Volume - 2
Issue - 1
January 2020
e-ISSN 2582-5755

10

Cryptography: A Never Ending Technology

– **Ayushi Singh**
Bachelor of Computer Applications, (BCA) 6th Semester, Amity University, (AIIT), Noida
https://orcid.org/0000-0002-6434-801X ayushi171717@gmail.com

In today's world, we see every person is having some personal or private data, which he/she wants to keep private and confidential so that no other person can access that data without his or her permission. Cryptography is a technique to implement this process. Cryptography is being used from very ancient times about thousands of years ago. It keeps on modernizing with the time. Let's see in this article what cryptography is all about.

ARTICLE HISTORY
Paper Nomenclature: View Point (VP)
Paper Code: CYBNMV2N1JAN2020VP2
Submission Online: 08-Jan-2020
Manuscript Acknowledged: 10-Jan-2020
Originality Check: 11-Jan-2020
Originality Test Ratio: 2%
Peer Reviewers Comment: 17-Jan-2020
Blind Reviewers Remarks: 19-Jan-2020
Author Revert: 20-Jan-2020
Camera-Ready-Copy: 28-Jan-2020
Editorial Board Citation: 31-Jan-2020
Published Online First: 31-Mar-2020

Keywords
- Cryptography
- Encryption
- Steganography
- Bitcoin
- Technology

Introduction:

Cryptography is the process or technique to hide the personal or private data of a user or an organization in such a manner that if any unauthorized user able to access that data then also he will not be able to understand the actual meaning of the data. To achieve cryptography, we use encryption and decryption technique.

Fig 1. Cryptography

History of cryptography

Cryptography was first seen in 1900 BC in the walls of a tomb in non-standard hieroglyphs from in old kingdom of Egypt. Let's understand the Types of cryptography.

cryptography, in this cryptography we are having a plain text and a key using which the plain text is converted into cipher text.

Formula: C= P+K

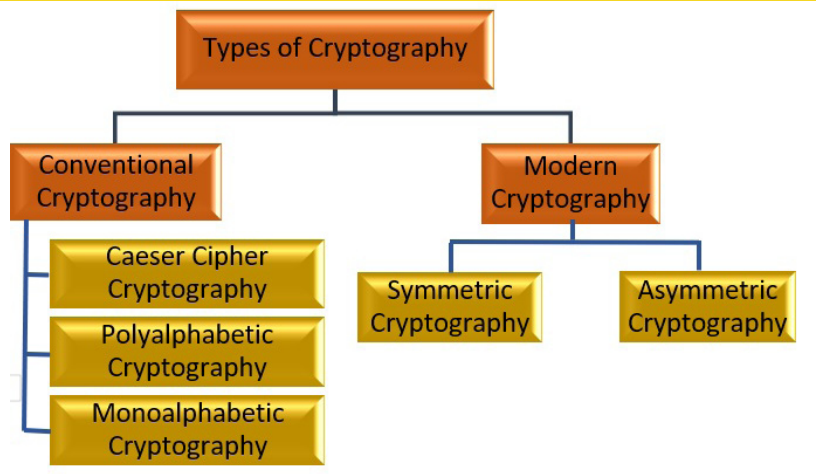


Fig 2. Hierarchy of Cryptography

Conventional Cryptography:

Caesar-cipher Encryption Technique:

It was the first encryption technique introduced in conventional

Example:

Plain text, p= **"Amira"**

Key, k = 5

Cipher text, C= **"Frnwf"**

Monoalphabetic Technique: In this conventional cryptography technique, we replace all the 26 characters of alphabet with corresponding 26 alphabets without repetition.

Example:

Plain text, p= **"Amira"**

Cipher text, C= **"Kmbnk"**

Polyalphabetic Encryption Technique:

In this conventional cryptography technique, we are making a matrix from A-Z, i.e., of size 26X26 (also called The Vigenere Table), and we have a plaintext and a key using which we convert the plain text to ciphertext.

Example:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plain text, p= **"UPASH"**

Key, K=" EEGKS"

Cipher text, C= **"YCGHZ"**

Similarly, there are many conventional encryption techniques like:

- Hill cipher technique
- Transposition technique
- Steganography

Modern Cryptography:

Nowadays we start using the modern cryptography which is basically on coding, complex algorithms and hard patterns.

Types of modern Cryptography:

Symmetric Key Cryptography:

In this cryptography technique we are having a single key or same key for both the purpose's, i.e. encryption and decryption.

Examples:

- DES
- Triple DRE
- RC4/RC5
- Blowfish
- Serphent

Asymmetric Key Cryptography:

In this cryptography technique we are having two different keys, where one key is called public key and the other key is called private key, if we are using public key for encryption then we have to use private key for decryption or vice versa.

