****

**LAB ASSIGNMENT**

**Data and Network Security**

|  |  |  |
| --- | --- | --- |
| Name | : | Hendianto Mohammad Farid |
| Matrix ID | : | CB24153 |
| Lecture Name | : | Mr. Syahrizal Azmir Bin Md. Sharif |
| Date of Submission | : | October 2024 |

PLEASE FOLLOW INSTRUCTIONS CAREFULLY

1. This lab assignment is an individual assignment.
2. The mark is 60% which brings 15% out of the total assessment mark.
3. Read the task instructions given carefully and follow the rubric given to complete your task.

THE LEARNING OUTCOME

This assignment will be evaluated based on the learning outcome of CO2.

CO2: Construct and organize attack and defence methods into computer and network environments. (Psychomotor).

THE TASK NEEDS TO FOLLOW

In this individual assignment, you need to complete all tasks given. There are six main tasks. Please do it on your own and in your own words and provide references where appropriate.

SUBMISSION REQUIREMENTS AND MARKS DISTRIBUTION

1. The front page must contain a **name, id, section, lecturer name and date of submission**.
2. Task 1 – 10 marks
3. Task 2 – 10 marks
4. List of references

\* Submission based on each task in 2 weeks. The overall mark for lab assignments altogether is 60 marks. There will be 3 Lab Assignments throughout the semester.

# TASK 1

* 1. Find around five attacks on any cybersecurity attack data whether for a month, for a year or several years of data. Provide a reference for your attack data.

Here are five primary attacks on any cybersecurity attack data Q2 2024:

1. **Malware**

|  |  |
| --- | --- |
| **Percentage**: 22.7% | **Total Incidents**: 156 |

Malware is a category of malicious software specifically crafted to infiltrate, damage, or gain unauthorized control over systems. It encompasses a wide array of threats, including:

**Viruses**: Programs that replicate themselves and spread across devices.

**Trojans**: Malware disguised as legitimate software, deceiving users into executing it.

**Worms**: Self-replicating malware that spreads without user intervention.

Malware can lead to data theft, system corruption, espionage, or the disruption of critical services.

1. **Ransomware**

|  |  |
| --- | --- |
| **Percentage**: 15.4% | **Total Incidents**: 106 |

Ransomware attacks involve malware that encrypts a victim’s data, rendering it inaccessible. The attacker then demands a ransom, often in cryptocurrency, for the decryption key.

**Notable Tactics**: Double extortion, where attackers threaten to leak sensitive data if the ransom is not paid.

**Target Sectors**: Healthcare, education, and critical infrastructure are frequently targeted due to their reliance on data availability.

Ransomware attacks can disrupt operations, lead to significant financial losses, and damage an organization’s reputation.

1. **Vulnerability Exploitation**

|  |  |
| --- | --- |
| **Percentage**: 11.6% | **Total Incidents**: 80 |

Attackers exploit unpatched software vulnerabilities to execute malicious code, escalate privileges, or gain unauthorized access to systems.

**Common Exploits**: Zero-day vulnerabilities, buffer overflows, and SQL injections.

**Prevalence**: Highly targeted in environments where patch management is insufficient.

**Risk Mitigation**: Continuous monitoring, timely updates, and employing robust vulnerability management practices are crucial to minimize these risks.

1. **Account Takeover (ATO)**

|  |  |
| --- | --- |
| **Percentage**: 10.2% | **Total Incidents**: 70 |

Account takeover attacks occur when cybercriminals gain unauthorized access to a user’s account, often using stolen or brute-forced credentials.

**Methods**: Phishing campaigns, credential stuffing, and social engineering tactics.

**Implications**: Once inside an account, attackers can exfiltrate sensitive data, conduct financial fraud, or impersonate the user to commit further crimes.

**Targets**: Banking services, e-commerce platforms, and corporate email accounts are commonly affected.

1. **Targeted Attacks**

|  |  |
| --- | --- |
| **Percentage**: 10.0% | **Total Incidents**: 69 |

These are well-planned, strategic cyberattacks aimed at specific organizations, government bodies, or critical infrastructure.

**Sophisticated Techniques**: Advanced Persistent Threats (APTs), spear-phishing, and custom malware.

**Purpose**: Often driven by espionage, sabotage, or financial motives.

**Characteristics**: Attackers invest considerable time and resources to study their targets, sometimes breaching networks and remaining undetected for months.

**Other Techniques**

* **Percentage**: 30.1%
* **Total Incidents**: 207
* **Breakdown of Techniques**:
  + **Coordinated Inauthentic Behavior**: Efforts to manipulate public opinion or deceive individuals via fake accounts or automated bots.
  + **DDoS (Distributed Denial-of-Service)**: Overwhelming systems with massive volumes of traffic to disrupt service availability.
  + **Malicious Script Injection**: Attacks like Cross-Site Scripting (XSS) that inject harmful scripts into websites, potentially compromising user data.
  + **Malvertising**: Distributing malware through online advertisements on reputable websites.
  + **Misconfiguration Exploitation**: Attacks that exploit system misconfigurations, such as open ports or poorly secured databases.
  + **Brute Force and Credential Stuffing**: Automated attempts to gain unauthorized access by systematically trying password combinations or using previously breached credentials.

