International Journal of Advanced Engineering and Management Research
Vol. 2 Issue 4, 2017

www.ijaemr.com ISSN: 2456-3676

A NEW METHOD IN THE CRYPTOGRAPHY

Shirmohammad Tavangari

Department of Computer Engineering, Babol University, Iran

ABSTRACT

This article discusses cryptography as one of the most important network security issues. The algorithm presented here is faster and at the same time more structurally more complex.

The approach outlined in this article for cryptography will be the same Which converts the word into a ASCII code, and then math is done on it, and the new word is encrypted, and the new word will be two's complement and the result will be the message we send to the receiver. Many methods have been published in this regard, but in this article we have tried to introduce a new method with its own characteristics, which has been shown to function in this way than other methods.

Key Words: Security, Network, Algorithm, cryptography, network security

INTRODUCTION

The root of the word "cryptography", derived from the Greek word, means "confidential writing of texts." Cryptography has a long and lively history that dates back thousands of years ago. Encryption specialists distinguish between encryption. The key is to convert a character to a character or bit to bit without having to pay attention to the linguistic contents of that message. The conversion code replaces the word with one word or another. Today codes are not used, although the use of it has a long history. The most successful code ever written was invented by the US Army and during the Second World War in the Pacific.[1]

Encryption is a computer-based information system. The use of cryptography has a long historical history. Before the information age, most users of information encryption were governments, especially military ones. The history of encrypting information dates back to the Roman Empire. Nowadays, most information cryptography methods and models are used in conjunction with computers. The discovery and detection of information stored on a computer normally stored in a computer and lacking any scientific method of encryption can easily be performed without the need for specialized expertise. **Cryptography** or **cryptology** is the

practice and study of techniques for secure communication in the presence of third parties called adversaries[2]. More generally, cryptography is about constructing and analyzing protocol that prevent third parties or the public from reading private messages;[3] various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation [4] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematic, computer science, and electrical engineering. Applications of cryptography include military communications, electronic commerce, ATM cards, and computer passwords.

Definition

Many definitions are encrypted, but the definition I provide is that:

Cryptography is a knowledge that explores ways to hide information during sending, away from unsafe factors.

Methods presented in cryptography

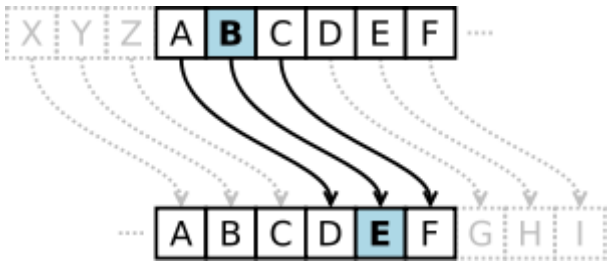
Many methods have been presented and published in this regard, which we are trying to express in two terms.

Quantum cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. Currently used popular public-key encryption and signature schemes can be broken by quantum adversaries. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication (see below for examples). For example, it is impossible to copy data encoded in a quantum state and the very act of reading data encoded in a quantum state changes the state. This is used to detect eavesdropping in quantum key distribution.

