Decrypting Cryptography

-Roop Inder Singh

-CSE-CCVT 1st Year

One might have often come across individuals who have professional inclination towards data and cyber security and one might have often also heard them discussing or talking about a tool that they use, which is called cryptography that empowers them to achieve their endeavours. Today we shall decode this term cryptography and understand the meaning and finer nuances associated with the term.

The term cryptography has been made up of two words *kryptos* (meaning hidden) and *graphien* (meaning writing) and hence means hidden-writing. It is basically the science of encoding the message or the data that is to be sent from the source to the destination through an IT Network to prevent third parties or adversaries to gain access to high profile or private data during its transport. This signal that is being transferred is encrypted by using a key, which is a reference table or a protocol, and after the transfer of the message/ data is complete then it is decoded or decrypted by using a matching pair of key that yield the original message. Cryptography helps a lot in the secure transfer of data and preventing pilferage and loss of data or stealing of the same by miscreants or black-hat hackers. Hence, cryptography plays an important part for enforcing the principles of Data Integrity and Confidentiality of data during the data transfer. Many data-communication and transportation firms, corporate houses, almost all the military network communications and advanced protocol based data transfer on the internet rely upon cryptography to keep their data safe and their secrets locked tight.

No matter how cutting edge the science of cryptography seems, but it isn't totally a thing of 21st century and one might be surprised at the fact that it has been popular since the early stages of 20th century. In early twentieth century the idea of cryptography was employed with the help of rotor cipher machines which were basically primitive mechanical computers that were able to convert analogous signals from a source (such as a Morse-code telegraph) and jumbled them up according to a predefined mathematical algorithm to ensure secure communication. In the mid-twentieth century, during the

Second World War (1939-1945) the art of cryptography was further perfected by the German mathematicians who with the help of more advanced computing approaches available at that time created the enigma code that was used by the German Army to help the German generals secretly communicate with other generals and commanders as well as transmit commands to its naval fleet and soldiers on the battlefield without anyone noticing the same. The code was processed, i.e. encrypted as well as decrypted by a machine called the Lorenz Cipher machine. Over the years along with the great advancement in technology, the cryptographic methods that are employed to safely transmit the data have also progressed by leaps and bounds and more advanced and secure methods for encrypting the messages and the data being transferred have propped up. However, a large portion of the protocols and rules that govern it are still based on computational mathematics.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. The Modern Cryptographic theory uses a number of ideologies and protocols to achieve the much needed data integrity and privacy. The modern field of cryptography can be divided into several areas of study. The chief ones are as follows:

SYMMETRIC KEY CRYPTOGRAPHY: - Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). In this the sender as well as the receiver have private keys that are only known to them alone. This is a more secure way and is quite popular.

ASYMMETRIC KEY CRYPTOGRAPHY: - Asymmetric-key cryptosystems do not use the same key for encryption and decryption of a message, on the contrary, both the sender and receiver have different set of keys and one of them is publicly available in a designated server while the other one is private.

CRYPTANALYSIS: Cryptanalysis is the process of analysing the in use cryptographic patterns and protocols and trying to improve on them and make them more secure. The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

Since the advent of modern cryptographic protocols and methods, it has becoming increasingly difficult to pilfer, steal or modify the data when it is on the move much to the agony of the hackers and miscreants but then again it is imperative to understand that just given that a message has been encrypted doesn't imply that it is totally safe from being hacked either. It is after all possible to crack open an encrypted package by using the same good old mathematics that it is based on although the time required may vary depending on how good the encryption was. Also, there are methods like brute force attacks that can break into any and all forms of encryption no matter what by applying elaborate mathematical algorithms and permutations although the time taken for the operation to yield the result may be astronomical.

So now one of the primary objectives is to make the encryption protocols and algorithms such that they are so complex to decrypt without a dedicated key that they can't be decoded in a practical amount of time which will render trying to crack them futile and fruitless. To sum up, the boost cryptography has given to communication reliability and data security and its like the one–time-pad cryptographic schema (that is the most robust cryptographic technique and can't be broken even with unlimited computing power) more than aptly justify why it is so famous anti-pilferage measure and why it is here to stay and serve for long.