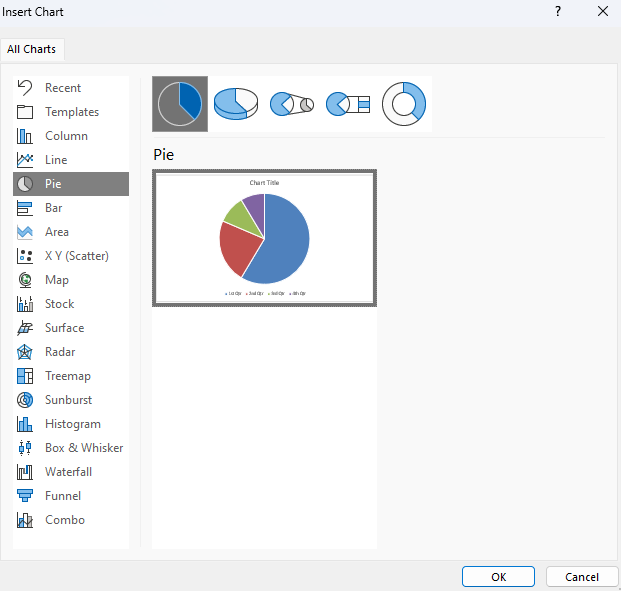
**Diverse Impact**: These techniques often lead to financial fraud, data breaches, reputation damage, or significant service disruption.

**Reference:**

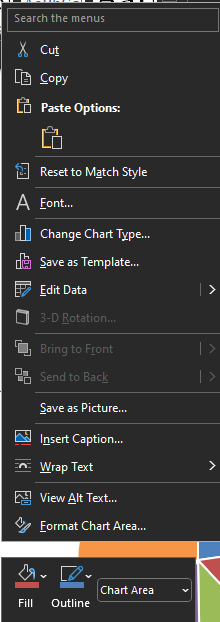
Passeri, P. (2024, October 3). *Q2 2024 Cyber Attacks Statistics*. Hackmageddon. <https://www.hackmageddon.com/2024/10/03/q2-2024-cyber-attacks-statistics/>

* 1. Given the attack data that you search, use **Microsoft Excel,** and process the data using the steps below:
     1. Calculate the total attack for each category. Then, generate a graph and explain the graph.

We can generate a graph from Microsoft Word (included Excel)



Select pie data



Click Edit Data >



* + 1. Based on the graph in 1., identify the highest attack.

Based on the data provided in Q2 2024, Malware is the highest attack, accounting for 22.7% of the total incidents (156 out of 688).

* + 1. Give several possible reasons why the highest attack in 2., has been identified as the most occurred attack.

Malware can be spread through various channels, such as email attachments, malicious websites, infected USB drives, and software downloads, making it easy for attackers to distribute.

The shift towards remote work environments has made systems more vulnerable, as home networks are generally less secure than corporate environments.

A significant factor in the success of malware attacks is human error. Users often fall victim to phishing emails or download malicious attachments, allowing malware to spread easily.

Cybercriminals often use malware to steal data, conduct financial fraud, or extort money, making it a highly lucrative attack method.

Modern malware has become highly sophisticated, using techniques like polymorphic malware (which changes its code to evade detection) and fileless malware (which resides in system memory and leaves no trace on disk).

* + 1. Create an awareness statement to the public on how to reduce and prevent the attack from happening in the future. Provide five actions that need to be taken by users.

"Prevent Malware Infections: Protect Your Devices and Data"

Malware attacks are on the rise, and it is crucial for everyone to understand how to protect themselves from these threats. Cybercriminals are continuously evolving their tactics, so staying informed and cautious can make a significant difference. Here are five actions you can take to prevent malware infections:

Use Reliable Antivirus Software: Install and regularly update a trusted antivirus program on all your devices. Antivirus software can help detect and remove malware before it causes harm.

Keep Your Software Updated: Regularly update your operating system, browsers, and all software applications. Software updates often include security patches that fix vulnerabilities exploited by malware.

Be Cautious with Emails and Attachments: Avoid opening email attachments or clicking on links from unknown or suspicious senders. Always verify the sender’s authenticity before engaging.

Download Only from Trusted Sources: Only download software from official websites or trusted app stores. Avoid pirated software, as it often contains hidden malware.

Regularly Backup Your Data: Create regular backups of important files and store them securely, either on an external hard drive or in the cloud. This way, if you do fall victim to a malware attack, you won’t lose your data.

Stay vigilant and proactive to keep your digital world safe from malware threats. Cybersecurity is everyone's responsibility.

***You need to provide step by step snapshot for the Excel part on how you process the data with a clear explanation.***

* 1. Go to https://ccid.rmp.gov.my/Laws/Computer\_Crime\_Act\_1997.pdf webpage. Get the information below:
     1. How many parts are in the CCA?

The **Computer Crimes Act 1997 (CCA)** of Malaysia, formally codified as **Act 563**, is systematically organized into **three distinct parts**, each addressing specific legislative concerns related to computer-related offences and the corresponding legal framework.

1. **Part I: Preliminary**

This section lays the foundational framework for the Act, including its **short title, commencement date, and key definitions** that establish the operational scope of the law. Specifically, it provides crucial interpretations of terms such as "computer," "computer network," "data," and "program," which are integral to understanding the context and application of the Act. The clarity offered in these definitions is fundamental, as it delineates the parameters within which the law operates and ensures there is no ambiguity regarding the entities regulated under the Act.

