



What Is Encryption?

Encryption is the process of converting or scrambling data and information into an unreadable, encoded version that can only be read with authorized access. Encryption is a widely used security tool that can prevent the interception of sensitive data, either while stored in files or while in transit across networks.

Watch video (01:59)

Cisco Secure Endpoint >



Why should we care about encryption?

What encryption algorithms should I use?

How do I send an encrypted email?

How do I detect encrypted threats?

Types of encryption algorithms

Types of data encryption

Why should we care about encryption?

Every time we make a purchase online, use the bank ATM, text or call somebody, encryption keeps the transaction or communication private and highly secure. Encryption provides a layer of security so information is only accessed by the authorized users. It has become an essential part of our modern day lives. We should care about encryption as it provides privacy, security, integrity of data, and authentication. In many cases it is required for regulatory compliance.

What encryption algorithms should I use?

This is a complicated question to answer. When deciding on an encryption algorithm, it is important to consider these questions:

- Is this algorithm up to date?
- Has this algorithm been through a validation process?
- Does the OS, application, or hardware support the encryption?

If any question cannot be answered in the affirmative, either a new algorithm should be chosen or more research should be done.

Because encryption is a constantly changing field, these decisions can be difficult. However, it is important to understand that encryption is very important to security. Making decisions based on partial knowledge about encryption can be dangerous. If you don't fully understand encryption, make sure you are using crypto designed and built by someone who does understand.

How do I send an encrypted email?

To properly [encrypt emails](#), businesses should invest in encryption tools designed for email. When choosing the tools, a business can decide on sender encryption or key management.

- **Sender encryption** provides tools for users to encrypt their emails, such as flagging as "urgent" or installing a plug-in with a clickable encryption button. In sender encryption, however, businesses are relying on the judgement of employees to decide what should be encrypted.
- **Key management** is typically a central system and set of rules that will act and encrypt emails. This central host can use big data to accurately encrypt sensitive data and information.

How do I detect encrypted threats?

While businesses are encrypting traffic to protect their data, attackers are encrypting threats. As Cisco CEO Chuck Robbins said at Cisco Live, "70 percent of the attacks that are launched are within encrypted traffic."

Decrypting all traffic, however, would be incredibly time consuming. Businesses must invest in tools that leverage big data to identify potential threats. [Machine learning](#) and [network analytics](#) can flag obscure indicators and behaviors that suggest an encrypted threat. Once identified, the network can quarantine and investigate the threat before damage occurs.

Types of encryption algorithms

There are two types of encryption algorithms: symmetric (also called shared key algorithm) and asymmetric (also known as public key algorithm).

- **Symmetric encryption** uses the same key for encryption and decryption. Because it uses the same key, symmetric encryption can be more cost effective for the security it provides. That said, it is important to invest more in securely storing data when using symmetric encryption.
- **Asymmetric encryption** uses two separate keys: a public key and a private key. Often a public key is used to encrypt the data while a private key is required to decrypt the data. The private key is only given to users with authorized access. As a result, asymmetric encryption can be more effective, but it is also more costly.

Types of data encryption

Here are some examples of common types of encryption used today.

Triple DES

The Triple Data Encryption Standard (DES), often written 3DES, is a version of the original DES encryption algorithm that encrypts data three times. The Triple DES uses three 64-bit keys, so the key length is 192 bits. Triple DES is a symmetric encryption, and the key is private. Because it encrypts data in 64-bit segments, Triple DES is considered a block cipher. Cipher Block Chaining (CBC), however, is an encryption mode that struggles at high data rates.

Blowfish

Blowfish is an encryption technique that was designed by Bruce Schneier in 1993. Similar to Triple DES, Blowfish is a symmetric block cipher. Unlike Triple DES, Blowfish does variable-length key encryption. Rather than set 64-bit segments, Blowfish encrypts segments ranging from 32 to 448 bits. Blowfish is an unpatented and unlicensed encryption technique. For this reason, it is free and available for public use.

RSA

The RSA encryption key, named after creators Ron Rivest, Adi Shamir, and Leonard Adelman, is the standard encryption technique for important data security. RSA is asymmetric cryptography, so there is one public key and one private key. The RSA algorithm uses prime factorization. Simply put, this key requires the factorization of a product involving two large prime numbers. While it seems easy, figuring out these two numbers can be difficult. Even for large computers, it can be expensive and exhaustive to decrypt. While RSA can be very useful, it becomes increasingly inefficient at higher security levels.

AES

Because of an increase in brute-force attacks on the original DES, the Advanced Encryption Standard (AES) was put into place in 2002. AES is a symmetric block cipher that was originally named Rijndael. This block cipher uses three separate keys: AES-128, AES-192, and AES-256. These three keys are used to encrypt and decrypt information of 128 bits. Since its adoption, AES has been used to protect classified government information and sensitive data.

ECC

Elliptic Curve Cryptography (ECC) is a very advanced approach. Often based on a common public key algorithm, ECC combines elliptic curves and number theory to encrypt data. These elliptic curves are within finite fields and are symmetrical over the x-axis of a graph. Given these properties, cryptographers can provide robust security with much smaller and efficient keys. For example, an RSA key of 15,360 bits would be equivalent to an ECC key of just 512 bits.

Source: [NIST Special Publication 800-57 Part 1 Revision 4](#) >

Resources

Get started

- [Cisco Umbrella](#)
- [Cisco Firepower Management Center](#)
- [Cisco Secure Endpoint](#)
- [Cisco Security software](#)
- [Cisco SecureX threat response](#)

Connect with us

- [Free trials for Cisco Secure](#)

Related topics

- [What Is Email Encryption?](#)
- [What Is IT Security?](#)
- [What Is Information Security?](#)
- [What Is Two-Factor Authentication?](#)
- [Malware Protection Best Practices](#)
- [User Authentication Policy](#)

Useful Links

- [Trials](#)
- [Demos](#)
<