Computer security, information security, and network security are interrelated but distinct fields focused on protecting digital assets. Computer security focuses on protecting individual computers and devices, while network security focuses on protecting the infrastructure and data flowing within a network. Information security encompasses all aspects of protecting information, regardless of its location or format,

Computer Security:

- ➢ Focuses on protecting individual computers, devices, and software from threats like malware, viruses, and unauthorized access.
- ➢ **Goal is** to ensure the integrity, confidentiality, and availability of data on a single machine.
- **Examples:**

  Antivirus software, firewall configuration on a single device, and security updates for operating systems.

Network Security:

- ➢ Focuses on protecting the network infrastructure and data transmitted across it, including firewalls, intrusion detection systems, and VPNs.
- ➢ **Goal is to** ensure secure communication and data transmission within and between networks.
- **Examples:**
  Implementing strong network protocols, configuring firewalls to block unauthorized access, and using VPNs for secure communication.

Information Security:

- ➢ A broader term encompassing the protection of all forms of information, including electronic data, physical documents, and knowledge, regardless of where it is located.
- ➢ Goal is to ensure the confidentiality, integrity, and availability of information assets, as well as compliance with relevant regulations and standards.
- **Examples:**

  Implementing access controls, encryption, secure backups, and disaster recovery plans.

Information Security (InfoSec)

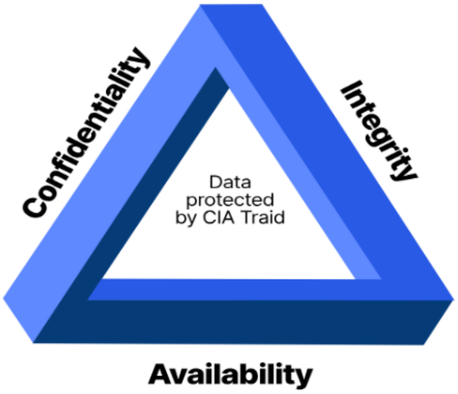
- Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect Data/information.
- This includes policy settings that prevent unauthorized people from accessing business or personal information.
- InfoSec covers a wide range of fields, from network and infrastructure security to testing and auditing.
- Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.
- The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

Types of Data

1. At rest
2. In motion

Basic Elements to secure Data/Information

- CIA Triad Information Security
  - **Confidentiality**
  - **Integrity**
  - **Availability**



Confidentiality

Confidentiality means keeping data a secret from everyone except those who we want to access it. The ISO/IEC 27000:2018 defines it as "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes." In practice, confidentiality ensures that sensitive information is protected from unauthorized access or disclosure. This is often achieved through mechanisms like encryption, access controls, and secure communication channels.

Integrity

Integrity ensures that data **hasn't become corrupted, tampered with, or altered in an unauthorized manner**. The ISO/IEC 27000:2018 defines it as "The property of accuracy and completeness." Maintaining data integrity means ensuring that information remains accurate, consistent, and trustworthy throughout its lifecycle. This is often achieved through methods such as hashing, digital signatures, and version control systems.

Availability

Availability means that data is readily accessible to authorized parties when they need it. The ISO/IEC 27000:2018 defines it as "The property of being accessible and usable upon demand by an authorized entity." Ensuring availability involves implementing robust systems, backup solutions, and disaster recovery plans to prevent disruptions and maintain access to critical information and services.

Two more terminologies:

- Authenticity
- Accountability

Computer Security Challenges

1. Not simple — easy to get it wrong
2. Must consider potential attacks,
3. Procedures used counter-intuitive
4. Involve algorithms and secret info
5. Must decide where to deploy mechanisms
6. Battle of wits between attacker / admin
7. Not perceived on benefit until fails.
8. Requires regular monitoring a process, not an event
9. too often an after-thought
10. Security should user friendly