1. **Part II: Offences**

This part is the **core of the Act**, detailing the specific offences that are prohibited and the corresponding penalties for each violatio

1. **Part III: Ancillary and General Provisions**.

This section outlines the **jurisdictional scope** and procedural guidelines for the enforcement of the Act.

* + 1. What are the offences covered in CCA?

The offences covered in the Computer Crimes Act 1997 include the following:

**Unauthorized access to computer material (Section 3)** – Covers instances where an individual gains access to computer data or programs without authorization.

**Unauthorized access with intent to commit or facilitate commission of further offence (Section 4)** – This offence applies when unauthorized access is made with an intent to commit another crime involving fraud, dishonesty, or causing injury.

**Unauthorized modification of the contents of any computer (Section 5)** – Involves intentionally modifying computer content without authorization, which can affect data integrity or system operations.

**Wrongful communication (Section 6)** – Involves communicating passwords, codes, or other means of access to someone who is not authorized to receive them.

**Abetments and attempts punishable as offences (Section 7)** – Covers cases where a person abets, attempts, or prepares for any of the offences specified in the Act.

**Obstruction of search (Section 11)** – Criminalizes the act of obstructing, hindering, or delaying a police officer from conducting searches under the Act.

* + 1. Under which offence has the highest attack in question B.2. above applied to?

Based on the listed offences, the highest potential for attacks or misuse often pertains to Section 4: Unauthorized access with intent to commit or facilitate commission of further offence.

* + 1. What is your argument for your answer in C.3. above?

Section 4 of the Computer Crimes Act 1997, which addresses "Unauthorized access with intent to commit or facilitate commission of further offence," is likely the most relevant offence for high-impact cyber-attacks, as demonstrated by recent attack data. This section encompasses unauthorized access aimed at enabling further criminal actions, including fraud, data breaches, and system sabotage, all of which align closely with the motivations behind some of the most prevalent cyber-attacks.

For instance, a Q2 2024 cybersecurity report highlights five key attack types: malware, ransomware, vulnerability exploitation, account takeover, and targeted attacks. Malware, responsible for 22.7% of incidents, involves unauthorized infiltration, often to initiate further destructive actions or exfiltrate data. Ransomware attacks (15.4%) also exemplify unauthorized access leading to extortion, with the added tactic of double extortion if ransoms are unpaid. Vulnerability exploitation, accounting for 11.6% of incidents, involves unauthorized access via unpatched systems, enabling attackers to commit further acts like data theft or disruption. Similarly, account takeover attacks (10.2%) allow criminals to exploit user credentials, often with the intent to carry out subsequent fraudulent actions or data exfiltration. Targeted attacks (10%) further underscore this pattern, with attackers often maintaining prolonged, undetected access, preparing for more significant theft or sabotage.

The extensive impact and increasing frequency of these attack types indicate a heightened focus on unauthorized access as a precursor to additional cybercrimes. The inclusion of fraud, espionage, and extortion within Section 4's remit underlines the Act's recognition of this offence's serious and often multi-layered consequences. Consequently, Section 4 stands out as the most applicable for addressing modern, high-impact cyber-attacks that involve complex, intentional misuse of unauthorized access, underscoring the law's role in countering sophisticated cyber threats.

# TASK 2

1. Given a plain text “WE LOVE INFORMATION SECURITY”. Encrypt and decrypt back the plain text using the cryptography ciphers below:
   1. Caesar cipher.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | B | C | D | E | F | G | H | I | J | K | L | M |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

**ENCRYPTION**

K=? we assume 3 (default)

| **Plaintext Letter** | **Position (P)** | **Calculation (P + K) mod 26** | **Ciphertext Position (C)** | **Ciphertext Letter** |
| --- | --- | --- | --- | --- |
| W | 22 | (22 + 3) mod 26 = 25 | 25 | Z |
| E | 4 | (4 + 3) mod 26 = 7 | 7 | H |
| L | 11 | (11 + 3) mod 26 = 14 | 14 | O |
| O | 14 | (14 + 3) mod 26 = 17 | 17 | R |
| V | 21 | (21 + 3) mod 26 = 24 | 24 | Y |
| E | 4 | (4 + 3) mod 26 = 7 | 7 | H |
| I | 8 | (8 + 3) mod 26 = 11 | 11 | L |
| N | 13 | (13 + 3) mod 26 = 16 | 16 | Q |
| F | 5 | (5 + 3) mod 26 = 8 | 8 | I |
| O | 14 | (14 + 3) mod 26 = 17 | 17 | R |
| R | 17 | (17 + 3) mod 26 = 20 | 20 | U |
| M | 12 | (12 + 3) mod 26 = 15 | 15 | P |
| A | 0 | (0 + 3) mod 26 = 3 | 3 | D |
| T | 19 | (19 + 3) mod 26 = 22 | 22 | W |
| I | 8 | (8 + 3) mod 26 = 11 | 11 | L |
| O | 14 | (14 + 3) mod 26 = 17 | 17 | R |
| N | 13 | (13 + 3) mod 26 = 16 | 16 | Q |
| S | 18 | (18 + 3) mod 26 = 21 | 21 | V |
| E | 4 | (4 + 3) mod 26 = 7 | 7 | H |
| C | 2 | (2 + 3) mod 26 = 5 | 5 | F |
| U | 20 | (20 + 3) mod 26 = 23 | 23 | X |
| R | 17 | (17 + 3) mod 26 = 20 | 20 | U |
| I | 8 | (8 + 3) mod 26 = 11 | 11 | L |
| T | 19 | (19 + 3) mod 26 = 22 | 22 | W |
| Y | 24 | (24 + 3) mod 26 = 1 | 1 | B |

