Encryption is a way to scramble information so that only those with 'keys' can understand what is being shared.

The importance of encryption
In our increasingly digital lives, the role of encryption has never been more essential.

I want to keep all my messages confidential!

Encryption makes information unintelligible, not inaccessible. Someone can still access your data, but it appears meaningless.

I don't expect anyone to read my messages, other than who I send them to!
Hey Marcus, I want to send you a secure message.

Let’s use encryption. It’s safe and efficient!

Each user has two keys: a public one and private one. Olivia finds Marcus’ public key and copies it to her device.

Olivia generates a secret, symmetrical key, encrypts a copy of it using Marcus’ public key, and sends it to him. He decrypts it with his private key.

Olivia and Marcus now have a shared, secret key which they can use for fast, efficient symmetric encryption.

The initial key exchange uses asymmetric encryption. The data itself is transferred using symmetric encryption.

Different types of encryption

Not all encryption is equal. The best systems balance safety and efficiency.

Symmetric encryption is like a cash box, where all users have the same secret key to see what’s inside.

Fast and efficient

Vulnerable to interception

With asymmetric encryption each user has their own public and private keys, providing additional security.

Safe and secure

Complexity means less efficiency

In hybrid systems, a mixture of encryption processes provides the best of both worlds. Asymmetric encryption is used for a secure key exchange, with the more efficient system of symmetric encryption used to transfer the data itself.

Safe and secure

Fast and efficient

Hey Marcus, I want to send you a secure message.

Let’s use encryption. It’s safe and efficient!

Each user has two keys: a public one and private one. Olivia finds Marcus’ public key and copies it to her device.

Olivia generates a secret, symmetrical key, encrypts a copy of it using Marcus’ public key, and sends it to him. He decrypts it with his private key.

Olivia and Marcus now have a shared, secret key which they can use for fast, efficient symmetric encryption.

The initial key exchange uses asymmetric encryption. The data itself is transferred using symmetric encryption.

Different types of encryption

Not all encryption is equal. The best systems balance safety and efficiency.

Symmetric encryption is like a cash box, where all users have the same secret key to see what’s inside.

Fast and efficient

Vulnerable to interception

With asymmetric encryption each user has their own public and private keys, providing additional security.

Safe and secure

Complexity means less efficiency

In hybrid systems, a mixture of encryption processes provides the best of both worlds. Asymmetric encryption is used for a secure key exchange, with the more efficient system of symmetric encryption used to transfer the data itself.

Safe and secure

Fast and efficient
Where threats come from

Knowing who wants to access your data highlights the importance of keeping it safe.

1. Some areas of law enforcement want backdoors to catch criminals. This creates access for bad actors, not just good ones.
2. Many governments think they should be able to break encryption in order to access their citizens’ messages.
3. Blackmailers would like to break encryption to target people’s private messages, photos and videos.
4. Personal banking and national economies rely on encryption. Vulnerabilities could lead to stolen money and financial data.
5. Criminals steal people’s identities, to commit crimes and evade capture. Weak encryption would enable this.

Threats can come from individuals, businesses, or even governments. These threats undermine the trustworthiness of the Internet.