Caesar cipher

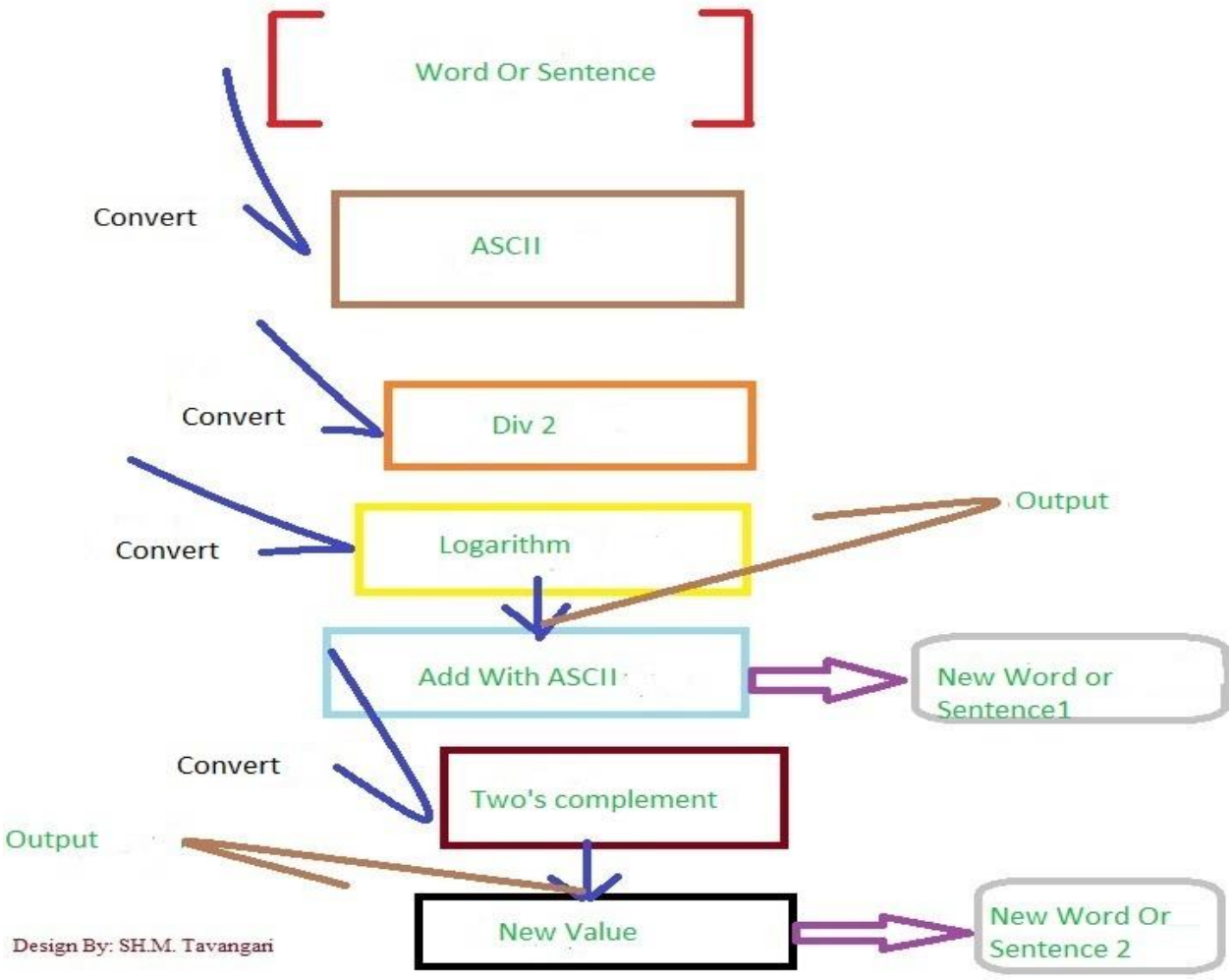
In cryptography, a **Caesar cipher**, also known as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A; E would become B, and so on. The method is named after Julius Caesar who used it in his private correspondence.



The algorithm is presented

In this section, I try to write the way I want to encrypt in step-by-step with the display of images to make the reader more understandable.

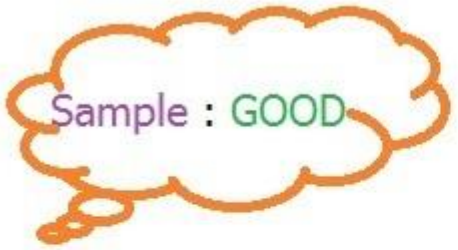
The overall shape of the new method

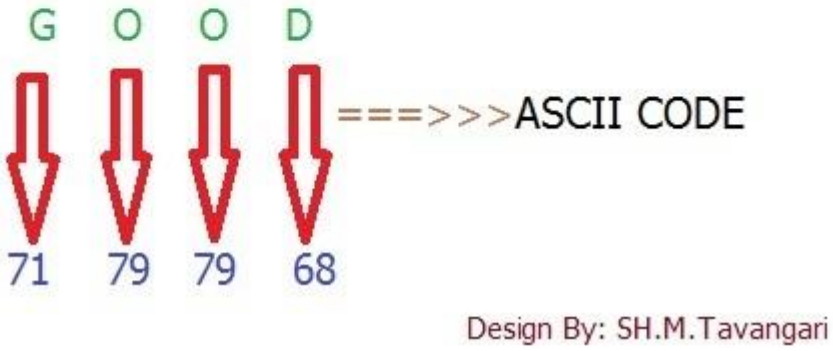


First stage

At this point, we convert the word or sentence into a ASCII code.

