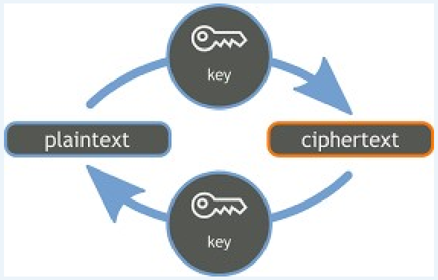
ISO/IEC 27001:2013 Information security management systems *-Cryptography-*

Security category – 10.1. Cryptographic controls

Control – 10.1.1. Policy on the use of cryptographic controls
The organization should develop and implement a policy for the use of cryptographic controls.



Cryptography is a system of coding information so it can be accessible selectively.

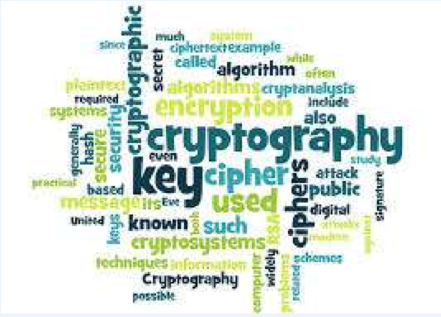
Symmetric - uses a single key to encrypt and to decrypt data
Asymmetric - uses what is called "public key

The blog of Panayotis Vryonis offers a very clear, simple and easy to understand for non-technical people explanation of cryptography.
https://blog.vrypan.net/2013/08/28/public-key-cryptography-for-non-geeks/

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Among the uses of cryptography:

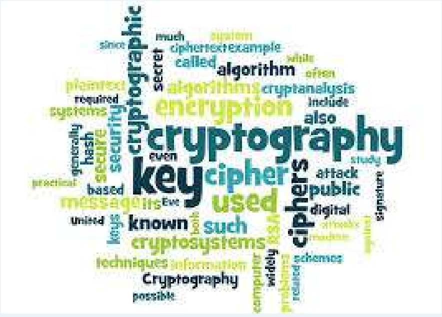
- protecting information that goes out of the organization;
- limiting access to files or folders on the servers;
- protecting confidential information sent by e-mail;
- protecting passwords;
- securing payments;
- digital signatures, …



The decision whether to use or not cryptographic controls belongs to the organization and to its needs to protect the information.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

ISO/IEC 27002 recommends a policy for the use of cryptographic controls that should address a few aspects:

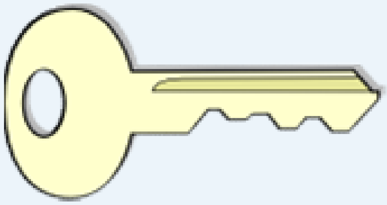


- general principles under which business information should be protected and the approach on the use of cryptographic controls;
- encryption algorithm used
- approach about using encryption for protection of information taken outside the organization;
- approach to key management – how are they protected and what happens in case keys are lost or compromised;
- responsibilities – who is in charge for the implementation of this policy and the management of the keys
- consistent implementation of the cryptographic controls throughout the whole organization

There are regulations and restrictions to the use of cryptographic controls that may exist in different countries and jurisdictions.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Control – 10.1.2. Key management
There should be a policy on the use, protection and lifetime of cryptographic keys.

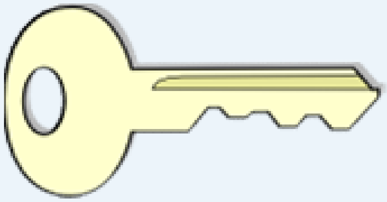


The organization has to protect the cryptographic keys against loss, modification, unauthorized access and disclosure.

Key management process should cover the whole lifecycle of the keys – generating, storing it, archiving, retrieving, distributing, retiring and destroying of keys.

ISO/IEC 27001:2013 Information security management systems
-Cryptography-

Policy on key management **- a set of rules that will apply to a number of activities like:**



- generating keys for different types of cryptographic systems and applications;
- issuing and obtaining public key certificates;
- distributing keys and their activation when received;
-storing keys;
- changing and updating keys;
- dealing with compromised keys;
- revoking keys – how are they withdrawn or deactivated;
- recovering keys that have been lost or corrupted;
- backup and archiving keys;
- destroying keys;
- logging and auditing key management related activities.

To reduce the likelihood of improper use ISO/IEC 27002 recommends defining activation and deactivation dates for keys - so that they can only be used for a period of time.

ISO/IEC 11770 – Key management