Name: CHAARU MANJURAJ KOMALA

Student ID: 2406827

[**LM Network Security and Cryptography (34231)**](https://canvas.bham.ac.uk/courses/65676) **Exercise 1 (Formative Assessment)**

#### Question – I

### Decrypt the following cipher text encrypted with the columnar transposition cipher (you need to find the key by brute-force search):

### **AVUEVLETSEISBNACBOOLEOBTILBDLCOBOOE**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | L | I | C | E | L | O |
| V | E | S | B | O | B | B |
| U | T | B | O | B | D | O |
| E | S | N | O | T | L | O |
| V | E | A | L | I | C | E |

The Decrypted Message is:

**ALICE LOVES BOB BUT BOB DOES NOT LOVE ALICE**

#### **Question – II**

### What is the output of the first round of the DES algorithm when the plain-text and the key are both all zeros?

**ROUND – I**

#### Question – III

### Remember that it is desirable for good block ciphers that a change in one input bit affects many output bits, a property that is called diffusion or avalanche effect. We will try to get a feeling for the avalanche property of DES.

### Let x be all zeros (0x0000000000000000) and y be all zeros except 1 in the 13th bit (0x0008 000000000000). Let the key be all zeros. After just one round, how many bits in the block are different when x is the input, compared to when y is the input? What about after two rounds? Three? Four?

|  |  |
| --- | --- |
| X (0x0000000000000000) | Y (0x0008 000000000000) |
| Formula  Round – I  **Round – II**  **Round – III**  Round – IV | **Formula**  **Round – I**  **Round – II**  **Round – III**  **Round – IV** |

Number of different bits in the block when is the input, compared to when is the input:

#### Question – IV

### Consider AES with 128-bit keys. Assume that the principal key k is all-zeros. Then the initial round key (k0) is also all-zeros. What is the first round subkey (k1) and the second round subkey (k2)?

Message: 0123456789ABCDEFFEDCBA9876543210

**Principal key (): 00000000000000000000000000000000**

Round Key in Round 0 ()

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Round Key in Round 1 ()

62 63 63 63 62 63 63 63 62 63 63 63 62 63 63 63

Round Key in Round 2 ()

9B 98 98 C9 F9 FB FB AA 9B 98 98 C9 F9 FB FB AA

#### Question – V

### **Programming exercise:** Let MY24SHA a hash function which outputs the first 24 bits (6 nibbles) of SHA-1. For example, SHA-1 of “mark” is f1b5a91d4d6ad523f2610114591c007e75d15084 so the MY24SHA of “mark” is f1b5a9.

### Find any collision for MY24SHA. Note: you should find two strings such that the unix command

### echo -n str | sha1sum - | cut -c1-6

### produces the same answer when str is replaced by each string. To enable me to verify your answer, please make sure the two strings are typable on a regular keyboard!

WORD – I: **abasedness**

WORD – II: **hydurilate**

MY24SHA of abasedness is **3fd8b0**

MY24SHA of hydurilateis **3fd8b0**