Review Paper on Cryptanalysis Techniques Application in Business Management

[1st] Mr. Suyash Barve
MITACSC ALANDI(D.)
Pune,India

[2nd] Mr. Bareen Shaikh
MITACSC ALANDI(D.)
Pune,India

***Abstract*- Cryptography it is the term used to share any hidden message or to study the hidden message. Data security ensures that our data is only accessible to the intended receiver and it prevents any modifications or alterations of the data. The need of automated tools for protecting files and other information stored on the computer became mandatory. This is required for a system like time-sharing system and also sometime need is even more acute for systems that can be accessed over a public telephone data network or internet. The present day the data security system consists of confidentiality, authenticity, integrity, non-repudiation. Our information needs to be secured by the different types of attacks, it is only possible by the certain technique like Substitution and Transposition technique that is followed by the Encryption and Decryption process in cryptography. In this paper various encryption and decryption techniques are discussed which can be applied on different types of cyber-attacks and which can be useful for various big organization for exchanging of confidential data or messages.**

KEYWORDS: Cryptanalysis, Cipher, encryption, decryption.

I. INTRODUCTION

Cryptography it is the term which is used to share any hidden message or to study the hidden messages. Cryptography is the art and science of achieving security by encoding messages to make them non-readable [1]. Information security is the main concern in front of all organizations. 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. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means .

II. OBJECTIVE:

To maintain privacy, confidentiality, data integrity, authenticity, and non-repudiation.

Types of cryptography:

A. Symmetric key cryptography:

The sender and the recipient both uses a same key for the encryption and the decryption of the message is known as the symmetric key cryptography.

B. Asymmetric key cryptography:

The key that is used for the encryption of the plain text by the sender, is not applicable while the decryption. It means that the sender and recipient both needs different keys while accessing the message.

III. ENCRYPTION

The plain text is transformed into cipher text by the encryption process. The plain text is encoded by the encryption process. In technical terms, the process of encoding plain text messages into cipher text messages is called as encryption.

IV. DECRYPTION:

The cipher text is transformed into plain text by the decryption process.

The cipher text is decoded by the decryption process. The reverse process of transforming cipher text messages back to plain text messages is called as decryption.

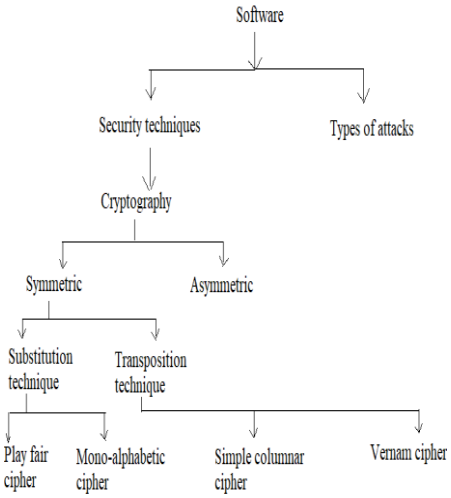

Fig. 1

Different types of techniques:

A) Substitution technique:

In the substitution technique, the characters of a plain text message are replaced by other characters, numbers or symbols.

- Mono-alphabetic cipher: Mono-alphabetic ciphers pose a difficult problem for a cryptanalyst because it can be very difficult to crack thanks to the high number of possible permutations and combinations [1]. If "A" is encrypted as "Y" in the cipher text. "A" will always get encrypted to "D".
- Polyfair cipher: The poly fair cipher is also called as playfair square, is a cryptographic technique that is used for manual encryption of data.

Now the word MOBILE is we are encrypting.
The word `MO BI LE` in plain text is encrypted as `DI NA FX`.

TABLE I

B) Transposition technique:

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

In the transposition technique some permutations are performed over the plain text alphabets.

C) Simple columnar technique: The plain text "MY NAME IS SUYASH" is encrypted by using the random key "Four".

TABLE II

M	Y	N	A
M	E	I	S
S	U	Y	A
S	H		

We arranged the column and row equal to the key value.
The cipher text is "MMSSYEVHNIY ASA".

D) Vernam cipher (one-time pad):

In the vernam cipher Algorithm the plain text message is 'SUYASH' and the key used is 'ILNPWJ'.

plain text - S U Y A S H
19 21 25 1 19 8
+
Key- I L N P W J
9 12 14 16 23 10

Initial total- 28 33 39 17 42 18
2 7 13 17 16 18
Cipher text- B G M O P R
The cipher text is 'BGMOPR'.

CONCLUSIONS

The research paper explains different techniques of the cryptography in which the communication can be encrypted and decrypted. Here the above techniques can be combined to create a more well-built and persuasive cipher text which cannot be easily decrypted by the third party. In business management these different techniques can be applied for the confidential information sharing between two business parties. In further paper the combined technique implementation work will be made.

REFERENCES

[1]Atul Kahate, CRYPTOGRAPHY AND NETWORK SECURITY.
[2]Savita Kumari research scholar, A research Paper on Cryptography Encryption and Compression Technique.
[3]Abdalbasit Mohammad Qadir, Nurhayat Varol