Encryption

- Encryption is the process of converting plaintext into ciphertext using an encryption algorithm and a secret key. There are several terminologies used in encryption, which are:
  1. **Plaintext:** The original message or data that is to be encrypted.
  2. **Ciphertext:** The encrypted message or data that is produced as a result of the encryption process.
  3. **Encryption algorithm:** A mathematical formula used to convert plaintext into ciphertext.
  4. **Key:** A secret code or password used to encrypt and decrypt data.
  5. Symmetric encryption: A type of encryption where the same key is used for both encryption and decryption.
  6. **Asymmetric encryption:** A type of encryption where two different keys, a public key and a private key, are used for encryption and decryption respectively.
  7. **Public key:** A key that is publicly available and can be shared with anyone for encryption.
  8. **Private key:** A key that is kept secret and is used for decryption.
  9. **Key length:** The length of the key used in encryption. Longer keys are generally considered more secure.
  10. **Block cipher:** A type of encryption algorithm that encrypts data in fixed-sized blocks.
  11. **Stream cipher:** A type of encryption algorithm that encrypts data one-bit or byte at a time.
  12. **Hash function**: A mathematical function that takes a message or data as input and produces a fixed-size output known as a hash. Hash functions are commonly used for data integrity and authentication.
  13. **Encipher(encrypt):**
  14. **Decipher (Decrypt):**
  15. **Cryptography:** Study of encryption principles/Methods
  16. **Cryptanalysis (Codebreaking):** Study of principles/Methods of deciphering ciphertext without knowing key.
  17. **Cryptology:** field of both Cryptography and cryptanalysis

Type of operation

The type of operations used for transforming plaintext to ciphertext

❖ **Substitution**

- substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element
- It can be **monoalphabetic** or **polyalphabetic**

❖ **Transposition**

- Transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

❖ **Product**

- Product system involve multiple stages of Substitution and Transposition

Encryption and decryption

❖ **Encryption**

is the process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver. Encryption is done by using encryption key.

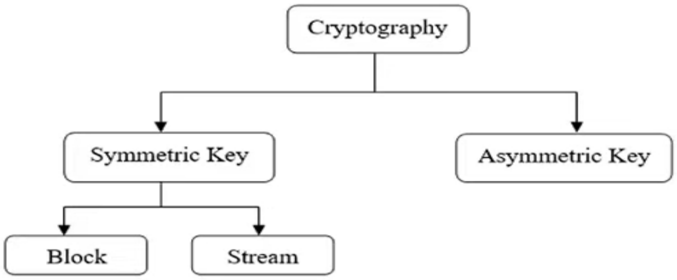
❖ **Decryption**

is the process of taking encrypted text or cipher text and converting it back into original text (plain text) that we can read and understand, It is done by using decryption key.

Types of encryption algorithms

There are two types of encryption algorithms:

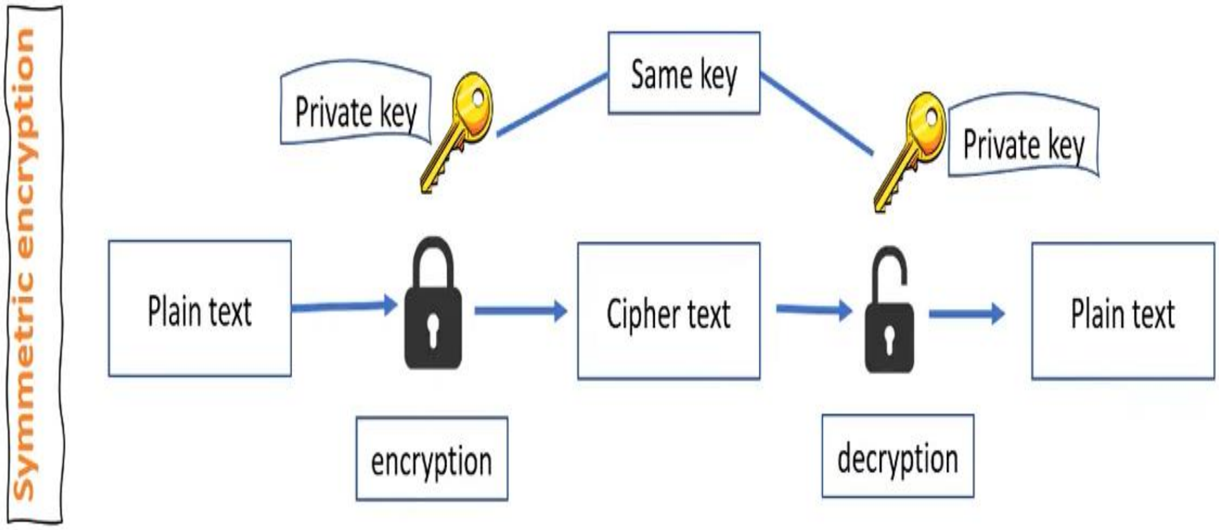
1. **Symmetric/private Key** (also called shared key algorithm)
2. **Asymmetric/Public Key** (also known as public key algorithm).



