WHAT IS IT?

Encryption is the process through which information or data is transformed (encoded) in such a way that is unreadable to anyone who does not have the knowledge of the way it was transformed.

The information thus becomes available only to the authorized parties. This authorization works based on keys. Encoding the information is made by using an encryption key while decoding the information is made by using a decryption key.

100-44 B.C. Caesar used a cipher to hide his military correspondence. The key in this case was simply to shift to the right by three.

The Greek historian Plutarch wrote, for example, about Spartan generals who sent and received sensitive messages using a scytale, a thin cylinder made out of wood. The general would wrap a piece of parchment around the scytale and write his message along its length. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense.

The Greeks were also the first to use ciphers, specific codes that involve substitutions or transpositions of letters and numbers.

WHEN WAS IT INVENTED?

Encryption prevents the interceptors of messages from having access to this information. Encryption does not prevent information from being intercepted by unwanted parties than the ones intended.

The easiest comparison that will help you understand this is: postcard versus letter in a sealed envelope. Unencrypted information transmitted via the Internet is like a message written on a postcard, anyone who can intercept it can read it. The encrypted information is like a letter, it is not visible even for those who are in contact with it. Of course these persons can open it, it's not the same thing for the encrypted message, and this is where the metaphor ends.

HOW DOES IT WORK?

Encryption example

<table>
<thead>
<tr>
<th>Plain text: A B C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption algorithm = move each letter one place to the left in the alphabet</td>
</tr>
<tr>
<td>Cipher text: B C D</td>
</tr>
</tbody>
</table>
There are two types of encryptions: symmetrical and public-key encryption.

In symmetrical encryption the encryption and decryption key are the same. So the communicating parts exchanging information among them have the same key.
In public-key encryption the encryption key is made public (public key) so anyone can use it to encrypt messages, but the decryption key is limitedly available to the intended receiving party (private key).

The public key is available to any computer that wants to have it and encrypt messages, while the private key is available only for your computer. For decoding a message both public and private keys are necessary. If somebody intercepts a message they will not be able to read it without the private key. The pair of keys is constructed using prime numbers (numbers that only have divisors of itself and one, such as 2, 3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is an infinite number of prime numbers which means infinite combinations and possibilities for keys. PGP, a very popular software that uses this type of encryption, works with the following process: the sender encrypts information using a symmetric key, the symmetric key is then encrypted using the public key of the receiver. The receiver uses its private key to decode the symmetric key. It then uses the symmetric key to decode the document.
A HISTORY OF ENCRYPTION

100-44 B.C. – Caesar used a cipher to hide his military correspondence. The key in this case was simply to shift to the right by three.

1973 – GCHQ describes for the first time this process of asymmetric encryption.

1977 – The first major asymmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES), approved for use in the 1970s. The DES uses a 56-bit key. Although a 56-bit key offers more than 70 quadrillion possible combinations (70,000,000,000,000,000), an attack of brute force (simply trying every possible combination in order to find the right key) could decipher encrypted data in a short while. DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys.


1991 – Phil Zimmermann writes and application with public key available called Pretty Good Privacy (PGP)

2010 – Symantec acquires PGP for $300M

WHERE IS ENCRYPTION USED?

It started out as being used by militaries and governments to allow secret communications.

Today it is used on a large scale by companies and civilians both to protect company and personal data.

Encryption protects security and privacy of the files on computer and it is also used to protect data transferred in different networks: on the internet, on mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

When it comes to security of information it is not only important to keep the confidentiality of the information but also the integrity and make sure the message is authenticating by employing methods like digital signatures.

DATA INTEGRITY

Hashing is another method through of transformation of a data in which you can ensure integrity of it. It ensures that the data has not been tampered with.

The same output can be produced by different inputs. This is an irreversible procedure, you cannot get from output to input.

Sources:
- https://ssd.eff.org/tech/encryption