يوم الامتحان: الاحد

تاريخ الامتحان: 9 / 6 / 2019 م

الزمن: ساعتان (1 ظهرا الي 3 عصرا)

المادة : التشفير (MC466)

الممتحن: د/ مصعب عبد الحميد محمد حسان

مدرس بقسم الرياضيات بكلية العلوم

الاسئلة و نموذج الإجابة

ورقة كاملة

Benha University
Faculty of Science
Dept. of Mathematics

Time: Two Hours
Second Semester 2018-2019
Date : 9/6/2019

Cryptography (MC466) for fourth Level Students (Computer Science)

Choose the correct answer for each of the following:[20x1.5+2x3+3x4=48 Marks]

1-In ……, different keys used for encryption and decryption.
(A) symmetric cipher (B) asymmetric cipher

2- ….. replaces each element of the plaintext with another element.
(A) Substitution cipher (B) Transposition cipher

3- In playfair cipher, if both letters fall in the same column, …..
(A) replace each with the the letter below it (circularly).
(B) replace each with the letter to its right (circularly).

4- Let we have the equation, 7 * d = 1 mod 120, then d = …..
(A) 104 (B) 103 (C) 107

5- Row cipher writes the message in …..
(A) a rectangle, row by row, and read the message off, column by column.
(B) a rectangle, column by column, and read the message off, row by row.
(C) a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

6- In feistal structure, the permutation step at the end of each round consists of swapping the modified L and R.
(A) Yes (B) No

7- DES encodes each ….. block of data.
(A) 64-bit (B) 128-bit

8- Which of the following belongs to GF(2^8) ?
(A) $2x^4+x^3+1$ (B) x^8+x^2+x+1 (C) $x^7+x^6+x^5+x+1$

9- In DES, S-Box tables contain values …..
(A) from 0 to 15 (B) from 0 to 31 (C) from 0 to 65

10- In DES, …..
(A) $L_n = R_{n-1}$ (B) $L_n = L_{n-1} + f(R_{n-1}, K_n)$

11- The plaintext in RSA is …..
(A) C ^ d mod n (B) C ^ e mod n (C) C ^ d mod e

12- In AES, if key length equals to 192 bits then the number of rounds equals to …..
(A) 10 (B) 12 (C) 14

13- In AES, last round has MixColumn Sublayer. This is correct?
(A) Yes (B) No

14- AES does not have a Feistel structure
(A) Yes (B) No

15- In AES, S-Box tables contain values …..
(A) from 0 to 65 (B) from 0 to 127 (C) from 00 to FF

16- In AES, we apply …..

(A) MixColumn Sublayer then ShiftRows Sublayer.

(B) ShiftRows Sublayer then MixColumn Sublayer.

17- In GF(2^8), the sum of the two polynomials $x^5+ x^4+ 1$ and $x^5+ x^2+ 1$ is …..

(A) $2x^5+ x^4+ x^2 + 2$ (B) $x^4+ x^2$ (C) $x^5 + x^4$

18- In AES, the irreducible polynomial P(x) = …..

(A) $x^7 +x^4+x^3+1$ (B) $x^7 +x^4+x^2+x+1$ (C) $x^8 +x^4+x^3+x+1$

19- In DNA method for decyption, we extract …..

(A) the first two and the last two characters from the sequence.

(B) the first and the last characters from the sequence.

20- In the naïve algorithm to encrypt and decrypt strings to DNA Sequences, The number of all arrangement in the database is …..

(A) 6 (B) 120 (C) 24 (D) 100

21- In AES, we use the following equation in MixColumn sublayer

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

(A) Yes (B) No

22- Suppose K = $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$, Using hill cipher, the cipher text of the plaintext "act" is …..

(A) MOH (B) POH (C) HOP

23- Suppose the key is $\begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}$, using hill cipher, the plaintext of the cipher text "SYI" is …..

(A) res (B) wea (C) afe

24- Suppose the key is " MONARCHY ", using Playfair Cipher, the cipher text of the plaintext " atsamewouldfallinthesamepair " is …..

(A) RSXBCLVNMUHKMSSERQCFXBCLSOKA

(B) HKCLVNMUMSSEXBRSXBCLSOKARQCF

25- Suppose the key is "14532", using row Cipher, the cipher text of the plaintext "thisisacolumnartransposition" is …..

(A) TSUTPI ILRSTX SOANIX HAMROO ICNASN

(B) TSUTPI SOANIX ILRSTX ICNASN HAMROO

Model Answer [Cryptography (MC466)]

1- B
2- A
3- A
4- B
5- C
6- A
7- A
8- C
9- A
10- A
11- A
12- B
13- B
14- A
15- C
16- B
17- B
18- C
19- A
20- C
21- A
22- B
23- B
24- A
25- A