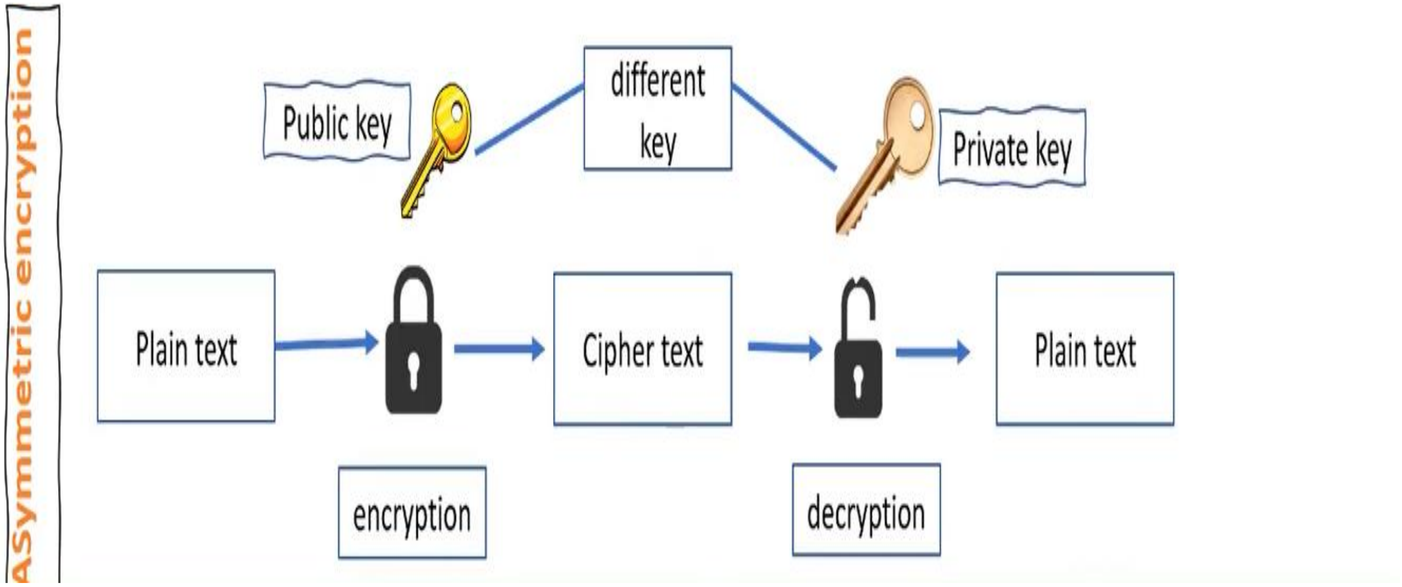
- **Symmetric encryption** uses the same key for encryption and decryption. Because it uses the same key, symmetric encryption can be more cost effective for the security it provides. That said, it is important to invest more in securely storing data when using symmetric encryption.

Examples:

1. Advanced Encryption Standard (AES) – 128, 192, 256 bits
2. Data Encryption Standard (DES)
3. Triple Data Encryption Standard (Triple DES) – advanced form of DES
4. Twofish - 128 bits – successor of Blowfish
5. Rivest Cipher 4 (RC4)
6. QUAD (Cipher)
7. Vigenere
8. Playfair

