Types of Encryption: 5 Encryption Algorithms & How to Choose the Right One

We'll break down the two main types of encryption — symmetric and asymmetric — before diving into the list of the 5 most commonly used encryption algorithms to simplify them like never before

Often blamed for hiding terrorist activities by political entities, encryption is one of those cyber security topics that's always in the headlines. Anyone who has a decent understanding of the different types of encryption may feel like a kind of injustice is being done to this remarkable technology that's at the heart of internet security and privacy. Encryption is a method of converting data into an undecipherable format so that only the authorized parties can access the information.

Cryptographic keys, in conjunction with encryption algorithms, are what makes the encryption process possible. And, based on the way these keys are applied, there are mainly two types of encryption methods that are predominantly used: "symmetric encryption" and "asymmetric encryption." Both of these methods use different mathematical algorithms (i.e., those encryption algorithms we mentioned moments ago) to scramble the data. This list of common encryption algorithms includes RSA, ECC, 3DES, AES, etc.

In this article, we'll learn about symmetric & asymmetric encryption and their prevailing encryption algorithms that are used to encrypt data.

Let's hash it out.

Type of Encryption #1: Symmetric Encryption

The symmetric encryption method, as the name implies, uses a single cryptographic key to encrypt and decrypt data. The use of a single key for both operations makes it a straightforward process, and hence it's called "symmetric." Here's a visual breakdown of how symmetric encryption works:

Let's understand the symmetric encryption process with a simple example:

There are two really close friends named Bob and Alice living in New York. For some reason, Alice has to move out of the city. The only way they can communicate with each other is through postal mail. But there's one problem: Bob and Alice are afraid that someone could read their letters.

To protect their letters from someone's eyes, they decide to write their message in such a way that each letter of the message is replaced by a letter seven positions down the alphabet. So, instead of writing "Apple," they would write "hwwsl" (A -> H, P -> W, L -> S, E -> L). To turn the data back into its original form, they'd have to replace the letter seven positions up the alphabet order.

Of course, this might sound too simple to you — and it is. That's because this technique was used centuries ago by Julius Caesar, the Roman emperor and military general. Known as "Caesar's cipher," this method works on the technique of alphabet substitution.

Today's encryption methods aren't as simple as that. The widely used encryption algorithms are so complex that even the combined computing power of many super-computers cannot crack them. And that's why we can relax and send our credit card information without any worries.

What Makes Symmetric Encryption a Great Technique

The most outstanding feature of symmetric encryption is the simplicity of its process. This simplicity of this type of encryption lies in the use of a single key for both encryption as well as decryption. As a result, symmetric encryption algorithms:

- Are significantly faster than their asymmetric encryption counterparts (which we'll discuss shortly),
- Require less computational power, and
- Don't dampen internet speed.

This means that when there's a large chunk of data to be encrypted, symmetric encryption proves to be a great option.

3 Common Types of Symmetric Encryption Algorithms

Like we saw with Caesar's cipher, there's specific logic behind every encryption method that scrambles data. The encryption methods that are used today rely on highly complex mathematical functions that make it virtually impossible to crack them.

What you may or may not realize is that there are hundreds of symmetric key algorithms in existence! Some of the most common encryption methods

include AES, RC4, DES, 3DES, RC5, RC6, etc. Out of these algorithms, DES and AES algorithms are the best known. While we can't cover all of the different types of encryption algorithms, let's have a look at three of the most common.

1. DES Symmetric Encryption Algorithm

Introduced in 1976, DES (data encryption standard) is one of the oldest symmetric encryption methods. It was developed by IBM to protect sensitive, unclassified electronic government data and was formally adopted in 1977 for use by federal agencies. DES uses a 56-bit encryption key, and it's based on the Feistel Structure that was designed by a cryptographer named Horst Feistel. The DES encryption algorithm was among those that were included in TLS (transport layer security) versions 1.0 and 1.1.

DES converts 64-bit blocks of plaintext data into ciphertext by dividing the block into two separate 32-bit blocks and applying the encryption process to each independently. This involves 16 rounds of various processes — such as expansion, permutation, substitution, or an XOR operation with a round key — that the data will go through as it's encrypted. Ultimately, 64-bit blocks of encrypted text is produced as the output.

