



Universal Session Based Symmetric Cryptographic Technique to Strengthen the Security

S. Govinda RaoDept. of CSE
TP inst. Of Science & Tech.,
Bobbili, A.P., India**D. Siva Prasad**Dept. of CSE
Rajah RSRKRR College
Bobbili, A.P., India**M. Eswara Rao**Dept. of CSE
TP inst. Of Science & Tech.,
Bobbili, A.P., India

Abstract: In this technical paper a session based symmetric key cryptographic technique, termed as SBSKCT, has been proposed. This proposed technique is very secure and suitable for encryption of large files of any type. SBSKCT considers the plain text as a string with finite no. of binary bits. This input binary string is broken down into blocks of various sizes (of $2k$ order where $k = 3, 4, 5, \dots$). The encrypted binary string is formed by shifting the bit position of each block by a certain values for a certain number of times and from this string cipher text is formed. Combination of values of block length, no. of blocks and no. of iterations generates the session based key for SBSKCT. For decryption the cipher text is considered as binary string. Using the session key information, this binary string is broken down into blocks. The decrypted binary string is formed by shifting the bit position of each block by a certain values for a certain number of times and from this string plain text is reformed. A comparison of SBSKCT with existing and industrially accepted TDES and AES has been done.

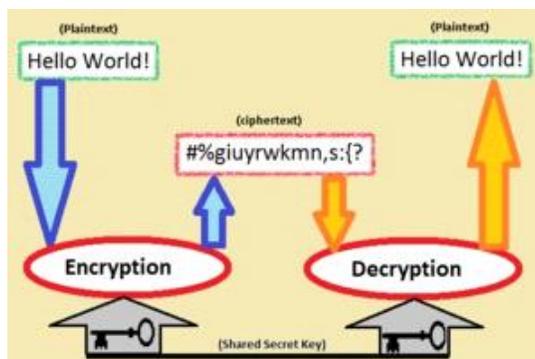
Key words: Cryptographic technique, SBSKCT, TDES, AES, Session key.

I. Introduction

About Network Security

Consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or Denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the Network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involving in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

About Cryptography:



Cryptography (or cryptology; from Greek κρυπτός, "hidden", "secret"; and γράφειν, graph in, "writing", or -λογία, -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries) .

More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-

repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The Originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. 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. These schemes are therefore termed computationally secure; theoretical advances, e. g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but Computationally secure mechanisms.

II. Symmetric key cryptographic algorithm:

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation that goes between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

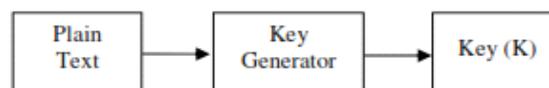
About Proposed System:

A session based symmetric key cryptographic technique, termed as SBSKCT, has been proposed. This proposed technique is very secure and suitable for encryption of large files of any type. SBSKCT considers the plain text as a string with finite no. of binary bits. This input binary string is broken down into blocks of various sizes (of 2^k order where $k = 3, 4, 5, \dots$). The encrypted binary string is formed by shifting the bit position of each block by a certain values for a certain number of times and from this string cipher text is formed. Combination of values of block length, no. of blocks and no. of iterations generates the session based key for SBSKCT. For decryption the cipher text is considered as binary string. Using the session key information, this binary string is broken down into blocks. The decrypted binary string is formed by shifting the bit position of each block by a certain values for a certain number of times and from this string plain text is reformed. A comparison of SBSKCT with existing and industrially accepted TDES and AES has been done.

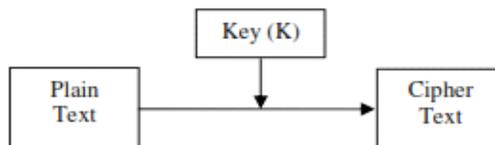
The SBSKCT algorithm consists of three major components:

- Key Generation
- Encryption Mechanism
- Decryption Mechanism

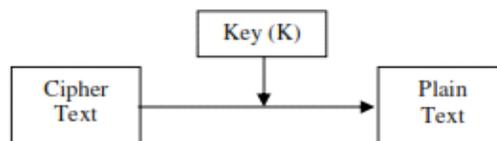
Key Generation:



Encryption Mechanism:



Decryption Mechanism:



Current System:

Industrially accepted TDES & AES private key algorithms are used currently. Even though they are good at security, they're taking much time to both encryption and decryption. These algorithms, encryption & decryption consist of several complex iterations, so it's little bit difficult to implement.

Proposed system:

This algorithm is very easy to implement. It takes less time for both encryption and decryption. we can select number of iteration to be done at sender in encryption process by sender at runtime to enhance the security.

System Scope:

The scope of the system is to give a text file or type message to send by the sender then encryption will be done after key generation, at the receiver side decryption will be done with the same key, finally get the original text.

System Objective:

The objectives of the system are as follows.

- Input text or browse a text file.
- Key generation process at the sender side.
- Several numbers of iterations will be done in different sections of text using session based symmetric key generated.
- Remaining several number of iterations will be done at the receiver side as a decryption process in several sections then finally we get the original text.

System Overview:

The overview of the system is as follows.

- Type text or browse a text file by sender.
- Key generation (matrix) will be done.
- Encryption process (several number of iterations in various sections of text) will be done by using key, generated.
- Decryption process will be done at receiver side then get the original text by receiver..

Functional Requirements:

Inputs:

1. Type text or browse file.

- Outputs:

- At sender side cipher text after perform several number of iterations on the basis of symmetric key.
- At the receiver side get the original text after perform several number of iterations by using the same key.

- Computations:

1. Type text or browse file.
2. Key generation.
3. Encryption (several number of iterations in various sections of the text)
4. Decryption process will be done at receiver side to get the original text.

III. Conclusions

This Cryptographic technique is using a session based symmetric key where which is generated randomly and several iterations will be done in each section in the encryption process as which is very secured so it's difficult to break the cipher text and there is no proper involvement of session key in each iteration so it's enhancing the security. So the proposed system is very secured comparing to the existed industrially accepted AES and RSA.

References

- [1] M. Bellare and P. Rogaway, "On the construction of variable length input Ciphers", in Proceedings of Fast Software Encryption. LNCS, vol. 1636, pp. 231–244. Springer, Heidelberg, 1999.
- [2] S.Patel, Z.Ramzan and G.Sundaram, "Efficient constructions of variable-input-length block ciphers", in Proceedings of Selected Areas in Cryptography 2004. LNCS, vol. 3357. Springer, Heidelberg, 2004.
- [3] J.K. Mandal, P.K. Jha, "Encryption through Cascaded Arithmetic Operation on Pair of Bits and Key Rotation (CAOPBKR)", National Conference of Recent Trends in Intelligent Computing (RTIC-06), Kalyani Government Engineering College, Kalyani, Nadia, India, 17-19 November 2006.