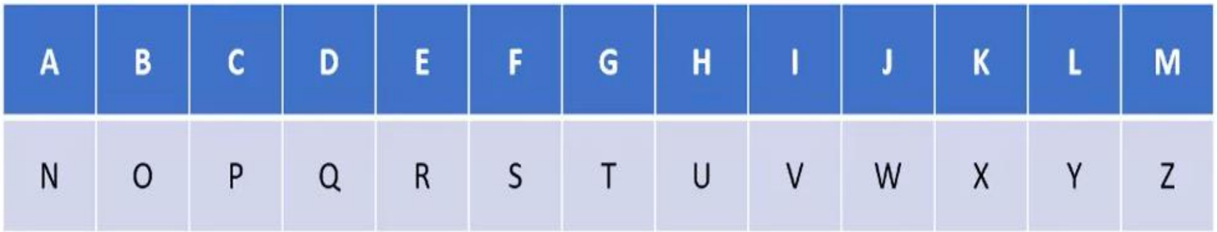


- **Asymmetric encryption** uses two separate keys: a public key and a private key. a public key is used to encrypt the data while a private key is required to decrypt the data. The private key is only given to users with authorized access. As a result, asymmetric encryption can be more effective, but it is also more costly.
  - The **public key** can only be used to encrypt the message and the **private key** can only be used to decrypt it.
  - This allows a user to freely distribute his or her public key to people who are likely to want to communicate with him or her without worry of compromise because only someone with the private key can decrypt a message.
  - To secure information between two users, the sender encrypts the message using the public key of the receiver. The receiver then uses the private key to decrypt the message.
  - The best-known public-key cryptosystem is RSA, named after its inventors: Rivest, Shamir, and Adleman.



ROT 13

- **ROT13** is a simple letter substitution cipher that replaces a letter with the 13th letter after it in the alphabet. it is **monoalphabetic cipher.**



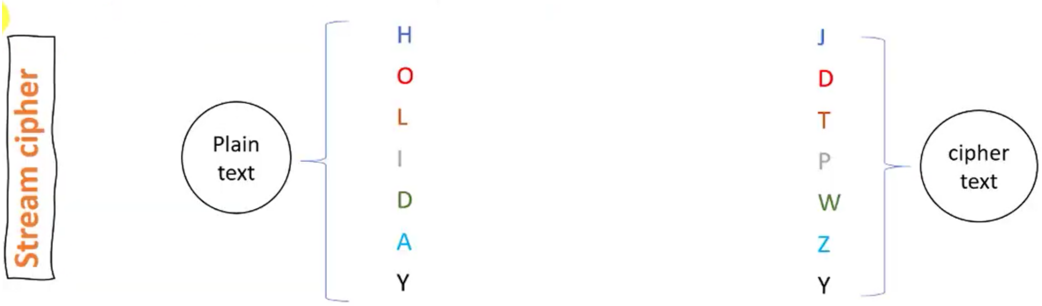
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- **ROT13** also known as Caesar Cipher, is a substitution cipher that replaces each letter of the alphabet with the letter 13 positions ahead of it.
- For example, the letter A is replaced with N, B with O, and so on. The process is reversible, and the same method is used to **decrypt** the message. The letter N is replaced with A, O with B, and so on.

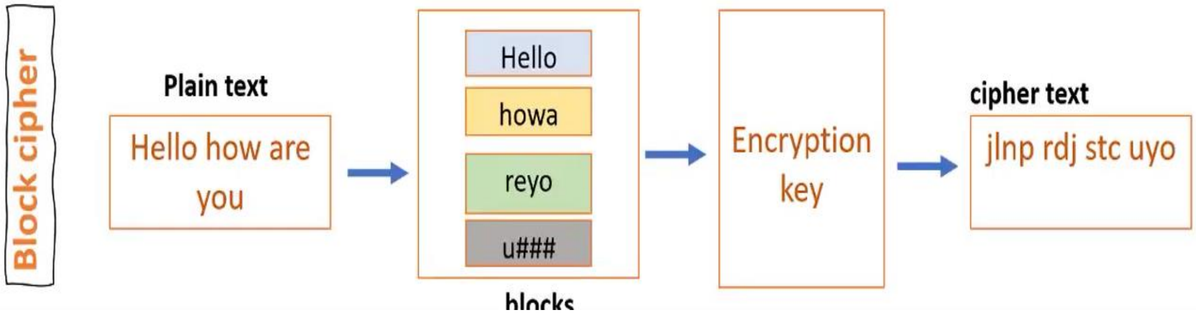
Example:
Plain Text: **SECURITY**
Cipher Text: **FRPHEVGL**

Stream VS Block Cipher

- A Stream cipher encrypts data one bit or one byte at a time rather than in fixed-size blocks in block cipher.
- It generates a keystream that is combined with the plaintext to the produce ciphertext.



