- Author: Petre Iordanescu
- Publisher: RENware Systems (www.renware.eu (http://www.renware.eu)), research, learning & innovation department
- Edition: 2021 August 24
- Language: EN, partial RO

About brief series. These materials are derived from author training sessions as course notes for students. It is intended as presentation of basic topics regarding a concept. These materials are intended to present for a concept whst is good for, its main topics and what to deep research to find out and learn more about it.

Cryptography. Brief. Overview.

Overview of cryptography

Briefley cryptography is a process of transforming information from a form in which its content can be understood (*clear information*) in a form in which the its content cannot be understood (*cryptic information*). This process is used from many years and is derived from human necessity to hide part of messages they exchange in order to be understood only by some persons and not by anybody.

Is important to mention that is not always necessary to make a perfect encryption (ie, mathematically impossible to decrypt). Often is enough to make a simpler encryption which just take enough time to be decrypted, time that will make the information obtained to be no more usable or valuable or not interesting, generally not relevant after some time.

But be aware to decryption because even if information is not relevant when was decrypted, it is possible to speed up the process for next decryption. Different methods are used avoid this issue, the most frequent being to change periodically the encryption keys.

A simple example

Probably the best known transformation is to translate a proposition by replacing all its characters with those shifted with 3 (for example) as position in alphabet. So, by this transformation the character A will become C, B will become D, and so on.

Even it is extreme simple example, this is nothing else that a basic form of real cryptography...

A little bit of math

The cryptography is first about mathematics and math is about numbers (in computers use clearly defined numbers not approximations, like square root of 2). Therefore, the cryptography can be easily understood if is accompanied by a basic math knowledge.

Definitions

Functions. A function is a transformation process from one value to another. The formal notation is $f(x) = y$ which means that function *f* transform value *x* in *y*.

Sets. All values of any *x* comes from a set named *source set* and all values of *y* results belong to a set named *target set*.

Encryption. Is the transformation process done by *f* over *x*.

Clear message. *x* is the message in its intelligible form.

Cryptic message. *y* is the message encrypted.

Decryption. Is the reverse of encryption. By description will obtain *x* from *y*.

Reverse function. Is the function that assures the decryption process. The reverse of function *f* is called *f^(-1)* and is defined as:

> if *f(x) = y* then *f^(-1)(y) = x*

Parameter. Is any variable by which a function depends, ie those which can be found in this part of function: (z, x, ...).

Notations

- **En** is an encryption function
- **Dc** is a decryption function
- **K** or **(K1, K2, Kn)** are parameters (keys) used in encryption and decryption as single / unique key or set of keys. These paeameters are named keys because must be given as function inputs...
- **M** is generally a message in clear
- **Mc** is a message in its encrypted form

Example 1. *Mc = En(M, K)* is the encryption of message *M* by using the key *K*, resulting message *Mc*.

Example 2. *M = Dc(Mc, K)* is the dencryption of message *Mc* by using the key *K*, resulting message *M*.

The notations, abbreviations and definitions will be used in all cryptography articles.

Properties (basic)

- Reversible vs not reversible
- Deterministic vs non deterministic
- Symmetrical vs asymmetrical

Reversible vs not reversible property

A **non reversible property** means that for a function *En* there is no *Dc* (from a mathematically point of view). This kind of functions are usually kinds of things that in math are named "concepts" and are solved by limits or series. In most cases they are not usable "as is" not only in cryptography but in

computers in general, because of computers necessity for "finite and concrete / clear numbers". We do not insist on this, being out of the article scope.

What is interesting is about those functions that are **hard reversible**. An encryption function is *not easier to reverse* if:

- by reversing produce ambiguous results
- determination of the reverse function will take enough time being useless when found
- determination of the reverse function will take enough resources being impracticable or impossible in real world

If a hard reversible function produce the same result for identical inputs (*M* and *K*), even if you can not decrypt a saved *Mc* (a password for example), you can still compare the *Mc* produced by entered data (user and password by continuing the example) with stored *Mc*, and can take useful decisions! And MOST IMPORTANT THING; if somebody access the database and get the saved passwords cannot decrypt them!!! (or cannot do it with usable results, the decryption being ambiguously).

Deterministic vs non deterministic property

A **deterministic** function *En* is one that has the property that for a given key *K*, the *En(M, K)* **produce different *Mc*** depending on *M*. In other words, *En(M1, K) ≠ En(M2, K) if M1 ≠ M2*.

In contrast, a **non deterministic** function, **can produce the same *Mc*** for different *Mn* with the same key. In other words, *En(M1, K) could be = En(M2, K) if M1 ≠ M2*.

At first look, a non deterministic function seems to be useless and not usable, but the *hashing* [more details in ref 1] alghoritms exactly with this kind of function works. And in cryptography these kind of functions are largely used.

NOTE: As can be seen, non deterministic syntagma is not exactly used as 'defined in dictionary'. The non deterministic property refer only to the reverse function (decrypting). Direct function (encrypting) must be deterministic otherwise is really not useful in practice.

A typical example of such function is the *modulo function* which gives the samd results for many numbers by dividing them to the same number (ie, the key). And the reverse function, gor the ssme reminder can find many numbers that are producing it (the result set is large, depending on key and password as message).

Symmetrical vs asymmetrical property

This property refers to the ability of a function *En* to be decrypt by a function *Dc* in the following conditions:

- a message *Mc = En(M, K)* will be decrypted into *M* using the same *K* used in encryption process (alghoritm, function). That is **symmetrical encryption**.
- a message *Mc = En(M, K)* will be decrypted into *M* using the another *K1* used in encryption process (alghoritm, function). That is **asymmetrical encryption**

In a **public (KPu) private (KPr)** keys alghoritm what is encrypted with *KPu* can be decrypted only and only with *KPr*. Reversing follows the same rules and pattern, what is encrypted with *KPr* can be decrypted only and only with *KPu*.

Notes and remarks

- in symmetrical alghoritms must be used the same *K* in *Dc* as used in *En*
- in asymmetrical alghoritms *K1* used in *Dc* must be different than *K* used in *En* (otherwise is symmetrical!)
- the asymmetric property is relative newly used un practice, because is hard to be executed manually (very complex and long calculations). The *Enigma* machine is one of the oldest asymmetrical "cryptography computer".
- the asymmetric property is at the base of modern computers security especially in networking; protocols like *https* and all what means *SSL* (Secure Socket Layer) and *TLS* (Transport Layer Security)

More details - ref [2].

Conclusions

The cryptography is strictly required when talking about security in computers and networking. It is si important that nowadays there are produced many specialised chips dedicated to cryptography alghoritms. And that chips exists with almost new produced computers, even for home computers.

The asymmetrical alghoritms has been "reinvented" the world, being ni big issue to have a digital certificate to electronic signature.

Notes and biographical references

- 1. Hashing in cryptography (https://en.m.wikipedia.org/wiki/Cryptographic_hash_function)
- 2. [Public private key] (https://en.m.wikipedia.org/wiki/Public-key_cryptography (https://en.m.wikipedia.org/wiki/Public-key_cryptography))