**Chipertext:** ZHORYHLQIRUPDWLRQVHFXULWB

**DECRPYTION**

| **Ciphertext Letter (C)** | **Position (C)** | **Calculation (C - K) mod 26** | **Plaintext Position (P)** | **Plaintext Letter** |
| --- | --- | --- | --- | --- |
| Z | 25 | (25 - 3) mod 26 = 22 | 22 | W |
| H | 7 | (7 - 3) mod 26 = 4 | 4 | E |
| O | 14 | (14 - 3) mod 26 = 11 | 11 | L |
| R | 17 | (17 - 3) mod 26 = 14 | 14 | O |
| Y | 24 | (24 - 3) mod 26 = 21 | 21 | V |
| H | 7 | (7 - 3) mod 26 = 4 | 4 | E |
| L | 11 | (11 - 3) mod 26 = 8 | 8 | I |
| Q | 16 | (16 - 3) mod 26 = 13 | 13 | N |
| I | 8 | (8 - 3) mod 26 = 5 | 5 | F |
| R | 17 | (17 - 3) mod 26 = 14 | 14 | O |
| U | 20 | (20 - 3) mod 26 = 17 | 17 | R |
| P | 15 | (15 - 3) mod 26 = 12 | 12 | M |
| D | 3 | (3 - 3) mod 26 = 0 | 0 | A |
| W | 22 | (22 - 3) mod 26 = 19 | 19 | T |
| L | 11 | (11 - 3) mod 26 = 8 | 8 | I |
| R | 17 | (17 - 3) mod 26 = 14 | 14 | O |
| Q | 16 | (16 - 3) mod 26 = 13 | 13 | N |
| V | 21 | (21 - 3) mod 26 = 18 | 18 | S |
| H | 7 | (7 - 3) mod 26 = 4 | 4 | E |
| F | 5 | (5 - 3) mod 26 = 2 | 2 | C |
| X | 23 | (23 - 3) mod 26 = 20 | 20 | U |
| U | 20 | (20 - 3) mod 26 = 17 | 17 | R |
| L | 11 | (11 - 3) mod 26 = 8 | 8 | I |
| W | 22 | (22 - 3) mod 26 = 19 | 19 | T |
| B | 1 | (1 - 3) mod 26 = (-2) mod 26 = 24 | 24 | Y |

* 1. Playfair cipher using a key “BALL”.

**ENCRYPTION**

PLAINTEXT: WE LOVE INFORMATION SECURITY

Key = BALL -> BAL (remove duplicate char)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

WE LO VE IN FO RM AT IO NS EC UR IT YZ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP | SX |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP | SX | HB |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP | SX | HB | QS |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP | SX | HB | QS | HU |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| B | A | L | C | D |
| E | F | G | H | I/J |
| K | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WE | LO | VE | IN | FO | RM | AT | IO | NS | EC | UR | IT | YZ |
| VF | CN | BK | GP | HM | WR | CR | HP | SX | HB | QS | HU | ZY |

VF CN BK GP HM WR CR HP SX HB QS HU ZY

Chipertext: VFCNBKGPHMWRCRHPSXHBQSHUZY

* 1. Vigenere cipher using a key “START”.

PLAINTEXT: WE LOVE INFORMATION SECURITY

|  |  |  |  |
| --- | --- | --- | --- |
| **P (num)** | **K (num)** | **(P+K) mod 26** | **C** |
| W (22) | S (18) | (22+18) mod 26 = 14 | O |
| E (4) | T (19) | (4+19) mod 26 = 23 | X |
| L (11) | A (0) | (11+0) mod 26 = 11 | L |
| O (14) | R (17) | (14+17) mod 26 = 5 | F |
| V (21) | T (19) | (21+19) mod 26 = 14 | O |
| E (4) | S (18) | (4+18) mod 26 = 22 | W |
| I (8) | T (19) | (8+19) mod 26 = 1 | B |
| N (13) | A (0) | (13+0) mod 26 = 13 | N |
| F (5) | R (17) | (5+17) mod 26 = 22 | W |
| O (14) | T (19) | (14+19) mod 26 = 7 | H |
| R (17) | S (18) | (17+18) mod 26 = 9 | J |
| M (12) | T (19) | (12+19) mod 26 = 5 | F |
| A (0) | A (0) | (0+0) mod 26 = 0 | A |
| T (19) | R (17) | (19+17) mod 26 = 10 | K |
| I (8) | T (19) | (8+19) mod 26 = 1 | B |
| O (14) | S (18) | (14+18) mod 26 = 6 | G |
| N (13) | T (19) | (13+19) mod 26 = 6 | G |
| S (18) | A (0) | (18+0) mod 26 = 18 | S |
| E (4) | R (17) | (4+17) mod 26 = 21 | V |
| C (2) | T (19) | (2+19) mod 26 = 21 | V |
| U (20) | S (18) | (20+18) mod 26 = 12 | M |
| R (17) | T (19) | (17+19) mod 26 = 10 | K |
| I (8) | A (0) | (8+0) mod 26 = 8 | I |
| T (19) | R (17) | (19+17) mod 26 = 10 | K |
| Y (24) | T (19) | (24+19) mod 26 = 17 | R |

