

Data Encryption – the Basics

A DEFINITION OF DATA ENCRYPTION

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

THE PRIMARY FUNCTION OF DATA ENCRYPTION

The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The outdated data encryption standard (DES) has been replaced by modern encryption algorithms that play a critical role in the security of IT systems and communications.

These algorithms provide confidentiality and drive key security initiatives including authentication, integrity, and non-repudiation. Authentication allows for the verification of a message's origin, and integrity provides proof that a message's contents have not changed since it was sent. Additionally, non-repudiation ensures that a message sender cannot deny sending the message.

THE PROCESS OF DATA ENCRYPTION

Data, or plaintext, is encrypted with an encryption algorithm and an encryption key. The process results in ciphertext, which only can be viewed in its original form if it is decrypted with the correct key.

Symmetric-key ciphers use the same secret key for encrypting and decrypting a message or file. While symmetric-key encryption is much faster than asymmetric encryption, the sender must exchange the encryption key with the recipient before he can decrypt it. As companies find themselves needing to securely distribute and manage huge quantities of keys, most data encryption services have adapted and use an asymmetric algorithm to exchange the secret key after using a symmetric algorithm to encrypt data.

On the other hand, asymmetric cryptography, sometimes referred to as public-key cryptography, uses two different keys, one public and one private. The public key, as it is named, may be shared with everyone, but the private key must be protected. The Rivest-Sharmir-Adleman (RSA) algorithm is a cryptosystem for public-key encryption that is widely used to secure sensitive data, especially when it is sent over an insecure network like the internet. The RSA algorithm's popularity comes from the fact that both the public and private keys can encrypt a message to assure the confidentiality, integrity, authenticity, and non-repudiability of electronic communications and data through the use of digital signatures.