Encryption

Definition - What does *Encryption* mean?

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption.

Encryption is essential for ensured and trusted delivery of sensitive information.

Techopedia explains *Encryption*

Symmetric-key encryption uses two secret, often identical keys or codes for computers involved in message transmission. Each secret key's data packet is self-encrypted. The first symmetric encryption algorithm is the Data Encryption Standard (DES), which uses a 56-bit key and is not considered attack-proof. The Advanced Encryption Standard (AES) is considered more reliable because it uses a 128-bit, a 192-bit or a 256-bit key.

Asymmetric-key encryption, also known as public-key encryption, uses private and public keys in tandem. The public key is shared with computers attempting to communicate securely with the user's computer. This key handles encryption, rendering the message undecipherable in transit. The private matching key remains private on the user's computer. It decrypts the message and makes it readable. Pretty good privacy (PGP) is a commonly used public-key encryption system.

Tech moves fast! Stay ahead of the curve with Techopedia!

Join nearly 200,000 subscribers who receive actionable tech insights from Techopedia.

| ✉ Enter your email address... | Subscribe |

Featured Q&A

More of your questions answered by our Experts (/experts)