**CHIPERTEXT:** OXLFOWBNWHJFAKBGGSVVMKIKR

**DECRPYTION**

|  |  |  |  |
| --- | --- | --- | --- |
| **C (num)** | **K (num)** | **(C - K) mod 26** | **P** |
| O (14) | S (18) | (14-18) mod 26 = 22 | W |
| X (23) | T (19) | (23-19) mod 26 = 4 | E |
| L (11) | A (0) | (11-0) mod 26 = 11 | L |
| F (5) | R (17) | (5-17) mod 26 = 14 | O |
| O (14) | T (19) | (14-19) mod 26 = 21 | V |
| W (22) | S (18) | (22-18) mod 26 = 4 | E |
| B (1) | T (19) | (1-19) mod 26 = 8 | I |
| N (13) | A (0) | (13-0) mod 26 = 13 | N |
| W (22) | R (17) | (22-17) mod 26 = 5 | F |
| H (7) | T (19) | (7-19) mod 26 = 14 | O |
| J (9) | S (18) | (9-18) mod 26 = 17 | R |
| F (5) | T (19) | (5-19) mod 26 = 12 | M |
| A (0) | A (0) | (0-0) mod 26 = 0 | A |
| K (10) | R (17) | (10-17) mod 26 = 19 | T |
| B (1) | T (19) | (1-19) mod 26 = 8 | I |
| G (6) | S (18) | (6-18) mod 26 = 14 | O |
| G (6) | T (19) | (6-19) mod 26 = 13 | N |
| S (18) | A (0) | (18-0) mod 26 = 18 | S |
| V (21) | R (17) | (21-17) mod 26 = 4 | E |
| V (21) | T (19) | (21-19) mod 26 = 2 | C |
| M (12) | S (18) | (12-18) mod 26 = 20 | U |
| K (10) | T (19) | (10-19) mod 26 = 17 | R |
| I (8) | A (0) | (8-0) mod 26 = 8 | I |
| K (10) | R (17) | (10-17) mod 26 = 19 | T |
| R (17) | T (19) | (17-19) mod 26 = 24 | Y |

Plaintext: WE LOVE INFORMATION SECURITY

* 1. Rail fence cipher with a key is 4.

ENCRYPTION

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W |  |  |  |  |  | I |  |  |  |  |  | A |  |  |  |  |  | E |  |  |  |  |  | Y |
|  | E |  |  |  | E |  | N |  |  |  | M |  | T |  |  |  | S |  | C |  |  |  | T |  |
|  |  | L |  | V |  |  |  | F |  | R |  |  |  | I |  | N |  |  |  | U |  | I |  |  |
|  |  |  | O |  |  |  |  |  | O |  |  |  |  |  | O |  |  |  |  |  | R |  |  |  |

WIAEY

EENMTSCT

LVFRINUI

OOOR

**Chipertext:** WIAEYEENMTSCTLVFRINUIOOOR

**DECRYPT:**

WIAEY EENMTSCT LVFRINUI OOOR

**Assign Characters to Rails: (key=4)**

Rail 0: Positions 0, 6, 12, 18, 24 → W, I, A, E, Y (5 characters)

Rail 1: Positions 1, 5, 7, 11, 13, 17, 19, 23 → E, E, N, M, T, S, C, T (8 characters)

Rail 2: Positions 2, 4, 8, 10, 14, 16, 20, 22 → L, V, F, R, I, N, U, I (8 characters)

Rail 3: Positions 3, 9, 15, 21 → O, O, O, R (4 characters)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W |  |  |  |  |  | I |  |  |  |  |  | A |  |  |  |  |  | E |  |  |  |  |  | Y |
|  | E |  |  |  | E |  | N |  |  |  | M |  | T |  |  |  | S |  | C |  |  |  | T |  |
|  |  | L |  | V |  |  |  | F |  | R |  |  |  | I |  | N |  |  |  | U |  | I |  |  |
|  |  |  | O |  |  |  |  |  | O |  |  |  |  |  | O |  |  |  |  |  | R |  |  |  |

Decrpyt text = WE LOVE INFORMATION SECURITY

* 1. Transposition cipher with a key is 31524.

Determining the grid Dimension

**Create the grid**

| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
| --- | --- | --- | --- | --- |
| W | E | L | O | V |
| E | I | N | F | O |
| R | M | A | T | I |
| O | N | S | E | C |
| U | R | I | T | Y |

Reorder Column with a key 31524

Col 3: LNASI

Col 1: WEROU

Col 5: VOICY

Col 2: EIMNR

Col 4: OFTET

Reassemble!

