

Encrypt the short text "IIT" by using the method of Hill cipher. Consider the keyword as "ALPHABETA" and a key matrix of size 3 x 3 (row-wise).

[Hint: Consider A=0, B=1, and so on.]

Select one:

- a. JXB
- b. JCM
- c. JXC ✓
- d. AXC

Your answer is correct.

The correct answer is: JXC

Question 3

Incorrect

Mark 0.00 out of 2.00

Flag question

The average complexity of an exhaustive search against the 2-key 3DES

Select one:

- a. 2^{111}
- b. 2^{112} ✗
- c. 2^{56}
- d. 2^{57}

Your answer is incorrect.

The correct answer is: 2^{111}

Question 4

Correct

Mark 2.00 out of 2.00

Flag question

The security of DES is increased by increasing the number of encryption using two keys k1 and k2 (e.g. 2DES) or by using 3 keys k1, k2, k3 (e.g. 3DES). For Substitution cipher, we can comment on its security as

Select one:

- a. No additional security can be gained by enciphering a message by using two monoalphabetic ciphers with two different keys in succession ✓
- b. Additional security can be gained by enciphering a message by using two monoalphabetic ciphers with two different keys in succession (say the plain text is encrypted by k = 4 and then the resulting ciphertext is encrypted by k = 8)

Your answer is correct.

The correct answer is: No additional security can be gained by enciphering a message by using two monoalphabetic ciphers with two different keys in succession

Question 5

Correct

Mark 2.00 out of 2.00

Flag question

Given a bit string x, let x' denotes the bitwise complement, i.e. the bit string obtained by flipping all bits of x. DES has the following complementation properties

$$DES_{k'}(x') = (DES_k(x))' \quad \text{for any x and k}$$

Now, taking the advantage of the above complementation property of DES, the complementation property of 2-key 3DES becomes

Select one:

- a. $3DES_{k1', k2'}(P') = (3DES_{k1,K2}(P))'$ ✓
- b. $3DES_{k2'}(P') = (3DES_{k1,K2}(P))'$

c. $3DES_{k1'}(P') = (3DES_{k1,K2}(P))'$

d. None of the above

Your answer is correct.

The correct answer is: $3DES_{k1', k2'}(P') = (3DES_{k1,K2}(P))'$

Question 6

Correct

Mark 2.00 out of 2.00

Flag question

Consider a 5-round 16-bit SPN block cipher with the S-box: $\{0, 1\}^4 \rightarrow \{0, 1\}^4$. The difference distribution of a few input-output of the S-box is as follows

		OUTPUT															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INPUT	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	8	0	0	0	0	6	0	2	0	0	0	0	2	0	2	2	2
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0

The propagation rate of the Differential Trail formed with the five active S-boxes S_2^1 (1110, 1000), S_1^2 (0100, 0110), S_2^3 (1000, 0100), S_3^3 (1000, 0100), S_2^4 (0110, 0011).

(Here, S_i^k (x, y) represents ith S-box of kth round with input x and output y.)

Select one:

a. 27/2048

b. 81/4096

c. 81/16384 ✓

d. 27/1024

Your answer is correct.

The correct answer is: 81/16384

Question 7

Incorrect

Mark 0.00 out of 2.00

Flag question

Narrowing down the key in DES, for a text message, the key search space can be reduced from approximately 2^{56} to 2^n after examining the first block of 8 bytes. (We assume that each text letter is encoded to a binary string of 8 bits and that there are 64 ASCII characters.) The value of n is

Select one:

a. 48 ✗

b. 40

c. 24

d. 32

Your answer is incorrect.

The correct answer is: 40

Question 8

Correct

Mark 2.00 out of 2.00

Flag question

Suppose Caesar sends a message to one of its generals, and the message contains only one letter. You can say about the message security that

Select one:

- a. The message is not secured
- b. Nothing can be told about its security
- c. The message has the perfect security, because the message could be any of the 26 letters of the alphabet ✓
- d. The message doesn't have the perfect security, because the message could be any of the 26 letters of the alphabet

Your answer is correct.

The correct answer is: The message has the perfect security, because the message could be any of the 26 letters of the alphabet

Question 9

Correct

Mark 2.00 out of 2.00

Flag question

Let e_1, e_2, e_3, and e_4 be the bias of four random variable X_1, X_2, X_3 and X_4 respectively where, $e_1 = e_2 = ½$ and $e_3 = e_4 = ¼$. The bias of (X1 ⊕ X2 ⊕ X3 ⊕ X4) is

Select one:

- a. 1/32
- b. 1/64
- c. 1/16
- d. 1/8 ✓

Your answer is correct.

The correct answer is: 1/8

Question 10

Correct

Mark 2.00 out of 2.00

Flag question

If the plain text message "ENCODE" is encrypted by Caesar cipher with key k = -5, the ciphertext becomes

Select one:

- a. ZIXJYZ ✓
- b. AJYKZA
- c. JSHTIJ

d. YHWIXY

Your answer is correct.

The correct answer is: ZIXJYZ

Finish review

QUIZ NAVIGATION

1 2 3 4 5 6 7 8 9 10

Show one page at a time

Finish review