Encryption…..

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*.

In computing, unencrypted data is also known as *plaintext*, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms,* or *ciphers*.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a *key*, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Importance of encryption

Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the following:

- **Confidentiality** encodes the message's content.
- **Authentication** verifies the origin of a message.

- **Integrity** proves the contents of a message have not been changed since it was sent.
- **Nonrepudiation** prevents senders from denying they sent the encrypted message.

How is it used?

Encryption is commonly used to protect data in transit and data at rest. Every time someone uses an ATM or buys something online with a smartphone, encryption is used to protect the information being relayed. Businesses are increasingly relying on encryption to protect applications and sensitive information from reputational damage when there is a data breach.

There are three major components to any encryption system: the data, the encryption engine and the key management. In laptop encryption, all three components are running or stored in the same place: on the laptop.

In application architectures, however, the three components usually run or are stored in separate places to reduce the chance that compromise of any single component could result in compromise of the entire system.

How does encryption work?

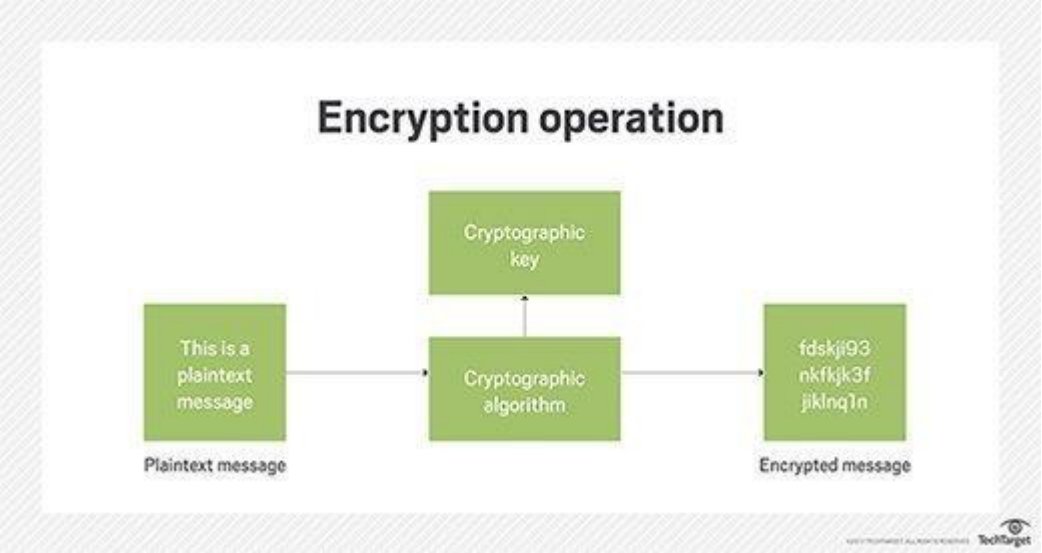
At the beginning of the encryption process, the sender must decide what cipher will best disguise the meaning of the message and what variable to use as a key to make the encoded message unique. The most widely used types of ciphers fall into two categories: symmetric and asymmetric.

Symmetric ciphers, also referred to as *secret key encryption*, use a single key. The key is sometimes referred to as a *shared secret* because the sender or computing system doing the encryption must share the secret

key with all entities authorized to decrypt the message. Symmetric key encryption is usually much faster than asymmetric encryption. The most widely used symmetric key cipher is the Advanced Encryption Standard (AES), which was designed to protect government-classified information.

Asymmetric ciphers, also known as *public key encryption*, use two different -- but logically linked -- keys. This type of cryptography often uses prime numbers to create keys since it is computationally difficult to factor large prime numbers and reverse-engineer the encryption. The Rivest-Shamir-Adleman (RSA) encryption algorithm is currently the most widely used public key algorithm. With RSA, the public or the private key can be used to encrypt a message; whichever key is not used for encryption becomes the decryption key.

Today, many cryptographic processes use a symmetric algorithm to encrypt data and an asymmetric algorithm to securely exchange the secret key.



Benefits of encryption

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network.

In addition to security, the adoption of encryption is often driven by the need to meet compliance regulations. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants to encrypt customers' payment card data when it is both stored at rest and transmitted across public networks.

Disadvantages of encryption

While encryption is designed to keep unauthorized entities from being able to understand the data they have acquired, in some situations, encryption can keep the data's owner from being able to access the data as well.

Key management is one of the biggest challenges of building an enterprise encryption strategy because the keys to decrypt the cipher text have to be living somewhere in the environment, and attackers often have a pretty good idea of where to look.

There are plenty of best practices for encryption key management. It's just that key management adds extra layers of complexity to the backup and restoration process. If a major disaster should strike, the process of retrieving the keys and adding them to a new backup server could increase the time that it takes to get started with the recovery operation.

Having a key management system in place isn't enough. Administrators must come up with a comprehensive plan for protecting the key management system. Typically, this means backing it up separately from

everything else and storing those backups in a way that makes it easy to retrieve the keys in the event of a large-scale disaster.

Encryption key management and wrapping

Encryption is an effective way to secure data, but the cryptographic keys must be carefully managed to ensure data remains protected, yet accessible when needed. Access to encryption keys should be monitored and limited to those individuals who absolutely need to use them.

Strategies for managing encryption keys throughout their lifecycle and protecting them from theft, loss or misuse should begin with an audit to establish a benchmark for how the organization configures, controls, monitors and manages access to its keys.

Key management software can help centralize key management, as well as protect keys from unauthorized access, substitution or modification.