Short Essay on The Importance of Cryptography

João Pedro Amaral Dias

November 2019

Nowadays we live in a tech world where data protection is very important and privacy is an essential good, and what better way to improve the protection of your data and your clients data then to learn the basis of cryptography. This talk, given by Adam Englander, explains the basics of cryptography to anyone who wants to learn more about the subject. The speaker tries to pass the message that cryptography is very important to secure communications even if this communication is made on your computer, like storing some file in your hard drive. During this talk is also explained the different methods used in cryptography and how can we be good when using them to fight attacks like brute-force or cryptoanalysis.

A mean to secure communications against third parties called adversaries is the definition given by the speaker to cryptography, in the beginning of the talk. He then proceeds by stating the difference between ancient cryptography and modern cryptography. Both differ in what is consider the secret, since in the ancient cryptography the secret was the algorithms used to encrypt data as of modern cryptography the secrets became the keys used by the algorithms, meaning that this algorithms became public and documented. This algorithms can be divided in symmetric algorithms, that use a shared key, and assymmetric algorithms, that use both public and private keys. This encryption algorithms alongside hashing, digital signature and key derivation answer the question on how cryptography is used. Hashing is defined as the creation of a representation of the data that cannot be reversed while digital signature is the process of hashing data with the help of a private key in order to identify the source of the data. The last method used in cryptography is key derivation that consist in cyclic hashing and is highlight as very important by the speaker specially when dealing with passwords. To support the thesis the speaker also talks about some cryptanalytic attacks used to try accessing data that is not owned by the attacker and how cryptography is important to defend against this attacks.

The protection of sensible data is the main argument presented by the speaker to support the thesis that cryptography is important, more precisely the protection of passwords. As the processing power increases, attacks that resort to brute-force and cryptoanalysis become stronger so the need to understand the basic concepts of cryptography and become better at it rises significantly. Other argument given to support the thesis is the necessity of data source validation. This is were digital signatures steps up as a good way to deal with this problem, as the file is hashed with the help of the user private key, protecting the file integrity and source. The used of this methodologies, although they seem difficult, are simplified in some programming languages that offer to the user well documented libraries that are easy to apply.

Even though the speaker encourages everyone to study cryptography some issues may rise when digging deeper in the field. As the complexity of the algorithms increase, the need for more processing power increases also and this may cause an increase of power consume by the user leading to expensive costs. There are solutions to this problems, like renting processing power, but this solution is not well regulated and can lead to legal trouble. Other argument that may discourage the focus on cryptography is that the attackers don't care about this legal issues so they do everything in their reach to get more processing power in order to improve theirs attacks. This difficult the job for someone who has a small business and is being introduced to the world of cryptography to protect his customers, as they don't have the means to fight this attacks.

Above all cryptography is a field with future and it's here to stay, because the data will always need protection and encryption is the best solution to protect the data against evil third parties. The processing power can be a blocker in some situations but the drop of hardware prices can help mitigating this issue. Also in the future this field can suffer some changes with the introduction to quantum computers and quantum algorithms giving people with some knowledge in standard cryptography some leverage to study this new field.