- A **block cipher** encrypts data in fixed-size blocks usually 64 or 128 bits at a time.
- The encryption algorithm processes each block of data separately using the cryptographic key



Caesar Cipher

- The **Caesar Cipher** is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications.
- This technique involves shifting the letters of the alphabet by a fixed number of places.
- For example, with a shift of three, the letter 'A' becomes 'D', 'B' becomes 'E', and so on.
- Thus, to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down. The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.
-
    - For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
    - Here is an example of how to use the Caesar cipher to encrypt the message "HELLO" with a shift of 3:

    1. Write down the plaintext message: HELLO
    2. Choose a shift value. In this case, we will use a shift of 3.
    3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

H becomes K (shift 3 from H)
E becomes H (shift 3 from E)
L becomes O (shift 3 from L)
L becomes O (shift 3 from L)
O becomes R (shift 3 from O)

4.The encrypted message is now “KHOOR”.

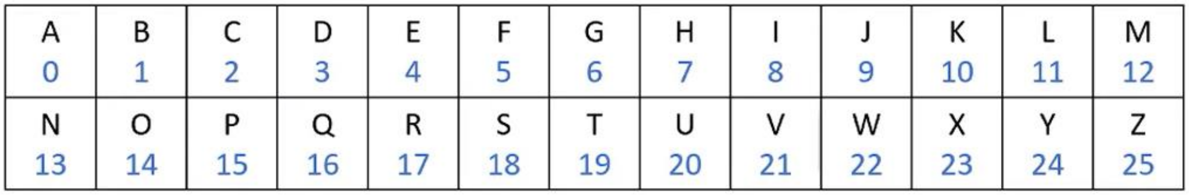
- To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

1. **The Caesar cipher formula for encryption is E(x) = (x + n) mod 26**
2. **The Caesar cipher formula for decryption is D(x) = (x - n) mod 26**
   where 'x' is the numerical value of the letter to be shifted, 'n' is the shift value (key), and 'mod 26' ensures the result stays within the range of the 26 letters of the alphabet.

❖ **Feature of Caesar Cipher**

1. Stream
2. Substitution
3. Monoalphabetic

1. Convert the given plain text in to cipher text using Caesar cipher.
   Palin text: BUZZ



A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25

For B

E(x) = (x + n) mod 26
E(B) = (B+N) mod 26
= (1+3) mod 26
=4 mod 26
=4(E)

For U

E(x) = (x + n) mod 26
E(U) = (U+N) mod 26
= (20+3) mod 26
=23 mod 26
=23(X)

For Z

E(x) = (x + n) mod 26
E(U) = (Z+N) mod 26
= (22+3) mod 26
=28 mod 26
=2(C)

For Z

E(x) = (x + n) mod 26
E(U) = (Z+N) mod 26
= (25+3) mod 26
=28 mod 26
=2(C)

So, cipher text of BUZZ is EXCC

If X have to change then

For X

E(x) = (x + n) mod 26
E(U) = (X+N) mod 26
= (23+3) mod 26
=26 mod 26
=0(A)

1. Convert the given Cipher text in to Plain text using Caesar cipher.
   Cipher text = EXCC

D(x) = (x - n) mod 26

For E

D(x) = (x - n) mod 26
D(E) = (E - N) mod 26
= (4-3) mod 26
=1 mod 26
=1(B)

For X

D(x) = (x - n) mod 26
D(X) = (X - N) mod 26
= (23-3) mod 26
=20 mod 26
=20(U)

For C

D(x) = (x - n) mod 26
D(X) = (C - N) mod 26
= (2-3) mod 26
=-1 mod 26
=25(Z)