Example:

- RSA
- DSA
- ECC
- DSS

Uses of Cryptography:

- It is used for secured and integrated data transmission system.
- It is used for secured and integrated storage system.
- It is used to provide security to multi-communication channels.
- It is used in cryptocurrency.

Advantages of Cryptography Technique:

- **Confidentiality:**

It provides privacy and security to our data from theunauthorized access and unauthorized users.

- **Authentication:**

It is having techniques like digital signature and MAC which helps us protect our data from spoofing and forgeries.

- **Data Integrity:**

Technique of Cryptography like hashing helps us assuring the user about data integrity.

Volume - 2 Issue - 1 | January 2020 | e-ISSN 2582-5755

- **Non-repudiation:**

Cryptography technology like digital signature helps the user or group to protect against the dispute which may occur due to denial of commitment done by the sender.

Best to come in Cryptography:

In coming future, we may see this Cryptography being more updated and modernized which can't be compromised at any cost.

We have already seen some implementation of Cryptography in the form of blockchain and cryptocurrency (like bitcoin, etherium), soon we will see the Cryptography everywhere, in our currency, gadgets, daily used techs and in many more things.

Conclusion:

In this article we saw how the Cryptography has changed the world in terms of data security and many more things. We show how Cryptography technology has evolved with time and how it'll be the main part of every technology in coming future. With the increase in technology we also need more and more security and this will never let the Cryptography technology go obsolete, Cryptography will keep rising with time.

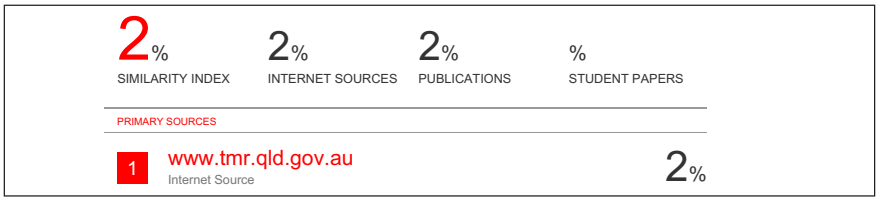
"Need data security,
Let's do Cryptography:)"

Ayushi Singh is a student of Amity University, pursuing her bachelors in computer applications (B.C.A.). She is passionate about seeking knowledge about the current trends going in Research & Innovation. Her area of interest is IoT and Block chaining. She is a creative thinker and love to work on what she Imagine. She is an energetic, productive, focused, goal oriented and organized student with an exceptional work ethic. She has made a part for LIGHTHUSKY.COM website where she has work upon the "Real Time Weather Data-fetch". She is also a technical member in BLESSINGS NGO where she maintains their website and other technical work. She is communicating with two research paper in journals. She has also applied three patents (in queue) in field of IoT and Blockchain.

ayushi171717@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
11-Jan-2020	1244826022 (Turnitin)	1195	6584



Note:- The Cybernomics had used the Turnitin plagiarism [http://www.Turnitin.com] tool to check the originality.

Reviewers Comment

Review 1: The paper has very well covered the theme of cryptography and its significance in todays time.

Review 2: The argument that national security is enhanced by perforating secure encryption has been roundly and consistently condemned by the security industry.

Review 3: The Law enforcement and technologists have been arguing over encryption controls for more than two decades. It has evolved with time and how it'll be the main part of every technology in coming future.

Editorial Excerpt

This article has 2% plagiarism which is accepted as per the standards of publication for the comments related to this manuscript are noteworthy to the theme "**Cryptography**". The author has covered all the facts in current scenario. As encryption technologies advance, everything will shift over to biometric markers like impressions, facial recognition and voice recognition. This type of skill will eliminate the need for remembering infuriating passwords and answers to secret questions After blind reviwers and editorial boards' remarks the article has been finalised to pulish and categorise under "**View Point** (VP)" category.

Acknowledgement

Special thanks to my parents (Mrs. Shweta Singh & Mr. Rajvir Singh) and all faculty mentors who have always supported me, in my interests. Special thanks to Ms. Rajbala Ma'am for motivating and giving me the opportunity to write the article "Cryptography: A never ending Technology" for Cybernomics.

Disclaimer

All views expressed in this paper are my/our own. Some of the content is taken from open source websites & some are copyright free for the purpose of disseminating knowledge. Those some We/I had mentioned above in the references section and acknowledged/cited as when and where required. The author/s has cited their joint own work mostly, Tables/Data from other referenced sources in this particular paper with the narrative & endorsement has been presented within quotes and reference at the bottom of the article accordingly & appropriately. Finally some of the contents which are taken or overlapped from open source websites for the knowledge purpose. Those some of i/we had mentioned above in the references section.

Citation

Ayushi Singh
"Cryptography: A Never Ending Technology"
Volume-2, Issue-1, Jan 2020.
(www.cybernomics.in)

Frequency: Monthly, Published: 2020
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in
https://orcid.org/0000-0002-7952-096X