Encrpted Text: LNASIWEROUVOICYEIMNROFTET

Decrpyt:

Determining the grid Dimension

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LNASI**WEROUVOICYEIMNROFTET

**3**1524

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
|  |  | L |  |  |
|  |  | N |  |  |
|  |  | A |  |  |
|  |  | S |  |  |
|  |  | I |  |  |

**WEROU**VOICYEIMNROFTET

**1**524

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
| W |  | L |  |  |
| E |  | N |  |  |
| R |  | A |  |  |
| O |  | S |  |  |
| U |  | I |  |  |

**VOICY**EIMNROFTET

**5**24

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
| W |  | L |  | V |
| E |  | N |  | O |
| R |  | A |  | I |
| O |  | S |  | C |
| U |  | I |  | Y |

**EIMNR**OFTET

**2**4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
| W | E | L |  | V |
| E | I | N |  | O |
| R | M | A |  | I |
| O | N | S |  | C |
| U | R | I |  | Y |

**OFTET**

**4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Col 1** | **Col 2** | **Col 3** | **Col 4** | **Col 5** |
| W | E | L | O | V |
| E | I | N | F | O |
| R | M | A | T | I |
| O | N | S | E | C |
| U | R | I | T | Y |

PLAINTEXT: WELOVEINFORMATIONSECURITY

* 1. Encrypt and decrypt back the plain text using RSA algorithm with p=5, q=11 and public key e=7. Do the encryption and decryption for each alphabet. Given the encryption formula is *C=Me mod n* and the decryption formula is *M=Cd mod n*.

**ENCRYPTION**

|  |  |  |
| --- | --- | --- |
| **Letter** | **M (Numerical Value)** |  |
| W | 22 |  |
| E | 4 |  |
| L | 11 |  |
| O | 14 |  |
| V | 21 |  |
| E | 4 |  |
| I | 8 |  |
| N | 13 |  |
| F | 5 | 25 |
| O | 14 |  |
| R | 17 |  |
| M | 12 |  |
| A | 0 |  |
| T | 19 |  |
| I | 8 |  |
| O | 14 |  |
| N | 13 |  |
| S | 18 |  |
| E | 4 |  |
| C | 2 |  |
| U | 20 |  |
| R | 17 |  |
| I | 8 |  |
| T | 19 |  |
| Y | 24 |  |

CHIPERTEXT=[33, 49, 11, 9, 21, 49, 2, 7, 25, 9, 8, 23, 0, 24, 2, 9, 7, 17, 49, 18, 15, 8, 2, 24, 29]

**DECRYPTION**

M=Cd mod n

|  |  |  |
| --- | --- | --- |
| **C (Ciphertext)** |  | **Decrypted Letter** |
| 33 |  | W |
| 49 |  | E |
| 11 |  | L |
| 9 |  | O |
| 21 |  | V |
| 49 |  | E |
| 2 |  | I |
| 7 |  | N |
| 25 |  | F |
| 9 |  | O |
| 8 |  | R |
| 23 |  | M |
| 0 |  | A |
| 24 |  | T |
| 2 |  | I |
| 9 |  | O |
| 7 |  | N |
| 17 |  | S |
| 49 |  | E |
| 18 |  | C |
| 15 |  | U |
| 8 |  | R |
| 2 |  | I |
| 24 |  | T |
| 29 |  | Y |

PLAINTEXT: WELOVEINFORMATIONSECURITY

* 1. Assume Hilmi and Jenny use a Diffie-Hellman protocol as a method to generate a shared private key with which they can then exchange information across an insecure channel. Hilmi and Jenny agree on using prime number, n = 47 and root number, g = 43. Hilmi’s random number hr = 3 and

Jenny’s random number jr = 5. Compute the public keys (Hilmipb and Jennypb) and the shared private keys (Hilmisc and Jennysc) of the Diffie-Hellman arrangement protocol. Use the shared secret key to encrypt and decrypt the plain text using a monoalphabetic substitution cipher.

**Answer:**

**Step I** generate a shared private key with Diffie-Hellman protocol

|  |  |
| --- | --- |
|  |  |
|  |  |

**ENCRYPTION** monoalphabetic substitution cipher

Plaintext: WE LOVE INFORMATION SECURITY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Plaintext Letter** | **Position (P)** | **Calculation (P + K) mod 26** | **Ciphertext Position (C)** | **Ciphertext Letter** |
| W | 22 | 22 + 13 mod 26 = 9 | 9 | J |
| E | 4 | 4 + 13 mod 26 = 17 | 17 | R |
| L | 11 | 11 + 13 mod 26 = 24 | 24 | Y |
| O | 14 | 14 + 13 mod 26 = 1 | 1 | B |
| V | 21 | 21 + 13 mod 26 = 8 | 8 | I |
| E | 4 | 4 + 13 mod 26 = 17 | 17 | R |
| I | 8 | 8 + 13 mod 26 = 21 | 21 | V |
| N | 13 | 13 + 13 mod 26 = 0 | 0 | A |
| F | 5 | 5 + 13 mod 26 = 18 | 18 | S |
| O | 14 | 14 + 13 mod 26 = 1 | 1 | B |
| R | 17 | 17 + 13 mod 26 = 4 | 4 | E |
| M | 12 | 12 + 13 mod 26 = 25 | 25 | Z |
| A | 0 | 0 + 13 mod 26 = 13 | 13 | N |
| T | 19 | 19 + 13 mod 26 = 6 | 6 | G |
| I | 8 | 8 + 13 mod 26 = 21 | 21 | V |
| O | 14 | 14 + 13 mod 26 = 1 | 1 | B |
| N | 13 | 13 + 13 mod 26 = 0 | 0 | A |
| S | 18 | 18 + 13 mod 26 = 5 | 5 | F |
| E | 4 | 4 + 13 mod 26 = 17 | 17 | R |
| C | 2 | 2 + 13 mod 26 = 15 | 15 | P |
| U | 20 | 20 + 13 mod 26 = 7 | 7 | H |
| R | 17 | 17 + 13 mod 26 = 4 | 4 | E |
| I | 8 | 8 + 13 mod 26 = 21 | 21 | V |
| T | 19 | 19 + 13 mod 26 = 6 | 6 | G |
| Y | 24 | 24 + 13 mod 26 = 11 | 11 | L |