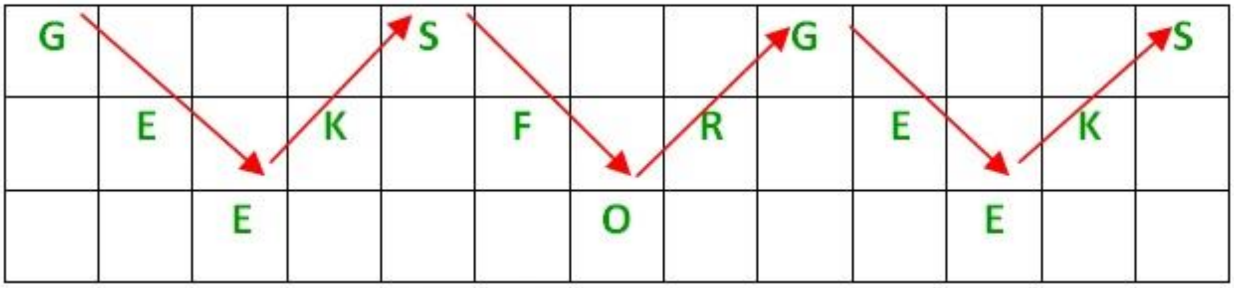
For C

D(x) = (x - n) mod 26
D(X) = (C - N) mod 26
= (2-3) mod 26
=-1 mod 26
=25(Z)

So, Plain text of EXCC is BUZZ

Rail Fence Cipher

- The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher.
- The rail fence cipher is the simplest transposition cipher.
- In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.
- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.
- For example, if the message is "Geeks for Geeks" and the number of rails = 3 then cipher is prepared as:



Decryption

As we’ve seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

- Hence, rail matrix can be constructed accordingly. Once we’ve got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

Implementation:
Let cipher-text = “GsGsekfrek eoe”, and Key = 3

- Number of columns in matrix = len(cipher-text) = 13
- Number of rows = key = 3

Hence original matrix will be of 3*13, now marking places with text as ‘*’ we get

–				–				–				–
	–		–		–		–		–		–	
		–				–				–		

Plain text = hello world

Depth =3

Vigenère Cipher

- Vigenère Cipher is a method of encrypting alphabetic text.
- It is polyalphabetic substitution symmetric key encryption methods.
- **How it Works**

1. **Keyword:** A keyword is chosen and repeated to match the length of the plaintext message.
    - For example, if the plaintext is "ATTACKATDAWN" and the keyword is "LEMON", the repeated keyword becomes "LEMONLEMONLE".
2. **Vigenère Square (Tabula Recta):** A 26x26 table is used. The first row contains the letters of the alphabet. Each subsequent row is a Caesar shift of the previous row by one position to the left.
3. **Encryption:** Each letter of the plaintext is paired with the corresponding letter of the keyword. The ciphertext letter is found at the intersection of the row corresponding to the keyword letter and the column corresponding to the plaintext letter in the Vigenère square.
    - Using the example above:
        - Plaintext: A T T A C K A T D A W N
        - Keyword: L E M O N L E M O N L E
        - Ciphertext: L X F O P V E F R N H R
4. **Decryption:** To decrypt, the ciphertext letter is located in the row corresponding to the keyword letter. The plaintext letter is the letter at the top of that column.

- Using the ciphertext "LXFOPVEFRNHR" and the keyword "LEMON":
    - Keyword letter 'L': Find 'L' in the 'L' row, the column heading is 'A'.
    - Keyword letter 'E': Find 'X' in the 'E' row, the column heading is 'T'.
    - And so on... resulting in the plaintext "ATTACKATDAWN".

Algebraic Description

The Vigenère cipher can also be described algebraically by assigning numbers 0-25 to the letters A-Z.

- **Encryption:** Ci= (Pi + Ki) mod26
    - Where:
        - Ci is the i-th letter of the ciphertext.
        - Pi is the i-th letter of the plaintext.
        - Ki is the i-th letter of the key (repeated).
        - mod26 is the modulo operation (the remainder after division by 26).
- **Decryption:** Pi = (Ci − Ki) mod26
    - If the result of the subtraction is negative, 26 is added to bring it into the 0-25 range.
    - For example:
        - Plaintext 'A' (0), Key 'L' (11): (0+11) mod 26=11, which is 'L'.
        - Ciphertext 'L' (11), Key 'L' (11): (11−11) mod 26=0, which is 'A'.

- **Example:** convert the given plain text into cipher text with the help of given key using Vigenère methods.

