CRYPTOGRAPHY

[1]Biswanath Ghosh, [1]Rohit Aich, [1]Arka Khag, [1]Sattam Nayak, [1]Prashant Kumar

[1]Department of Basic Science and Humanities

Institute of Engineering & Management, Salt Lake Electronics Complex, Kolkata-700091.

Abstract

The word cryptography was coined from two Greek words 'Krypto', meaning hidden and 'graphein' meaning writing. Thus, cryptography means hidden writing. Cryptography is the method of protecting important data and information from third parties called adversaries or the public. It is also known as encryption. Modern cryptography is basically based on Mathematics and Computer science. The roots of cryptography are found in Roman and Egyptian civilizations. Hieroglyph is the oldest cryptographic technique. Based on security needs and threats, various cryptographic methods such as symmetric key cryptography, public key, private key, microdots, etc are adopted [1]. It is a two step process; encryption and decryption. The encryption process uses a cipher (code) in order to encrypt plaintext and convert it into ciphertext. Decryption is the opposite of encryption that is to decode the encrypted message or information. Cryptography was used extensively in the American Revolutionary War, the First World War and the Second World War. For example if the code was 'CVVCEM' then it would mean 'ATTACK'. The initials of each letter is shifted by two places. This paper is basically a survey paper and we have studied the importance, features, advantages, and disadvantages and authenticated on the topic cryptography. **Note:** This paper is a **REVIEW PAPER**.

Keywords: *hieroglyph, cipher, cryptanalysis, cryptosystem, key, cryptology, encryption, decryption, alice, bob, confidential, authentication, data integrity, repudiation.*

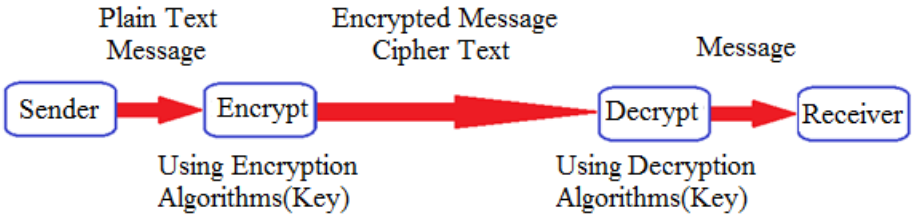
INTRODUCTION

As mentioned above, cryptography is the method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it [2].But, sometimes, it is not so secure. Attacker or third party may corrupt or hack or can change the data and can misuse it also. So, to provide security and protect valuable information and data, cryptography can be used. Alice and bob are two fictional characters commonly used as placeholders name in cryptology. Alice and Bob communicate over an insecure channel, such as the internet or a cell phone. An eavesdropper, Eve, is able to see the whole communication and to inject his/her own messages in the channel. Alice and Bob hence want to find a way to encode their communication so as to achieve privacy. Eve have no information about the content of the messages exchanged between Bob and Alice. Eve should not be able to impersonate Alice, and every time that Bob receives a message from Alice, he should be sure of the identity of the sender [1]. For example, if Alice is our laptop and Bob is your wireless router, you might want to make sure that your neighbor Eve cannot see what you are doing on the internet, and cannot connect

using your router. In the classical symmetric-key cryptography setting, Alice and Bob have met before and agreed on a secret key, which they use to encode and decode message, to produce authentication information and to verify the validity of the authentication information. In the public-key setting, Alice has a private key known only to her, and a public key known to everybody, including Eve; Bob too has his own private key and a public key known to everybody. In this setting, private and authenticated communication is possible without Alice and Bob having to meet to agree on a shared secret key.

Key is a piece of information that determines the functional output of a cryptographic algorithm. A key transform the plaintext into ciphertext and vice-versa. There are basically two types of keys: Symmetric cryptography and Asymmetric cryptography. Symmetric cryptography is used by the sender to encrypt the data and by recipient to decrypt the data. Asymmetric cryptography is a cryptographic system that uses a pair of keys: public keys which may be disseminated widely, and private keys which are known to the owner only. In such a system, any person can encrypt a message using the receiver's public key but that encrypted message can only be decrypted with receiver's private key [1]. The number of keys required increases as the square of number of network members.

When a message is sent using cryptography, it is changed before it is sent. The method of changing text is called a code or cipher. Example of the process of cryptography is as shown below:



The change makes the message hard to read. Someone who wants to read it must decode it (change it back). The changing back is the secret. Studying the ciphertext to discover the secret is called 'cryptanalysis'. Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems. In addition to mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side channel attack that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation[1,3].

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input and gives output a short, fixed length hash, which can be used for digital signature[1].

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptosystem. It uses the properties of the underlying cryptographic primitives to support the system's security properties. Some widely used cryptosystem include RSA encryption, PGP, etc.

Nowadays, computers are here to decode the code and they do it quite quickly and can even do very strong encryption. Examples are AES, RSA, etc. Cryptography is widely used in computer passwords, ATM cards, e-commerce, Net banking, chip based payment, military communications, etc.[1].

Quantum cryptography is the only known method for transmitting a secret key over distance that is secure in principle and based on the laws of physics. Current methods for communicating secret keys are all based on unproven mathematical assumptions. These same methods also are at risk of becoming cracked in the future, compromising today's encrypted transmissions retroactively. This matters very much if you care about long-term security[5]. In quantum computing, a qubit or quantum bit is a unit of quantum information the quantum analogue of the classical bit. Unlike a classical bit which can take only the value of either 0 or 1, the state of a qubit can be in a 'superposition' of 0 and 1 simultaneously.

DISCUSSION:

This paper is basically a **review paper** in we have studied the importance, features, advantages, disadvantages and authenticated on the topic cryptography.

Cryptography is thus the practice and study of techniques for secure communications in the presence of third parties. It is basically creating some protocols that prevent public from reading information, private messages, confidential data, data integrity, etc. cryptography was used extensively during the First and the Second World War for the transfer of data and information among the soldier so that enemies couldn't understand the message[4]. Modern cryptography is the intersection of mathematics, computer science, communication and electrical engineering. Cryptography is also known as encryption. Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption[1]. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

CONCLUSION

Cryptography is very much essential in our day to day life. Without cryptography, there will be no confidentiality, no security, no data integrity, and there will be obviously repudiation. Thus, without cryptography, the conduct of business over networks using the computer system was

extremely difficult. But, on the other hand, it has drawbacks also. A strongly encrypted, authentic and digitally signed information can be difficult to access. Sometimes, cryptography costs huge amount. So, there are both advantages and disadvantages of cryptography [6].

REFERENCES:

1. www.wikipedia.org

2. www.economictimes.indiatimes.com

3. www.searchsecurity.techtarget.com

4. Cryptography and Network Security by Stallings William

5. Cryptography, Network Security and Cyber Laws by Bernard L. Menezes

6. www.tutorialspoint.com