International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

CRYPTOGRAPHY

K. SREE LATHA
Lecturer, Dept. of Mathematics,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad,
Telangana, India.

S. SAILAKSHMI
Lecturer, Dept. of Mathematics,
Bhavan's Vivekananda College,
Sainikpuri, Secunderabad,
Telangana, India.

Abstract: Abstract: In the spirit of algebraic abstraction, this paper advocates the definition and use of higher levels of abstraction in cryptography (and beyond). If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems

Keywords: abstract cryptography, relevant aspect, particular model, abstract viewpoint.

I. INTRODUCTION

Discipline or techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. Only the use of a secret key can convert the cipher text back into human readable (clear text) form. Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another.

I. WHAT IS CRYPTOGRAPHY

Cryptography is a mathematical science that uses mathematics to create problems that are difficult to solve.Using these problems data can be secured by encryption.Using mathematic such as Fermats' theorem used in Public Key Encryption.If "P" is prime and "a" is a positive integer not divisible by "P",

$$\text{Then : } a^{p-1} = 1 \pmod{P}.$$

Cryptography is the technique to transform readable data to unreadable data. We deal with it every single day of our life. Many important areas of science use cryptography, but everyone of us has been using it for years, yet did not realize what he/she was doing. One can write and research endlessly when it comes to cryptography, there for this is just a little peak in the area where it is applied. Now let's see where cryptography is used.Cryptography - the art of writing or solving codes.

II. ENCRYPTION AND DECRYPTION

1. **ENCRYPTION**: (Gupta lekanam)
   The process of converting readable data (Plaintext) into a coded form (Cliphertext) to prevent it from being read by an unauthorized party.

2. **DECRYPTION**: (Vyakth parucu)
   The activity of making clear or converting from code into plain text.To converts an encrypted or coded text or message into plain text.

III. METHODS OF CRYPTOGRAPHY

Which cryptography method is the best? It depends on what the intent for the cipher is and how concerned you are that it may be broken. In this article I will discuss the different methods and help you determine which is best suited for your needs.

INTRODUCTION

Cryptography methods range from the simple to the complex. Simple methods of cryptography include the substitution (or Caesar's Alphabet) method. Reciprocal methods include the Enigma machine. Symmetrical and Asymmetrical methods came along later and are still in use today.

SUBSTITUTION METHODS

The substitution method is exactly what its name implies. The letters of the alphabet are either slid over a certain number of spaces (for example ABC becomes DEF) or are substituted for numbers or symbols (ABC for 123 or ABC for #*%). The main problem with this method is that the cipher is easily cracked. These methods are commonly seen in the newspapers in the puzzles section.

RECIPROCAL METHODS

The reciprocal method works like this. The plaintext is inputted into a machine that creates the cryptograph. The letters are "flipped" in pairs. For example, if "C" is substituted with "L", then any "L" in the plaintext will be substituted with "C" in the cipher. While this is more secure than plain substitution, if the cipher is entered into the same type of machine (with the same key), it will output the plaintext--without any work on the part of the person trying to read it.

SYMMETRIC METHOD

Symmetric methods are also known as single key ciphers. There is one key that is used to encrypt and decrypt the plaintext. The key needs to be passed on to the recipient. Also the fact that there is one key (or in some cases the two keys are directly related to each other), the key can be broken. Two variations of this are block cipher and stream ciphers. The stream is one bit of plaintext at a time, whereas the block is a number of bits at once. An example of symmetric keys is Data Encryption Standard (DES).

ASYMMETRIC METHOD

The Asymmetric method is also known as a public-key method. The key holder has two keys--a private key (which only they know) and a public key. When a person wants to encrypt a message or file, they use the Public key of the recipient to encrypt it. This ensures that only the recipient can read the message or file.

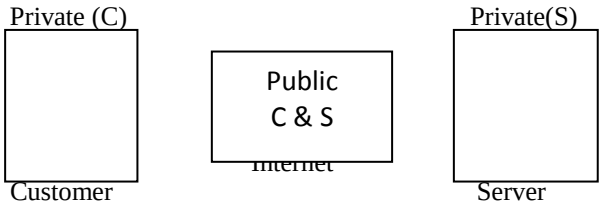
IV. USES

- The Caesar cipher was used to send coded messages to soldiers without the risk of the enemy forces reading the dispatches and discovering what they were planning.
- The Enigma Code was the "Unbreakable" German code used during WW2 that meant they could send message to the armed forces without the Allies reading their messages.
- Sending Secure information over a network like bank account information.

V. ONLINE TRANSACTIONS

- We need Crystography when purchasing goods online because we are sending our Credit Card Information over an unprotected network, the internet.
- So, online security needs to be able to perform two main functions.
  a) Confidentiality, (b) Authentication.

How it Works:



- So, if the customer would like to purchase a product on the internet form a Company like Amazon, they would use the server public key available on the internet to encrypt the data.
- Amazon would then need to use their private key to decrypt the data and be able to read the account details.
- The public & private keys are connected using mathematical sums.
- RSA uses prime numbers to keep the data secure.

VI. CRYPTOGRAPHY IN EVERYDAY LIFE

AUTHENTICATION/DIGITAL SIGNATURES

Authentication and digital signatures are a very important application of public-key cryptography.

Pretty Good Privacy (PGP) is a software package originally developed by Phil Zimmerman that provides encryption and authentication for e-mail and file storage applications. Zimmerman developed his freeware program using existing encryption techniques, and made it available on multiple platforms. It provides message encryption, digital signatures, data compression, and e-mail compatibility.

TIME STAMPING

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

ELECTRONIC MONEY

The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. Identified spending schemes reveal the identity of the customer and are based on more general forms of signature schemes. Anonymous schemes are the electronic analog of cash, while identified schemes are the electronic analog of a debit or credit card. There are also some +hybrid approaches where payments can be anonymous with respect to the merchant but not the bank or anonymous to everyone, but traceable.

Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts, digital signatures can replace handwritten signatures or a credit-card authorizations, and public-key encryption can provide confidentiality.

VII. ADVANTAGES OF CRYPTOGRAPHY

Cryptography is valuable for protecting sensitive data online, especially in a world in which an increasing number of systems are connected and attack by outsiders. It is also a valuable tool for authentication, allowing a user to verify his identity.

Cryptography's chief advantage is as a security tool. Any system connected to the Internet is bound to eventually be attacked by hackers, and it can be extremely difficult to create a system that is inaccessible to outsiders. However, the mathematical formulas involved in encryption are complex enough that even if a hacker manages to steal an encrypted file, he may never be able to break through the code and access the contents. It can protect data even when it is being transferred through a connection that is not secure.

VIII. CONCLUSION

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those

that are well known and well documented because they are also well tested and well studied. In fact, time is the only true test of good cryptography, any cryptographic scheme that stays in use eyar after year is most likely a good one. Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another.

IX. REFERENCES

- Albrecht Beutelspacher, Jorg Schwenk, Klaus – Dieter Wolfenstetter, Moderne Verfahren der Kryptographie, Vieweg, Braunschweig 2001(4)
- G.Brassard, Modern Cryptology
- Oded Goldreich, Modern Cryptography, Probabilistic Proofs and Pseudorandomness.
- Albrecht Beutelspacher: This was one of the first books that I read about codes and codebreaking. A good introduction to some of the technical aspects of cryptography.
- Hugh Sebag – Montefiore: This was published after I had written the Code Book, so I must admit that I have not read it. New interests mean that I have had to focus my reading elsewhere. But, by all accounts, this is excellent book.