Chipertext: JR YBIR VASBEZNGVBA FRPHEVGL

**DECRYPTION**

Chipertext: JR YBIR VASBEZNGVBA FRPHEVGL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ciphertext Letter** | **Position (C)** | **Calculation (C - K) mod 26** | **Plaintext Position (P)** | **Plaintext Letter** |
| J | 9 | 9 - 13 mod 26 = 22 | 22 | W |
| R | 17 | 17 - 13 mod 26 = 4 | 4 | E |
| Y | 24 | 24 - 13 mod 26 = 11 | 11 | L |
| B | 1 | 1 - 13 mod 26 = 14 | 14 | O |
| I | 8 | 8 - 13 mod 26 = 21 | 21 | V |
| R | 17 | 17 - 13 mod 26 = 4 | 4 | E |
| V | 21 | 21 - 13 mod 26 = 8 | 8 | I |
| A | 0 | 0 - 13 mod 26 = 13 | 13 | N |
| S | 18 | 18 - 13 mod 26 = 5 | 5 | F |
| B | 1 | 1 - 13 mod 26 = 14 | 14 | O |
| E | 4 | 4 - 13 mod 26 = 17 | 17 | R |
| Z | 25 | 25 - 13 mod 26 = 12 | 12 | M |
| N | 13 | 13 - 13 mod 26 = 0 | 0 | A |
| G | 6 | 6 - 13 mod 26 = 19 | 19 | T |
| V | 21 | 21 - 13 mod 26 = 8 | 8 | I |
| B | 1 | 1 - 13 mod 26 = 14 | 14 | O |
| A | 0 | 0 - 13 mod 26 = 13 | 13 | N |
| F | 5 | 5 - 13 mod 26 = 18 | 18 | S |
| R | 17 | 17 - 13 mod 26 = 4 | 4 | E |
| P | 15 | 15 - 13 mod 26 = 2 | 2 | C |
| H | 7 | 7 - 13 mod 26 = 20 | 20 | U |
| E | 4 | 4 - 13 mod 26 = 17 | 17 | R |
| V | 21 | 21 - 13 mod 26 = 8 | 8 | I |
| G | 6 | 6 - 13 mod 26 = 19 | 19 | T |
| L | 11 | 11 - 13 mod 26 = 24 | 24 | Y |

Plaintext: WE LOVE INFORMATION SECURITY

***Provide a step-by-step work on how you get the answer.***

1. **Cryptography Code**

Create your simple cipher code using any language. Write your pseudocode and algorithm for your version of encryption and decryption. Execute the code that will input a string of text from the user and generate the cipher text. After that, the cipher text will be input for the decryption algorithm and generate back the original string of text. Show the output.

***Provide the free error code and show the executable output (explain the output)***

**Algorithm and Pseudocode:**

|  |
| --- |
| **PROGRAM Encryalactic**  A program to encrypt and decrypt text using a galactic alphabet substitution cipher, where each Latin character is mapped to a unique galactic symbol. The program implements bidirectional conversion between standard text and galactic cipher text.  **DECLARATIONS:**  galacticMap: associative array of <character, string> // Mapping of Latin to galactic symbols  reverseMap: associative array of <string, character> // Inverse mapping for decryption  plaintext, ciphertext: string // Input/output text strings  i: integer // Loop counter  **1. ENCRYPTION ALGORITHM**  Input: Plain text string (Latin alphabet)  Output: Cipher text string (Galactic symbols)  BEGIN ENCRYPTION  1. Initialize galacticMap with Latin-to-Galactic character mappings  2. Initialize empty result string  3. For each character in input string:  3.1. Get current character  3.2. IF character exists in galacticMap THEN  - Append corresponding galactic symbol to result  3.3. ELSE  - Append original character to result unchanged  4. Return result string  END ENCRYPTION  **Pseudocode encrypt(text):**  /\*  INPUT: text - string to be encrypted  OUTPUT: encrypted text using galactic symbols  \*/  1. Initialize result as empty string  2. FOR each character c in text:  2.1. IF c exists in galacticMap:  result ← result + galacticMap[c]  2.2. ELSE:  result ← result + c // Preserve non-mapped characters  3. RETURN result  **2. DECRYPTION ALGORITHM**  Input: Cipher text string (Galactic symbols)  Output: Plain text string (Latin alphabet)  BEGIN DECRYPTION  1. Initialize reverseMap by inverting galacticMap  2. Initialize empty result string  3. Initialize position counter i = 0  4. While i < length of input string:  4.1. IF i+1 < input length AND (current char + next char) exists in reverseMap THEN  - Append corresponding Latin character to result  - Increment i by 2 (skip next character)  4.2. ELSE  - IF current char exists in reverseMap THEN  \* Append corresponding Latin character to result  - ELSE  \* Append original character unchanged  - Increment i by 1  5. Return result string  END DECRYPTION  **Pseudocode decryption:**  /\*  INPUT: text - galactic cipher text to be decrypted  OUTPUT: decrypted text in Latin alphabet  \*/  1. Initialize:  - result as empty string  - reverseMap by inverting galacticMap  - i as 0  2. WHILE i < length of text:  2.1. IF i + 1 < text length AND  (text[i] + text[i+1]) exists in reverseMap:  // Handle two-character galactic symbols  result ← result + reverseMap[text[i] + text[i+1]]  i ← i + 2  2.2. ELSE:  // Handle single characters  IF text[i] exists in reverseMap:  result ← result + reverseMap[text[i]]  ELSE:  result ← result + text[i]  i ← i + 1  3. RETURN result  **SUPPORTING DATA STRUCTURES:**  1. galacticMap (Latin to Galactic):  - Key: Latin character (A-Z, a-z)  - Value: Corresponding galactic symbol  Example: {'A':'ᔑ', 'B':'ʖ', 'C':'ᓵ', ...}  2. reverseMap (Galactic to Latin):  - Key: Galactic symbol  - Value: Corresponding Latin character  Example: {'ᔑ':'A', 'ʖ':'B', 'ᓵ':'C', ...}  **COMPLEXITY ANALYSIS:**  1. Encryption:  - Time Complexity: O(n) where n is input string length  - Space Complexity: O(n) for result string  2. Decryption:  - Time Complexity: O(n) where n is input string length  - Space Complexity: O(n) for result string  **ERROR HANDLING:**  1. Invalid Characters:  - Non-mapped characters are preserved unchanged  - Special characters and spaces remain unmodified  2. Edge Cases:  - Empty string returns empty string  - Single character processing in decryption  - Multi-byte galactic symbol handling |

