Contents

[INTODUCTION TO INS 2](#_Toc12346331)

[Cryptography techniques 2](#_Toc12346332)

[Asymmetric encryption 4](#_Toc12346333)

[Difference Between Symmetric and Asymmetric Encryption 5](#_Toc12346334)

# INTODUCTION TO INS

1. What is cryptography?

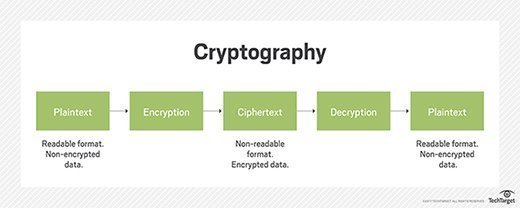
Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."[1]

Cryptography techniques

Cryptography is closely related to the disciplines of [cryptology](https://searchsecurity.techtarget.com/definition/cryptology) and [cryptanalysis](https://searchsecurity.techtarget.com/definition/cryptanalysis). It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling [plaintext](https://searchsecurity.techtarget.com/definition/plaintext) (ordinary text, sometimes referred to as cleartext) into [ciphertext](https://whatis.techtarget.com/definition/ciphertext) (a process called [encryption](https://searchsecurity.techtarget.com/definition/encryption)), then back again (known as decryption). Individuals who practice this field are known as cryptographers.[1]

Modern cryptography concerns itself with the following four objectives:[1]

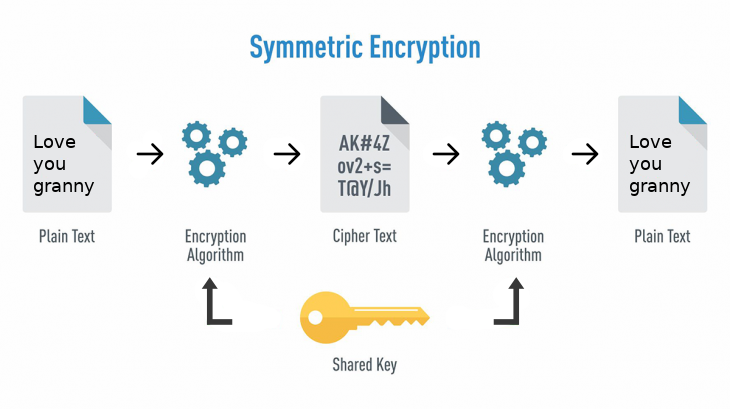
1. **Confidentiality**: the information cannot be understood by anyone for whom it was unintended
2. **Integrity:**the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. **Non-repudiation**: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
4. **Authentication**: the sender and receiver can confirm each other's identity and the origin/destination of the information



1. What is symmetric and asymmetric key cryptography?

Symmetric encryption

In **symmetric encryption**, you use the same key for both **encryption** and **decryption** of your data or message. Taking the example I gave above, sending a secure message to your granny, both of you need to have the same key in order to **encrypt** and **decrypt** the messages that you may exchange with each other.[2]



### Asymmetric encryption

**Asymmetric encryption** is quite the opposite to the **symmetric encryption** as it uses not one key but a pair of keys: a **private** one and a **public** one. One might ask:[2]

You use one to **encrypt** your data, which is called **public key,** and the other to **decrypt**the encrypted message, which is called the **private key.**

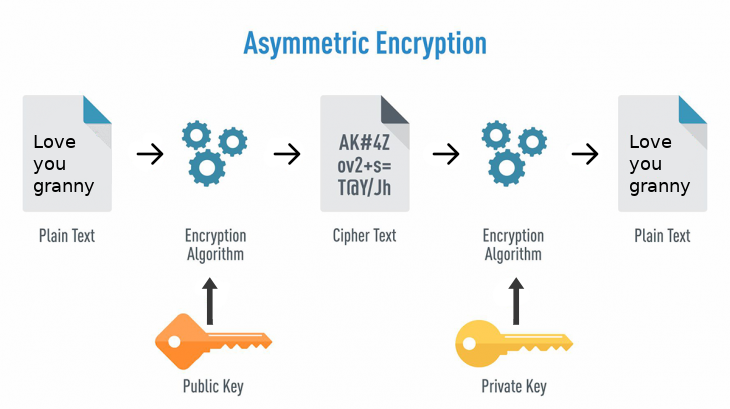
When you encrypt your message using, let’s say, your granny’s public key, that same message can only be decrypted using her private key.

#### Private keys

Your **private key**, as the name states, is yours and it must be kept private, as it’s the only key that can **decrypt** any messaged that was **encrypted** with your **public key**.

#### Public keys

**Public keys**as, yet again, the name states, are public and thus no security is required because of it should publicly available and can be passed over the internet. The **public key**is used to **encrypt**a message that can only be **decrypted** using, as I written above, its **private** counterpart.



Terms used:[3]

* **Encryption**: It is the process of locking up information using cryptography. Information that has been locked this way is encrypted.
* **Decryption**: The process of unlocking the encrypted information using cryptographic techniques.
* **Key**: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography.
* **Steganography**: It is actually the science of hiding information from people who would snoop on you. The difference between steganography and encryption is that the would-be snoopers may not be able to tell there’s any hidden information in the first place.

## Difference Between Symmetric and Asymmetric Encryption

* Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
* Symmetric encryption is an old technique while asymmetric encryption is relatively new.
* Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
* Asymmetric encryption takes relatively more time than the symmetric encryption.

Reference:

1. <https://searchsecurity.techtarget.com/definition/cryptography>
2. <https://hackernoon.com/symmetric-and-asymmetric-encryption-5122f9ec65b1>
3. <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>