Group work 1:

Network Security and Cryptography

Question 1

In a secure communication experiment, two students, **Alice** and **Brian**, agree to protect their text messages using a **double row–column transposition cipher**. Instead of using numerical digits as the key, they decide to use a six-letter word to determine the column order. Each letter in the keyword is assigned a positional number based on its alphabetical order. The encryption process involves writing the plaintext in a rectangular grid (rows and columns) under the key letters, rearranging columns according to the alphabetical order of the key, and then reading off the ciphertext column by column. The procedure is repeated **twice** to form the final ciphertext this is known as **double transposition**.
The pair select the word **"PLANET"** as their key for the 6-column grid. Alice wants to send Brian the confidential message:
"CRYPTOGRAPHY IS FUN AT THE MOMENT FOR SURE"
Spaces are to be removed before encryption.
Required:
a) Construct the transposition table using the keyword "PLANET" and perform double encryption of the plaintext "CRYPTOGRAPHYISFUNATTHEMOMENTFORSURE."
b) Decrypt the resulting ciphertext to verify the accuracy of your encryption process.
c) with the same key and by double transposition, decrypt: "ITGTTRXEOLENGXNIISSENVYAHIEXUSKIEHORFIBTIX"

Question 2:

In a basic cryptography experiment, two students, **Alice** and **Brian**, decide to protect their messages using a monoalphabetic substitution cipher. This classical encryption technique replaces each letter of the plaintext alphabet with another unique letter of the ciphertext alphabet. The relationship between plaintext and ciphertext letters is determined by a substitution key, which remains constant for all letters in the message.
Unlike the Caesar cipher, where letters are shifted by a fixed number of positions, the monoalphabetic cipher allows any random rearrangement of the alphabet, significantly increasing security. However, the cipher's main weakness lies in its vulnerability to frequency analysis, where attackers analyze letter frequency patterns to infer the substitution key.
For their communication, Alice and Brian agree on the following substitution key:

Plaintext Alphabet:
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
Ciphertext Alphabet:
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
Alice wants to send Brian the message:
“MEET ME IN THE LAB IN THE AFTERNOON TODAY”
Required:
a) Using the given substitution key, **encrypt** Alice’s message.
b) **Analyze** the main weakness of the monoalphabetic cipher and explain how an attacker could exploit it.

Question 3

In a data security experiment, a team of software engineering students at Kigali Institute of Technology is developing a lightweight encryption system for short text messages. Since their communication software must handle both uppercase and lowercase letters, as well as spaces, commas, and periods, they decide to implement an Affine Cipher modulo 55 to accommodate all 52 alphabetic characters and three punctuation marks.

To represent characters numerically, they assign the following mappings:

- Uppercase letters (A–Z) → 0 to 25
- Lowercase letters (a–z) → 26 to 51
- Space = 52, Comma = 53, Period = 54

Consider the encryption function: $E(x) \equiv y = (14x + 20) \bmod 55$
Encrypt the plaintext: Good morning my dear, I love you.
Find the decryption function and the ciphertext you got in the previous message to check your accuracy.

Question 4:
Two students communicate on unsecured communication channel. They started encrypting their message using Hill cipher with the following key. $K = \begin{pmatrix} -3 & 0 & 1 \\ 2 & -5 & 3 \\ 7 & -6 & 2 \end{pmatrix}$ *modulo* 26. Student A wishes to send a message to student B, **“I am bored at home, come.**” Ignore punctuations and encrypt the message. Use the appropriate key to decrypt the ciphertext to whether your encryption process went well.

Question 5

In October 2024, **Horizon Logistics Ltd**, a medium-sized transportation company, experienced a serious network incident that disrupted its nationwide shipment tracking system. The company's IT infrastructure relied on a central data server connected to regional branches through a virtual private network (VPN). The incident began when several employees reported that their computers were unusually slow and that unfamiliar programs were running in the background. A detailed investigation revealed that an employee had unknowingly downloaded an attachment from a fake email disguised as a supplier invoice. Once opened, the document silently executed hidden code that gave external attackers remote access to the company's internal network. Within hours, customer delivery data and financial records were being copied to unknown destinations. Some workstations began displaying intrusive advertising pop-ups, while others experienced browser redirections to malicious websites. These symptoms caused severe performance degradation and exposed sensitive corporate information. Two days later, the company's central database became inaccessible. Files were renamed with unreadable extensions, and a digital note appeared demanding payment in cryptocurrency to restore access. Around the same time, the IT team discovered that keystrokes and login credentials were being transmitted to an external IP address each time users logged into their ERP system. Further analysis confirmed that several types of malicious software were operating simultaneously some collecting data silently, others spreading through the network, and one designed to encrypt essential business files.

Horizon Logistics temporarily disconnected all regional offices from the VPN, engaged external cybersecurity consultants, and initiated a recovery plan using offline backups. The financial impact was significant, as shipment data and invoices for over 300 clients were delayed for nearly a week. Management later acknowledged that poor user awareness, outdated antivirus software, and weak access control policies had contributed to the breach.

Required:
a) Carefully read the case study and identify at least four different types of cyberattacks that affected Horizon Logistics Ltd. Provide appropriate names for each and describe how they manifested in the scenario.
b) Suggest effective preventive measures both technical and administrative that the company should implement to reduce the likelihood of similar network breaches in the future.

Question 6

In 2024, **Bright Wave Communications**, a digital service provider, began upgrading its internal data protection system to enhance secure communication between departments. Previously, the company relied on symmetric encryption, where a single shared key was used for both encryption and decryption. Although effective for small-scale operations, this approach posed serious challenges in key management every pair of communicating users required a unique secret key, making the system difficult to scale and vulnerable to interception during key exchange.

To solve this issue, the cybersecurity team adopted public-key encryption, which uses two mathematically related keys: a public key for encryption and a private key for decryption. This structure eliminates the need to share secret keys directly, allowing anyone to send an encrypted message securely using only the recipient’s public key. The recipient alone, possessing the private key, can decrypt it. One of the most widely used public-key algorithms is the RSA cryptosystem, named after its inventors Rivest, Shamir, and Adleman. RSA’s strength lies in the mathematical difficulty of factoring large composite numbers derived from prime numbers.

To test the concept, Bright Wave’s cryptography analyst proposes creating an RSA system using two prime numbers: $p=31$ and $q=29$

Required:

a) Using p and q, construct an RSA cryptosystem by determining n, $\varphi(n)$, selecting a suitable public exponent e, and computing the private key d.

b) Discuss the strengths of the RSA cryptosystem compared to symmetric encryption methods in terms of key distribution and scalability.

c) Analyze the weaknesses or vulnerabilities of RSA, particularly when small prime numbers are used.

d) Encrypt the plaintext 4 and decrypt the ciphertext 3.

Notice: Use Microsoft Excel or a convenient programming of your choice for some computations. However, you will provide the code and the name of the programming language that you have used.