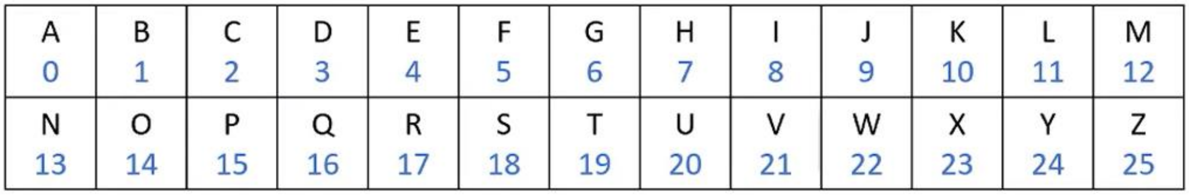
Plain text =HELLO

Key = ABCD

Note = key will be repetitive until it become equal to length of plain text.

Now, Solution
Plain text = H E L L O

Key =A B C D A



A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

As we know

Ci= (Pi + Ki) mod26

For H

Ci= (Pi + Ki) mod26
= (p1 + k1) mod 26
= (H + A) mod 26
= (7+ 0) mod 26
= 7 mod 26
=7(H)

For E

Ci= (Pi + Ki) mod26
= (p2 + k2) mod 26
= (E + B) mod 26
= (4+ 1) mod 26
= 5 mod 26
=5(F)

For L

Ci= (Pi + Ki) mod26
= (p3 + k3) mod 26
= (L + C) mod 26
= (11+ 2) mod 26
= 13 mod 26
=13(N)

For L

Ci= (Pi + Ki) mod26
= (p4 + k4) mod 26
= (L + D) mod 26
= (11+ 3) mod 26
= 14 mod 26
=14(O)

For O

Ci= (Pi + Ki) mod26
= (p5 + k5) mod 26
= (O + A) mod 26
= (11+ 0) mod 26
= 14 mod 26
=14(O)

Cipher text of HELLO = HFNOO using ABCD Key.

In above example if we add in plain text Z then key would be B

Then for Z

Ci= (Pi + Ki) mod26

= (P6 + K6) mod 26
= (Z + B) mod 26
= (25+ 1) mod 26
= 26 mod 26
=0(A)

In above example if we add in plain text Y And key would for example U.

Then for Y

Ci= (Pi + Ki) mod26

= (Y + U) mod 26
= (24+ 20) mod 26
= 44 mod 26
=remainder of 44 divided by 26 is 18
18(S)

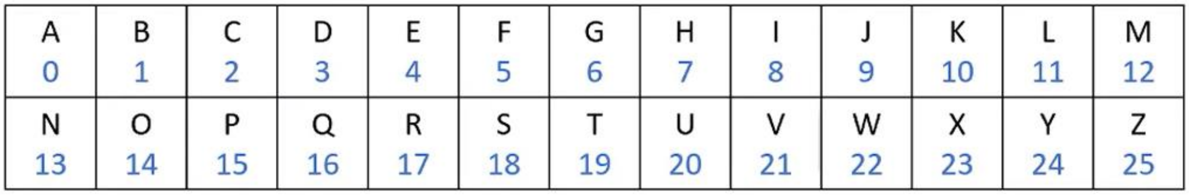
Example: Convert the given cipher text in to plain text with the help of given key using Vigenère methods.

Cipher Text: X W C F R

Key : T Z C

Now, Solution
Cipher Text: X W C F R

Key : T Z C T Z



A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12
N 13	O 14	P 15	Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25

For Decryption

Pi = (Ci − Ki) mod 26

<u>For X</u>

Pi = (Ci − Ki) mod 26

= (C1 – K1) mod 26

= (X – T) mod 26

= (23 -19) mod 26

= 4 mod 26

=4 (E)

For W

Pi = (Ci − Ki) mod 26
= (C2 – K2) mod 26
= (W – Z) mod 26
= (22 -25) mod 26
= -3 mod 26
= 23 (X)

For C

Pi = (Ci − Ki) mod 26
= (C3 – K3) mod 26
= (C – C) mod 26
= (2-2) mod 26
= 0 mod 26
= 0(A)

For F

Pi = (Ci − Ki) mod 26
= (C4 – K4) mod 26
= (F – T) mod 26
= (5-19) mod 26
= -14 mod 26
= 12 (M)

For R

Pi = (Ci − Ki) mod 26
= (C5 – K5) mod 26
= (R – Z) mod 26
= (17-25) mod 26
= -8 mod 26
= 18 (S)

So the plain text of X W C F R = E X A M S using key TZC