Today, DES is no longer in use as it was cracked by many security researchers. In 2005, DES was officially deprecated and was replaced by the AES encryption algorithm, which we'll talk about momentarily. The biggest downside to DES was its low encryption key length, which made brute-forcing easy against it. TLS 1.2, the most widely used TLS protocol today, doesn't use the DES encryption method.

2. 3DES Symmetric Encryption Algorithm

3DES (also known as TDEA, which stands for triple data encryption algorithm), as the name implies, is an upgraded version of the DES algorithm that was released. 3DES was developed to overcome the drawbacks of the DES algorithm and was put into use starting in the late 1990s. To do so, it applies the DES algorithm thrice to each data block. As a result, this process made 3DES much harder to crack than its DES predecessor. It also became a widely used encryption algorithm in payment systems, standards, and technology in the finance industry. It's also become a part of cryptographic protocols such as TLS, SSH, IPsec, and OpenVPN.

All encryption algorithms ultimately succumb to the power of time, and 3DES was no different. The Sweet32 vulnerability discovered by researchers Karthikeyan Bhargavan and Gaëtan Leurent unplugged the security holes that exist within the 3DES algorithm. This discovery caused the security industry to consider the deprecation of the algorithm and the National Institute of Standards and Technology (NIST) announced the deprecation in a draft guidance published in 2019.

According to this draft, the use of 3DES is to be scrapped in all new applications after 2023. It's also worth noting that TLS 1.3, the latest standard for SSL/TLS protocols, also discontinued the use of 3DES.

3. AES Symmetric Encryption Algorithm

AES, which stands for "advanced encryption system," is one of the most prevalently used types of encryption algorithms and was developed as an alternative to the DES algorithm. Also known as Rijndael, AES became an encryption standard on approval by NIST in 2001. Unlike DES, AES is a family of block ciphers that consists of ciphers of different key lengths and block sizes.

AES works on the methods of substitution and permutation. First, the plaintext data is turned into blocks, and then the encryption is applied using the encryption key. The encryption process consists of various sub-processes such as sub bytes, shift rows, mix columns, and add round keys. Depending upon the size of the key, 10, 12, or 14 such rounds are performed. It's worth noting that the last round doesn't include the sub-process of mix columns among all other sub-processes performed to encrypt the data.

The Advantage of Using the AES Encryption Algorithm

What all of this boils down to is to say that AES is safe, fast, and flexible. AES is a much quicker algorithm compared to DES. The multiple key length options are the biggest advantage you have as the longer the keys are, the harder it is to crack them.

Today, AES is the most widely used encryption algorithm — it's used in many applications, including:

- Wireless security,
- Processor security and file encryption,
- SSL/TLS protocol (website security),
- Wi-Fi security,
- Mobile app encryption,
- VPN (virtual private network), etc.

Many government agencies, including the National Security Agency (NSA), rely on the AES encryption algorithm to protect their sensitive information.

Type of Encryption #2: Asymmetric Encryption

Asymmetric encryption, in contrast to the symmetric encryption method, involves multiple keys for encryption and decryption of the data. Asymmetric encryption encompasses two distinct encryption keys that are mathematically related to each other. One of these keys is known as the "public key" and the other one as the "private key." Hence, why the asymmetric encryption method is also known as "public key cryptography."

As we saw in the above example, symmetric encryption works great when Alice and Bob want to exchange information. But what if Bob wants to communicate with hundreds of people securely? Would it be practical if he used different mathematical keys for each person? Not really, because that would be a lot of keys to juggle.

To resolve this issue, Bob uses public key encryption, which means that he gives the public key to everyone who sends him the information and keeps the private key to himself. He instructs them to encrypt the information with the public key so that the data can only be decrypted using the private key that he has. This eliminates the risk of key compromise as the data can only be decrypted using the private key that Bob has in his possession.

What Makes Asymmetric Encryption a Great Technique

The first (and most obvious) advantage of this type of encryption is the security it provides. In this method, the public key — which is publicly available — is used to encrypt the data, while the decryption of the data is done using the private key, which needs to be stored securely. This ensures that the data remains protected against man-in-the-middle (MiTM) attacks. For web/email servers that connect to hundreds of thousands of clients ever minute, asymmetric encryption is nothing less than a boon as they only need to manage and protect a single key. Another key point is that public key cryptography allows creating an encrypted connection without having to meet offline to exchange keys first.