Implement to Typescript

Source code:

<https://github.com/IRedDragonICY/encryalactic>

Focus mainly encryption/decryption functionality

page.tsx

|  |
| --- |
| …(Other codes)…  const galacticMap: Record<string, string> = {  A: "ᔑ", B: "ʖ", C: "ᓵ", D: "↸", E: "ᒷ", F: "⎓", G: "⊣", H: "⍑", I: "╎", J: "⋮",  K: "ꖌ", L: "ꖎ", M: "ᒲ", N: "リ", O: "𝙹", P: "!¡", Q: "ᑑ", R: "∷", S: "ᓭ", T: "ℸ",  U: "⚍", V: "⍊", W: "∴", X: "∵", Y: "⨅", Z: "⨀",  a: "ᔑ", b: "ʖ", c: "ᓵ", d: "↸", e: "ᒷ", f: "⎓", g: "⊣", h: "⍑", i: "╎", j: "⋮",  k: "ꖌ", l: "ꖎ", m: "ᒲ", n: "リ", o: "𝙹", p: "!¡", q: "ᑑ", r: "∷", s: "ᓭ", t: "ℸ",  u: "⚍", v: "⍊", w: "∴", x: "∵", y: "⨅", z: "⨀" };  const encrypt = (text: string) =>  text.split("").map((c) => galacticMap[c] || c).join("");  const decrypt = (text: string) => {  const rev = *Object*.entries(galacticMap).reduce<Record<string, string>>(  (acc, [latin, galactic]) => {  acc[galactic] = latin;  return acc;  },  {}  );  let res = "";  let i = 0;  while (i < text.length) {  if (i + 1 < text.length && rev[text[i] + text[i + 1]]) {  res += rev[text[i] + text[i + 1]];  i += 2;  } else {  res += rev[text[i]] || text[i];  i++;  }  }  return res; };  …(other codes)… |

A screenshot of a computer

Description automatically generated

**Demo web:**

<https://encryalactic.vercel.app/>

**Example Encryption**

|  |  |  |
| --- | --- | --- |
| Plaintext | : | I love anime |
| Chipertext | : | ╎ ꖎ𝙹⍊ᒷ ᔑリ╎ᒲᒷ\ |

A screenshot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Plaintext | : | data and network security |
| Chipertext | : | ↸ᔑℸᔑ ᔑリ↸ リᒷℸ∴𝙹∷ꖌ ᓭᒷᓵ⚍∷╎ℸ⨅ |

A screenshot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Plaintext | : | xyzartificial inteligencexyz |
| Chipertext | : | ∵⨅⨀ᔑ∷ℸ╎⎓╎ᓵ╎ᔑꖎ ╎リℸᒷꖎ╎⊣ᒷリᓵᒷ∵⨅⨀ |

A screenshot of a computer

Description automatically generated

**Example decryption**

|  |  |  |
| --- | --- | --- |
| Chipertext | : | ᒷꖎᔑ╎リᔑ |
| Plaintext | : | elaina |

A screen shot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Chipertext | : | ℸ⍑ᒷ ᓭꖌ⨅ ╎ᓭ ʖꖎ⚍ᒷ |
| Plaintext | : | the sky is blue |

A screen shot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Chipertext | : | ℸ⍑ᒷ ᓭꖌ⨅ ╎ᓭ ʖꖎ⚍ᒷ |
| Plaintext | : | Hendianto Mohammad Farid |

A screenshot of a computer

Description automatically generated

**Marking Guide**

|  |  |  |  |
| --- | --- | --- | --- |
| Item | 0 | In between | Full mark |
| Front page | Not provide |  | Provide all |
| Task 1 | Not provide | Missing task and not complete | Provide all and complete |
| Task 2 | Not provide | Missing task and not complete | Provide all and complete |
| List of references | Not provide |  | Correct and complete |