**Encryption / Decryption Notes**

<https://www.ibm.com/docs/en/sdk-java-technology/8?topic=processes-secret-key-cryptography>

Secret-key cryptography is also called **symmetric cryptography** because the same key is used to both encrypt and decrypt the data. Well-known secret-key cryptographic algorithms include Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and Rivest Cipher 4 (RC4).

<https://www.ibm.com/docs/en/sdk-java-technology/8?topic=works-cryptographic-processes>

* [**Secret Key Cryptography**](https://www.ibm.com/docs/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/secretkeycryptography.html)  
  With secret-key cryptography, both communicating parties, Alice and Bob, use the same key to encrypt and decrypt the messages. Before any encrypted data can be sent over the network, both Alice and Bob must have the key and must agree on the cryptographic algorithm that they will use for encryption and decryption
* [**Public Key Cryptography**](https://www.ibm.com/docs/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/publickeycryptography.html)  
  Public-key cryptography solves the logistical problem of key distribution by using both a public key and a private key. The public key can be sent openly through the network while the private key is kept private by one of the communicating parties. The public and the private keys are cryptographic inverses of each other; what one key encrypts, the other key will decrypt.
* [**Comparison Between Secret Key and Public Key Cryptography**](https://www.ibm.com/docs/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/secretpublickeycomp.html)  
  Both secret-key cryptography and public-key cryptography have strengths and weaknesses. With secret-key cryptography, data can be encrypted and decrypted quickly, but because both communicating parties must share the same secret key information, the logistics of exchanging the key can be a problem. With public-key cryptography, key exchange is not a problem because the public key does not need to be kept secret, but the algorithms used to encrypt and decrypt data require extensive computations, and are therefore very slow.
* [**Public Key Certificates**](https://www.ibm.com/docs/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/publickeycertificates.html)  
  A public key certificate provides a safe way for an entity to pass on its public key to be used in asymmetric cryptography. The public key certificate avoids the following situation: if Charlie creates his own public key and private key, he can claim that he is Alice and send his public key to Bob. Bob will be able to communicate with Charlie, but Bob will think that he is sending his data to Alice.

# [**https://www.ibm.com/docs/en/sdk-java-technology/8?topic=cp-cryptographic-hash-functions-message-authentication-codes-digital-signatures**](https://www.ibm.com/docs/en/sdk-java-technology/8?topic=cp-cryptographic-hash-functions-message-authentication-codes-digital-signatures)

# **Cryptographic Hash Functions, Message Authentication Codes, and Digital Signatures**

A cryptographic hash function is similar to a checksum. The main difference is that whereas a checksum is designed to detect accidental alterations in data, a cryptographic hash function is designed to detect deliberate alterations. When data is processed by a cryptographic hash function, a small string of bits, known as a hash, is generated. The slightest change to the message typically makes a large change in the resulting hash. A cryptographic hash function does not require a cryptographic key. A hash function often used with TLS is Secure Hash Algorithm (SHA). SHA was proposed by the [U.S. National Institute of Standards and Technology (NIST)](https://www.ibm.com/links?url=http%3A%2F%2Fwww.nist.gov%2Findex.html).

## Message Authentication Code

A message authentication code (MAC) is similar to a cryptographic hash, except that it is based on a secret key. When secret key information is included with the data that is processed by a cryptographic hash function, the resulting hash is known as an HMAC.

If Alice wants to be sure that Charlie does not tamper with her message to Bob, she can calculate an HMAC for her message and append the HMAC to her original message. She can then encrypt the message plus the HMAC using a secret key that she shares with Bob. When Bob decrypts the message and calculates the HMAC, he will be able to tell if the message was modified in transit. With TLS, an HMAC is used with the transmission of secure data.

## Digital Signatures

Once a cryptographic hash is created for a message, the hash is encrypted with the sender's private key. This encrypted hash is called a digital signature.

<https://www.sciencedirect.com/topics/computer-science/secret-key-encryption#:~:text=Encryption%20is%20the%20foundation%20of,to%20encrypt%20and%20decrypt%20data>.

### **What Is Encryption?**

Encryption is a form of cryptography that “scrambles” plain text into unintelligible [cipher text](https://www.sciencedirect.com/topics/computer-science/ciphertext). Encryption is the foundation of such security measures as digital signatures, digital certificates, and the PKI that uses these technologies to make computer transactions more secure. Computer-based [encryption techniques](https://www.sciencedirect.com/topics/computer-science/encryption-technique) use keys to encrypt and decrypt data. A key is a variable (sometimes represented as a password) that is a large binary number—the larger, the better. Key length is measured in bits, and the more bits in a key, the more difficult the key will be to “crack.”

The key is only one component in the [encryption process](https://www.sciencedirect.com/topics/computer-science/encryption-process). It must be used in conjunction with an encryption algorithm (a process or calculation) to produce the cipher text. [Encryption methods](https://www.sciencedirect.com/topics/computer-science/encryption-method) are usually categorized as either symmetric or asymmetric, depending on the number of keys that are used. We discuss these two basic types of [encryption technology](https://www.sciencedirect.com/topics/computer-science/encryption-technology) in the following sections.

#### **Symmetric Encryption**

Symmetric encryption is also called *secret key encryption*, and it uses just one key, called a shared secret, for both encrypting and decrypting. This is a simple, easy-to-use method of encryption, but there is one problem with it: The key must be shared between the sender and the recipient of the data, so a secure method of key exchange must be devised. Otherwise, if a third party intercepts the key during the exchange, an unauthorized person can easily decrypt the data.

