**NAME: UBUA VERA**

**MATRIC NUMBER: 16/SCI01/048.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: REVISED QUESTIONS PART III.**

**START DATE: 15-06-2020.**

**END DATE: 30-06-2020.**

**QUESTION**

Kindly use these questions to revise the topics we have treated so far. It will come in batches, this is the third batch. The rest will be posted as times goes on. Kindly attempt it and submit online.

1. In vigenere cipher, decrypt this given ciphertext “VJDM XL WPHQBI” using “keyword” as the key.
2. In one time pad, given the plaintext “numeric” perform character encoding.
3. In one time pad, given the plaintext “COLLEGE OF SCIENCE” perform character encoding.
4. In Rail Fence Transposition, encrypt the following plaintext “ILOVEBEAUTIFULCAKES” using two depth transposition.
5. In Rail Fence Transposition, encrypt the following plaintext “ILOVEBEAUTIFULCAKES” using two depth transposition. The key is given as 524613.
6. In Rail Fence Transposition, encrypt the following plaintext “ILOVEBEAUTIFULCAKES” using two depth transposition. The key is given as 524613, while the key for the second transposition is given as 415362.
7. Using the rail fencing technique decrypt the following plaintext: “CNODCPETICDAYUEIHRHSOE”.
8. Decipher the following using two level transposition:

Cipher: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Key: 4312567

**ANSWER**

1. Key: “keyword”

Ciphertext: “VJDM XL WPHQBI”

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | k | e | y | w | o | r | d | k | e | y | w | o |
| Numeric representation | 10 | 4 | 24 | 22 | 14 | 17 | 3 | 10 | 4 | 24 | 22 | 14 |

Key numeric representation: 10 4 24 22 14 17 3 10 4 24 22 14

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext | V | J | D | M | X | L | W | P | H | Q | B | I |
| Key | k | e | y | w | o | r | d | k | e | y | w | o |
| Numeric representation | 10 | 4 | 24 | 22 | 14 | 17 | 3 | 10 | 4 | 24 | 22 | 14 |
| Plaintext | k | e | e | p | i | t | s | e | c | r | e | t |

**Plaintext: keep it secret**

1. Plaintext: numeric

Keyword: decimal

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

n + d = 13 + 3 = 16

u + e = 20 + 4 = 24

m + c = 12 + 2 = 14

e + i = 4 + 8 = 12

r + m = 17 + 12 = 29

i + a = 8 + 0 = 8

c + l = 2 + 11 = 13

**Ciphertext: qyomdin**

1. Plaintext: COLLEGE OF SCIENCE

Keyword: SOCIETY IS INSIGHT

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

C + S = 2 + 18 = 20 = U

O + O = 14 + 14 = 28 = C

L + C = 11 + 2 = 13 = N

L + I = 11 + 9 = 20 = U

E + E = 4 + 4 = 8 = I

G + T = 6 + 19 = 25 = Z

E + Y = 4 + 24 = 28 = C

O + I = 14 + 8 = 22 = W

F + S = 5 + 18 = 23 = X

S + I = 18 + 8 = 26 = A

C + N = 2 + 13 = 15 = P

I + S = 8 + 18 = 26 = A

E + I = 4 + 8 = 12 = M

N + G = 13 + 6 = 19 = T

C + H = 2 + 7 = 9 = J

E + T = 4 + 19 = 24 = Y

**Ciphertext: UCNUIZC WX APAMTJY**

1. Plaintext: “ILOVEBEAUTIFULCAKES”

Using two depth transposition

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I |  | O |  | E |  | E |  | U |  | I |  | U |  | C |  | K |  | S |
|  | L |  | V |  | B |  | A |  | T |  | F |  | L |  | A |  | E |  |

**Cipertext: IOEEUIUCKS LVBATFLAE**

1. Plaintext: “ILOVEBEAUTIFULCAKES”

Key: 524613

Using two depth transposition

Column out: 5 2 4 6 1 3

 I L O V E B

 E A U T I F

 F U L C A K

 E S

**Cipertext: EIALAUSBFKOULIEFEVTC**

1. Plaintext: “ILOVEBEAUTIFULCAKES”

Using two depth transposition

Key for the first transposition: 524613

Key for the second transposition: 415362

Column 1 out: 5 2 4 6 1 3

 I L O V E B

 E A U T I F

 F U L C A K

 E S

Column 2 out: 4 1 5 3 6 2

 I L O V E B

 E A U T I F

 F U L C A K

 E S

**Cipertext for first key: EIALAUSBFKOULIEFEVTC**

**Ciphertext for second key: LAUSBFKVTCIEFEOULEIA**

1. Ciphertext: “CNODCPETICD AYUEIHRHSOE”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C |  | N |  | O |  | D |  | C |  | P |  | E |  | T |  | I |  | C |  | D |  |
|  | A |  | Y |  | U |  | E |  | I |  | H |  | R |  | H |  | S |  | O |  | E |

**Plaintext: can you decipher this code**

1. Using two level transposition:

Cipher: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Key: 4312567

Column out: 4 3 1 2 5 6 7

 T T N A A P T

 M T S U O A O

 D W C O I X K

 N L Y P E T Z

**Plaintext: ttnaaptmtsuoaodwcoixknlypetz**