|  |  |
| --- | --- |
| Course: | INFO-6001-23W |
| Project: | Assignment #2 |
| Due Date: | 19/01/2023 |
| Submitting: |  |
| Professor: | Steve Spencer |
| Student Name / No: | Gihan Shamike Liyanage / 1142109 |

|  |  |  |
| --- | --- | --- |
| Marks | What are the Marks Awarded For? | Mark Assigned |
| 20 | Part 1 a |  |
| 20 | Part 1 b |  |
| 20 | Part 2 |  |
| 40 | Correct answers |  |
| 100 |  |  |

**Part 1**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **O** | **X** | **F** | **O** | **R** | **D** |
| **3** | **6** | **2** | **4** | **5** | **1** |
|  |  |  |  |  |  |
| F | A | N | S | H | A |
| W | E | C | O | L | L |
| E | G | E | I | S | I |
| N | L | O | N | D | O |
| N | C | A | N | A | D |
| A |  |  |  |  |  |

**Output -** ALIODNCEOAFWENNASOINNHLSDAAEGLC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S** | **T** | **R** | **E** | **E** | **T** |
| **4** | **5** | **3** | **1** | **2** | **6** |
|  |  |  |  |  |  |
| A | L | I | O | D | N |
| C | E | O | A | F | W |
| E | N | N | A | S | O |
| I | N | N | H | L | S |
| D | A | A | E | G | L |
| C |  |  |  |  |  |

**Output -** OAAHEDFSLGIONNAACEIDCLENNANWOSL

1. The double transposition cipher is a way of encryption that involves reorganising the letters of a plaintext message according to two different keywords. The first step of the encryption process is creating a matrix that is the same length as the plaintext message. Number of columns are determining by the first keyword’s length. Keyword letters will write above each column. Then letters of the plaintext message will be inserted into the matrix row by row. Then rearrange the matrix columns considering only the alphabetical order of keyword letters. First output cipher text is getting by concatenating letters of matrix column by column. To get final output cipher text, repeat the same process with second keyword, by taking first output cipher text as the input.

This method creates a cipher text which can be decrypted back. Decryption can be achieved by reversing the same process if the keywords are known. From this point double transposition cipher deviates from hashing.

**Part 2**

**Cipher to decode** - UKLISTENAQYWSOIYCPRGECNOMASNSDIAAK

**Keywords**: Summer

Winter

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S** | **U** | **M** | **M** | **E** | **R** |
| **5** | **6** | **2** | **3** | **1** | **4** |
|  |  |  |  |  |  |
| N | S | T | W | U | P |
| O | D | E | S | K | R |
| M | I | N | O | L | G |
| A | A | A | I | I | E |
| S | A | Q | Y | S | C |
| N | K | Y | C |  |  |

**Output -** NSTWUPODESKRMINOLGAAAIIESAQYSCNKYC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **W** | **I** | **N** | **T** | **E** | **R** |
| **6** | **2** | **3** | **5** | **1** | **4** |
|  |  |  |  |  |  |
| S | P | R | I | N | G |
| C | O | M | E | S | A |
| N | D | I | S | T | A |
| K | E | N | A | W | A |
| Y | S | O | Q | U | I |
| C | K | L | Y |  |  |

**Output –** SPRINGCOMESANDISTAKENAWAYSOQUICKLY

**Decoded plain text** - SPRINGCOMESANDISTAKENAWAYSOQUICKLY