The second crucial feature that asymmetric encryption offers is authentication. As we saw, the data encrypted by a public key can only be decrypted using the private key related to it. Therefore, it makes sure that the data is only seen and decrypted by the entity that's supposed to receive it. In simpler terms, it verifies that you're talking to the person or organization that you think you are.

The 2 Main Types of Asymmetric Encryption Algorithms

1. RSA Asymmetric Encryption Algorithm

Invented by Ron Rivest, Adi Shamir, and Leonard Adleman (hence "RSA") in 1977, RSA is, to date, the most widely used asymmetric encryption algorithm. Its potency lies in the "prime factorization" method that it relies upon. Basically, this method involves two huge random prime numbers, and these numbers are multiplied to create another giant number. The puzzle here is to determine the original prime numbers from this giant-sized multiplied number.

It turns out this puzzle is virtually impossible — if using the right key length that's generated with enough entropy — for today's super-computers, let alone humans. In 2010, a group of researchers did research, and it took them more than 1,500 years of computing time (distributed across hundreds of

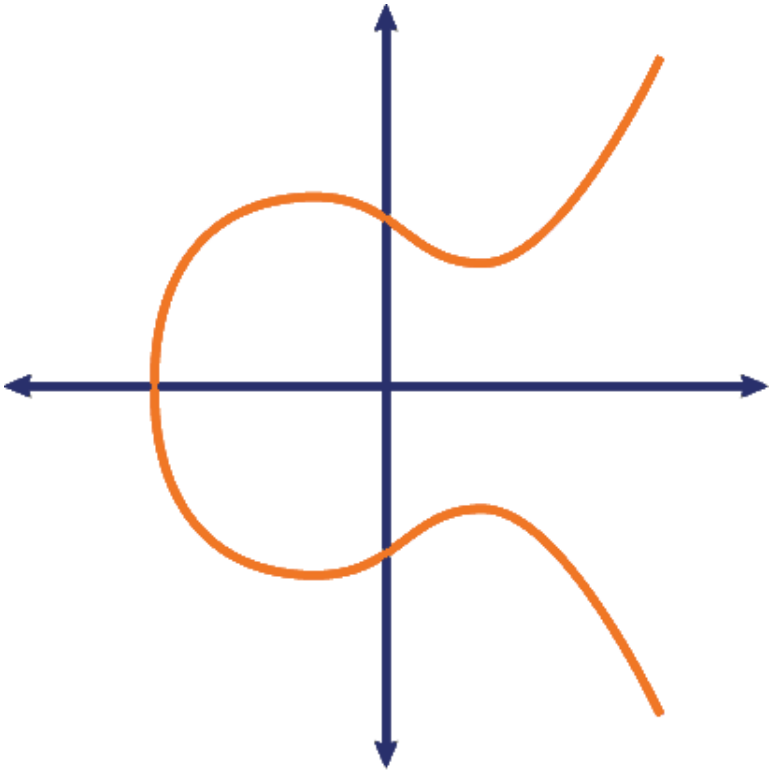
computers) to crack RSA-768 bit key – which is way below the standard 2048-bit RSA key that's in use today.

The Advantage of Using the RSA Encryption Algorithm

A great advantage that RSA offers is its scalability. It comes in various encryption key lengths such as 768-bit, 1024-bit, 2048-bit, 4096-bit, etc. Therefore, even if the lower key-lengths are successfully brute-forced, you can use encryption of higher key lengths because the difficulty of brute-forcing the key increases with each expanding key length.

RSA is based on a simple mathematical approach, and that's why its implementation in the public key infrastructure (PKI) becomes straightforward. This adaptability with PKI and its security has made RSA the most widely used asymmetric encryption algorithm used today. RSA is extensively used in many applications, including SSL/TLS certificates, crypto-currencies, and email encryption.

2. ECC Asymmetric Encryption Algorithm



In 1985, two mathematicians named Neal Koblitz and Victor S. Miller proposed the use of elliptic curves in cryptography. After almost two decades, their idea was turned into a reality when ECC (Elliptic Curve Cryptography) algorithm entered into use in 2004-05.

