Encryption in cyber security is the conversion of data from a readable format into an encoded format. Encrypted data can only be read or processed after it's been decrypted.

Encryption is the basic building block of data security. It is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for malicious purposes.

How encryption work

When information or data is shared over the

internet, it goes through a series of network devices worldwide, which form part of the public internet. As data travels through the public internet, there is a chance it could be compromised or stolen by hackers. To prevent this, users can install specific software or hardware to ensure the secure transfer of data or information. These processes are known as encryption in network security.

Encryption involves converting human-readable plaintext into incomprehensible text, which is known as ciphertext. Essentially, this means taking readable data and changing it so that it appears random. Encryption involves using a cryptographic key, a set of mathematical values both the sender and recipient agree on. The recipient uses the key to decrypt the data, turning it back into readable plaintext.

The more complex the cryptographic key, the more secure the encryption – because third parties are less likely to decrypt it via brute force

attacks (i.e. trying random numbers until the correct combination is guessed).

Encryption is also used to protect passwords. Password encryption methods scramble your password, so it's unreadable by hackers.

Techniques of encryption

● **Symmetric encryption keys:** This is also known as private key encryption. The key used to encode is the same as the one used to decode, making it best for individual users and closed systems. Otherwise, the key must be sent to the receiver. This increases the risk of compromise if it's intercepted by a third party, such as a hacker. This method is faster than the asymmetric method.

● **Asymmetric encryption keys:** This type uses two different keys — public and private — that

are linked together mathematically. The keys are essentially large numbers that have been paired with each other but aren't identical, hence the term asymmetric. The private key is kept secret by the owner, and the public key is either shared amongst authorized recipients or made available to the public at large.

Benefits of encryption

Encryption helps maintain data integrity

Hackers don't just steal information; they can also alter data to commit fraud. While it is possible for skilled hackers to alter encrypted data, recipients of the data will be able to detect the corruption – allowing for a quick response.

Encryption helps organizations adhere to

regulations

Many industries – for example, financial services or healthcare providers – have strict regulations about how consumer data is used and stored. Encryption helps organizations meet those standards and ensure compliance.

Encryption helps when moving data to cloud storage

More and more users and organizations are storing their data in the cloud, which means cloud security is essential. Encrypted storage helps to maintain the privacy of that data. Users should ensure that data is encrypted in-flight, while in use, and at rest in storage.

Encryption helps organizations secure offices

Many organizations have remote offices, especially post-pandemic. This can pose cybersecurity risks as data is being accessed from several different locations – encryption helps guard against theft or accidental loss of data.

Data encryption protects intellectual property.

Digital rights management systems encrypt data at rest — in this case, intellectual property such as songs or software—to prevent reverse engineering and unauthorized use or reproduction of copyrighted material.

Uses of encryption

Most of us encounter encryption every day. Popular uses include:

- Every time you use an ATM or buy something online with a smartphone, encryption is used to protect the information being relayed.

- Securing devices, such as encryption for laptops.

- Most legitimate websites use "secure sockets layer" (SSL), which is a form of encrypting data when it is being sent to and from a website. This keeps attackers from accessing that data while it is in transit. Look for the padlock icon in the URL bar and the "s" in the "https://" to ensure you are conducting secure, encrypted transactions online.

- Your WhatsApp messages are also encrypted, and you may also have an encrypted folder on your phone.

- Your email can also be encrypted with

protocols such as OpenPGP.

- VPNs – Virtual Private Networks – use encryption, and everything you store in the cloud should be encrypted. You can encrypt your whole hard drive and even make encrypted voice calls.

- Encryption is used to prove the integrity and authenticity of information using what are known as digital signatures. Encryption is an integral part of digital-rights management and copy protection.

- Encryption can be used to erase data. Since deleted information can sometimes be brought back using data recovery tools, if you encrypt the data first and throw away the key, the only thing that anybody can recover is the ciphertext and not the original data.

Encryption in cyber security is a way of protecting private information from being stolen

or compromised.