Example: Word= **GOOD**





Second stage

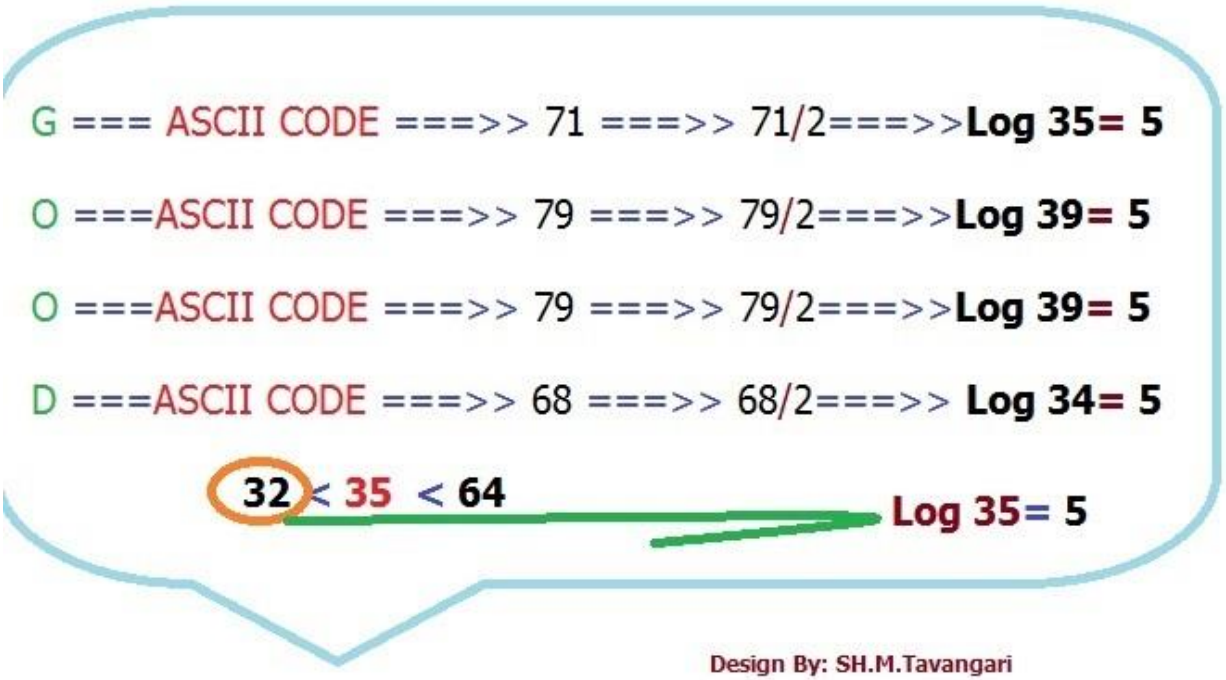
At this point, we divide the obtained ASCII codes into 2 and then obtain the logarithms.

Note 1

The most important point to note here is that if the numbers obtained are decimal, the floor is taken.