In the ECC encryption process, an elliptic curve represents the set of points that satisfy a mathematical equation ($y^2 = x^3 + ax + b$).

Like RSA, ECC also works on the principle of irreversibility. In simpler words, it's easy to compute it in one direction but painfully difficult to reverse it and come to the original point. In ECC, a number symbolizing a point on the curve is multiplied by another number and gives another point on the curve. Now, to crack this puzzle, you must figure out the new point on the curve. The mathematics of ECC is built in such a way that it's virtually impossible to find out the new point, even if you know the original point.

The Advantage of Using the ECC Encryption Algorithm

Compared to RSA, ECC offers greater security (against current methods of cracking) as it's quite complex. It provides a similar level of protection as RSA, but it uses much shorter key lengths. As a result, ECC applied with keys of greater lengths will take considerably more time to crack using brute force attacks.

Another advantage of the shorter keys in ECC is faster performance. Shorter keys require less networking load and computing power, and that turns out to be great for devices with limited storage and processing capabilities. When the ECC is used in SSL/TLS certificates, it decreases the time it takes to perform SSL/TLS handshakes considerably and helps you load the website faster. The ECC encryption algorithm is used for encryption applications, to apply digital signatures, in pseudo-random generators, etc.

The challenge with using ECC, though, is that many server software and control panels haven't yet added support for ECC SSL/TLS certificates. We're hoping that this changes in the future, but this means that RSA is going to continue to be the more widely used asymmetric encryption algorithm in the meantime.

Hybrid Encryption: Symmetric + Asymmetric Encryption

First, let me clarify that hybrid encryption is not a "method" like symmetric and asymmetric encryption are. It's taking the best from both of these methods and creating a synergy to build robust encryption systems.

As advantageous as symmetric and asymmetric encryption are, they both have their downsides. The symmetric encryption method works great for fast encryption of large data. Still, it doesn't provide identity verification, something that's the need of the hour when it comes to internet security. On the other hand, asymmetric encryption — thanks to the public/private key pair — makes sure that the data is accessed by your intended recipient. However, this verification makes the encryption process painfully slow when implemented at scale.

In many applications, such as website security, there was a need to encrypt the data at a high speed and the verification of identity was also required to ensure the users that they're talking to the intended entity. That's how the idea of hybrid encryption was born.

The hybrid encryption technique is used in applications such as SSL/TLS certificates. SSL/TLS encryption is applied during a series of back-and-forth communications between servers and clients (web browsers) in a process that's known as the "TLS handshake." In this process, the identity of both parties is verified using the private and public key. Once both parties have confirmed their identities, the encryption of the data takes place through symmetric encryption using an ephemeral (session) key. This ensures speedy transmission of the tons of data that we send and receive on the internet every minute.

Types of Encryption Methods: What We Hashed Out

If you're wondering which type of encryption is better than the other, then there won't be any clear winner as both symmetric and asymmetric encryption bring their advantages to the table, and we cannot choose only one at the expense of the other.

From the security perspective, asymmetric encryption is undoubtedly better as it ensures authentication and non-repudiation. However, the performance is also an aspect that we can't afford to ignore, and that's why symmetric encryption will always be needed.

Here's the summary of what we hashed out for as far as types of encryption are concerned:

Symmetric Encryption	Asymmetric Encryption
A single key is used to encrypt and decrypt data.	A key pair is used for encryption and decryption. These keys are known as public key and private key.

As it uses only one key, it's a simpler method of encryption.	Thanks to the key pair, it's a more complex process.
Symmetric encryption is primarily used for encryption.	Asymmetric encryption ensures encryption, authentication, and non-repudiation.
It provides faster performance and requires less computational power compared to asymmetric encryption.	It's slower than symmetric encryption and requires higher computational power because of its complexity.
Smaller key lengths are used to encrypt the data (e.g., 128-256-bit length).	Usually, asymmetric encryption methods involve longer keys (e.g. 1024-4096-bit length).
Ideal for applications where a large amount of data needs to be encrypted.	Ideal for applications where a small amount of data is used by ensuring authentication.
Standard symmetric encryption algorithms include RC4, AES, DES, 3DES, and QUAD.	Standard asymmetric encryption algorithms include RSA, Diffie-Hellman, ECC, El Gamal, and DSA.