#### **Asymmetric Encryption**

To address the problem of key exchange, another type of encryption was developed. Asymmetric encryption is also called [*public key encryption*](https://www.sciencedirect.com/topics/computer-science/public-key-encryption), but it actually relies on a key pair. Two mathematically related keys, one called the public key and another called the private key, are generated to be used together. The private key is never shared; it is kept secret and is used only by its owner. The public key is made available to anyone who wants it. Because of the time and amount of computer processing power required, it is considered “mathematically unfeasible” for anyone to be able to use the public key to re-create the private key, so this form of encryption is considered very secure.

The primary advantage of asymmetric encryption is that there is no need to securely transmit a secret key. Instead, the public key is published openly, made available to the entire world. There is no need to keep it secret, because it can't be used alone. The encryption process works like this:

1

The sender of a message uses the intended recipient's public key, which is freely available, to encrypt a message.

2

The recipient decrypts the message using his or her private key. Only the private key associated with the public key that encrypted it can be used to decrypt the message.

This key pair can also be used to provide for [authentication](https://www.sciencedirect.com/topics/computer-science/authentication) of a message sender's identity using the keys a little differently: This time the sender uses his or her own private key to encrypt the message. This system provides no confidentiality, because anyone can decrypt the message using the owner's public key. However, it does verify the sender's identity, because if the associated public key will decrypt the message, it could only have been encrypted with that person's private key.

Obviously, the most important issue in [public key cryptography](https://www.sciencedirect.com/topics/computer-science/public-key-cryptography) is the protection of the private keys. This concept is especially important because compromise of a private key not only allows the unauthorized person to read private messages sent to the owner, but also allows the key thief to “sign” transactions emulating the owner, thus stealing the owner's identity. When the key pair is used for secure credit card or banking transactions, this loophole can be disastrous.

<https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future>

**How Encryption Works**

Encryption is a way for data—messages or files—to be made unreadable, ensuring that only an authorized person can access that data. Encryption uses complex algorithms to scramble data and decrypts the same data using a key provided by the message sender. Encryption ensures that information stays private and confidential, whether it's being stored or in transit. Any unauthorized access to the data will only see a chaotic array of bytes.

There are two kinds of cryptographic key systems, symmetric, and asymmetric.

### Symmetric Key Systems

In a symmetric key system, everyone accessing the data has the same key. Keys that encrypt and decrypt messages must also remain secret to ensure privacy. While it's possible for this to work, securely distributing the keys to ensure proper controls are in place makes symmetric encryption impractical for widespread commercial use.

### Asymmetric Key Systems

An asymmetric key system, also known as a public/private key system, uses two keys. One key remains secret—the private key—while the other key is made widely available to anyone who needs it. This key is called the public key. The private and public keys are mathematically tied together, so the corresponding private key can only decrypt that information encrypted using the public key.

## Encryption in Action

Here's an example of how encryption works with email-friendly software Pretty Good Privacy (PGP) or GnuPG—also known as GPG—for open-source aficionados. Say I want to send you a private message. I encrypt it using one of the programs listed below.

Here's the message:

wUwDPglyJu9LOnkBAf4vxSpQgQZltcz7LWwEquhdm5kSQIkQlZtfxtSTsmawq6gVH8SimlC3W6TDOhhL2FdgvdIC7sDv7G1Z7p  
CNzFLp0lgB9ACm8r5RZOBiN5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2THg2iDrW3NGQZfz3SSWviwCe7GmNIvp5jEkGPCG  
cla4Fgdp/xuyewPk6NDlBewftLtHJVf=PAb3

Once encrypted, the message becomes a jumbled mess of random characters. But, equipped with the key I send you, you can decrypt it and find the original message:

Come on over for hot dogs and soda!

Whether it's in transit like our hot dog party email or resting on your hard drive, encryption works to keep prying eyes out of your business—even if they happen to gain access to your network or system.

The technology comes in many forms, with key size and strength generally being the most significant differences in one variety to the next.

## Common Encryption Algorithms

### 1. Triple DES

[Triple DES](https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained) was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more accurate. Despite slowly being phased out, Triple DES has, for the most part, been replaced by the Advanced Encryption Standard (AES).

### 2. AES

The [Advanced Encryption Standard (AES](https://cybernews.com/resources/what-is-aes-encryption/)) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.

AES is largely considered impervious to all attacks, except for brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

### 3. RSA Security

[RSA](https://searchsecurity.techtarget.com/definition/RSA) is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key to encrypt the message and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers a lot of time and processing power to break.

### 4. Blowfish

[Blowfish](https://searchsecurity.techtarget.com/definition/Blowfish) is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for its tremendous speed and overall effectiveness. Meanwhile, vendors have taken full advantage of its free availability in the public domain. You'll find Blowfish in software categories ranging from e-commerce platforms for securing payments to password management tools, where it protects passwords. It's one of the more flexible encryption methods available.

### 5. Twofish

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor [Twofish](https://searchsecurity.techtarget.com/definition/Twofish). Keys used in this algorithm may be up to 256 bits in length, and as a symmetric technique, you only need one key. Twofish is one of the fastest of its kind and ideal for use in hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it.

### 6. Crypto-JS

Easy to use. Incorporated with Javascript (a javascript package) and NPM, so fits with code we’re using. The team decided on this, but customer may provide input.