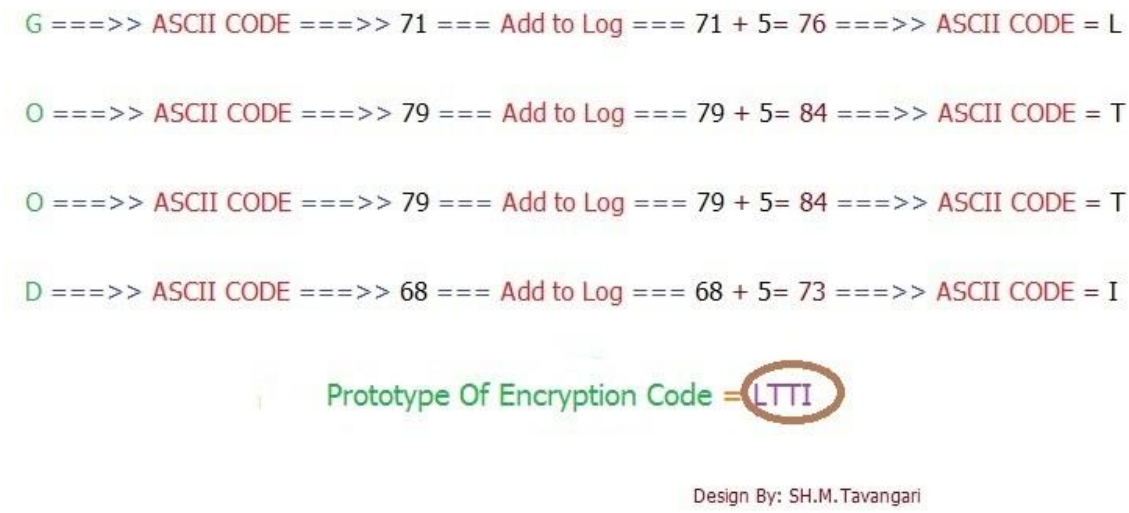
Note 2

The other thing to keep in mind here is that the logarithmic reason is to add a few more data to the encryption code (a deception for those who want to crack the code!)



Third level

In this step, we get the logic number of the original ASCII code and the encrypted prototype is obtained.

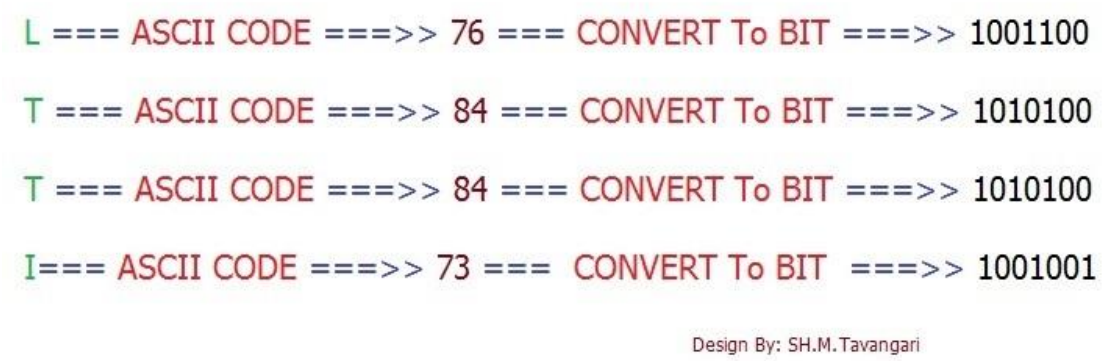


Stage Four

At this point, we convert the encrypted code again to the skype code and then to the bit.

Note

These bits are 7 bits!



Step Five

At this point, the resulting bits are taken two's complement, and then the resulting number is converted into a ASCII code, and the original encryption code is obtained when the recipient's direction is to be sent.

Very important point:

If the ASCII code is converted to two's complement, the result is less than 32 or more than 127, we will automatically write the letter (although it is less likely!).

Conclusion

The algorithm is better in terms of its efficiency and complexity, while the user's confusion is more than the other way to crack the password. The biggest advantage of this method is that the user who wants to crack the code and reach the master password must break the encrypted code after the code is encrypted first and finally it reaches the target, that this algorithm is designed in a layered manner and this It makes the work hard and causes the user's headache.

References

1-Network Security Essential, William Staling, Pearson Publications Ltd

2- Rivest Ronald L. *(1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science.* ***1****. Elsevier.*

3- Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.

4- Rivest Ronald L *.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. Association for Computing Machinery.* ***21*** *(2): 120–126. doi:10.1145/359340.359342*

5- *Cryptography: Theory and Practice*, Third Edition (Discrete Mathematics and Its Applications), 2005, by Douglas R. Stinson, Chapman and Hall/CRC