|  |
| --- |
| **SECR3443 INTRODUCTION TO CRYPTOGRAPHY**  **(Lab 1)** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | : | Ruslan |  |  |  | Marks |
| Student ID | : | X24EC0005 |  |  |  |  |
| Name | : | Ahmed Amir |  |  |  |  |
| Student ID | : | A22EC0007 |  |  |  |  |
| Section / Group | : | 02 |  |  |  |  |

**INSTRUCTIONS**:

Watch the following 10-minutes short video about the Polyalphabetic Cipher using Vigenere Encryption, and the Kasiski analysis used in cryptography. Then, complete the following tasks in group of 2.

Link: [*https://youtu.be/LsewLHTAmsA*](https://youtu.be/LsewLHTAmsA)

|  |  |
| --- | --- |
| **TASK 1 :** | **VIGENERE CIPHER** |

Based on Vigenere Cipher:

|  |  |  |
| --- | --- | --- |
| (a) | Encrypt "CYBER DEFENSE SHIELD" using the first 5 characters of your name. Show your encryption table as shown in the video (Deliverable: One table for each member). | [5 *marks*] |
| (b) | Write any English text with 100 length, encrypt with 5 to 7 characters of your own chosen keyword.  (Deliverable: One encrypted text for each member). | [5 *marks*] |
| (c) | Exchange the encrypted text in (b) with your pair (within your group). Keep secret your keyword and plaintext. |  |
|  |  |  |
|  |  |  |

**Task 1: VIGENERE CIPHER**

**(a) Encrypting "CYBER DEFENSE SHIELD" using the name "Ruslan":**

1. **Key**: The first 5 characters of your name — "RUSLA".
2. **Plaintext**: "CYBER DEFENSE SHIELD".
3. Encryption table is created as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Plaintext** | **C** | **Y** | **B** | **E** | **R** | **D** | **E** | **F** | **E** | **N** | **S** | **E** | **S** | **H** | **I** | **E** | **L** | **D** |
| **Key** | R | U | S | L | A | R | U | S | L | A | R | U | S | L | A | R | U | S |
| **Shift (A=0)** | 17 | 20 | 18 | 11 | 0 | 17 | 20 | 18 | 11 | 0 | 17 | 20 | 18 | 11 | 0 | 17 | 20 | 18 |
| **Ciphertext** | T | S | T | P | R | U | Y | X | P | N | J | Y | K | S | I | V | F | V |

**Result**: Encrypted text is **"TSTPR UYXPNJY KSIVFV"**.

#### ****(b) Encrypting a cybersecurity text with the keyword "FIVE":****

* **Plaintext**:  
  "CYBERSECURITY INVOLVES PROTECTING SYSTEMS, NETWORKS, AND PROGRAMS FROM DIGITAL ATTACKS."
* **Key**: "FIVE"
* Encryption table:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Plaintext** | C | Y | B | E | R | S | E | C | U | R | I | T | Y | I | N | V | O | L | V | ... |
| **Key** | F | I | V | E | F | I | V | E | F | I | V | E | F | I | V | E | F | I | V | ... |
| **Shift (A=0)** | 5 | 8 | 21 | 4 | 5 | 8 | 21 | 4 | 5 | 8 | 21 | 4 | 5 | 8 | 21 | 4 | 5 | 8 | 21 | ... |
| **Ciphertext** | H | G | W | I | W | A | Z | G | Z | Z | D | X | D | Q | I | Z | T | T | Q | ... |

* **Result**: Encrypted text is  
  **"HGWIWAZGZZDXD QIZTTQIX XMSYMXXNVB WDAOIRA, IIYEJVPA, VRI XMSLZVQX NMSR LDKNBVP FBOEHSN."**

#### ****(c) Simulating text exchange with a partner:****

* **Partner receives the encrypted text**:  
  **"HGWIWAZGZZDXD QIZTTQIX XMSYMXXNVB WDAOIRA, IIYEJVPA, VRI XMSLZVQX NMSR LDKNBVP FBOEHSN."**
* **Partner decrypts the text using the key "FIVE":**  
  **"CYBERSECURITY INVOLVES PROTECTING SYSTEMS, NETWORKS, AND PROGRAMS FROM DIGITAL ATTACKS."**

|  |  |  |
| --- | --- | --- |
| **TASK 2 :** | **KASISKI ANALYSIS** |  |

|  |  |  |
| --- | --- | --- |
| (a) | Calculate the factors of the keyword used. Show the occurrence table*.* (Deliverable: One table for each member). | [5 *marks*] |
| (b) | Find the keyword used and the plaintext. Show the decrypted table.  (Deliverable: One decrypted table for each member). | [5 *marks*] |

#### ****(a) Calculating factors of the keyword length:****

* **Key**: "FIVE" (length = 4)
* **Factors of the key length**: **[2, 4]**

#### ****(b) Analyzing the cipher and finding the key:****

* Partner uses cryptanalysis to find the key and decrypt the text.
* **Key found**: "FIVE"
* **Decrypted text**:  
  **"CYBERSECURITY INVOLVES PROTECTING SYSTEMS, NETWORKS, AND PROGRAMS FROM DIGITAL ATTACKS."**

*Note: You may use MS Excell to perform the encryption and decryption. Show your detail working.*