PalArch's Journal of Archaeology of Egypt / Egyptology

TOWARDS DATA CRYPTOGRAPHY OPTIMIZER COLLABORATIVE AUTOLYSIS BIT GENERATOR

Parvesh Kumar[1], Dr. K.P. Yadav[2]

[1]Phd Scholar Himalayan University
[2]Director Academic & research IIMT College of engineering (UP).

Parvesh Kumar[1], Dr. K.P. Yadav[2], TOWARDS DATA CRYPTOGRAPHY OPTIMIZER COLLABORATIVE AUTOLYSIS BIT GENERATOR,-- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(16), 132-136. ISSN 1567-214x

Keywords: Cryptography, Autolysis, Optimization, Encryption.

ABSTRACT

Research technique computer technique, e-commerce application, social network and all other organization huge amount of data uses daily. And everyone uses a computer or mobile device and other component also needs to understand how to keep their computer, system and protect data secure. Secure computer system does not allow data to be disclosed to anyone who is not authorized to access it. So to protect data several encryption techniques are used DES, AES, and RSA. The billions GB of data are send or received from one network machine to other network machine so it is very necessary to protect data from the unauthorized access. The security protection is very critical issues in the software industry various types of algorithm table are used. Now present most of the tools support encryption or decryption method using one table (DES, AES, and RSA) and others.

In the research we observe present world many types of tools uses to protect data and support various algorithm method and tables to protect the data and create a layer, dual layer and multi-layer to protect the data but there is various gaps between the data security. Hackers use various gaps method to decrypt the data.

In this research we tried to found various gaps in data security, we analyze security gaps on various tools several of tools use separate algorithm methods to encrypt the data and many protection layers create to secure data.

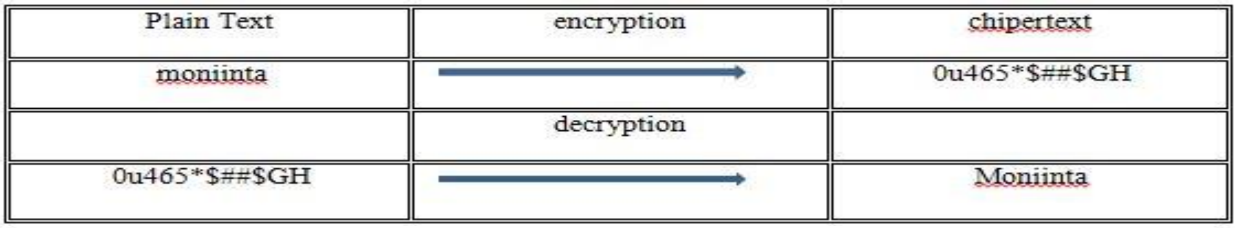
In research "Data Cryptography Optimizer Collaborative Autolysis bit Generator" method created and tried to fill the gaps between security layers, Data cryptography optimizer tools use table encrypted method for encrypt data and second table encrypted method for decrypt data files, here we use two table method for data encryption and decryption.

Introduction

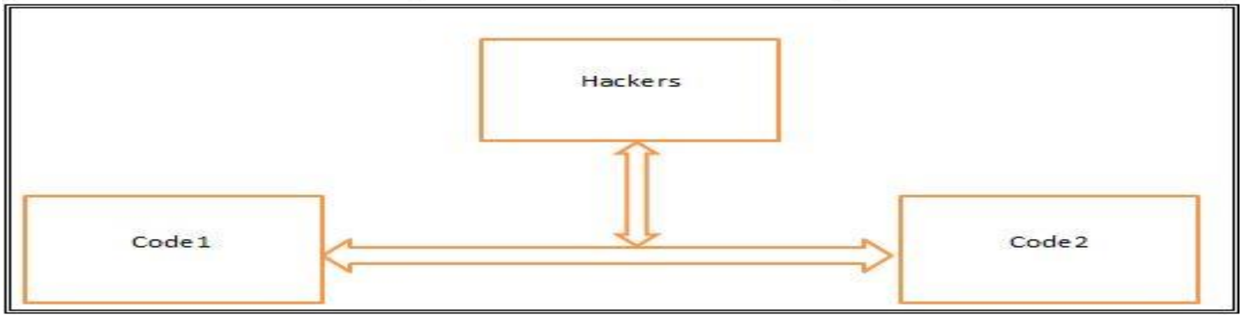
NEED FOR THE STUDY

A research study shown that Cryptography is method of securing data and files through use of codes so that only authorized person can understand it and process it for encryption and decryption. Preventing unauthorized access to data. Cryptography techniques which are used to protect data are obtained from mathematical concepts and a set of rule based security calculations. Cryptography is the study of protect communications from outside sources. Encryption algorithms take the real data (plaintext) and converts it into (chiper text) coded.

In this research we have deeply studies about cryptography and find out the gaps between data security. Here in figure we have shown the encryption and decryption process.



Plain Text	encryption	chipertext
moniinta	→	0u465*$##$GH
	decryption	
0u465*$##$GH	→	Moniinta



IMPORTANCE ON ENCRYPTED DATA

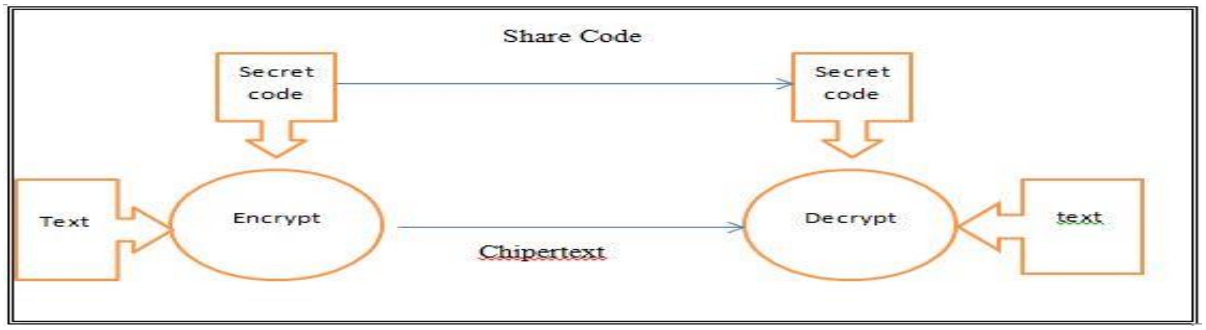
Encryption plays an important role in network life to secure data .
Encryption encodes the data files.
Encryption verifies the origin of a data.
The contents of a data have not been changed since it was sent.
Encryption prevents senders from denying they sent the encrypted data.

BENEFITS OF ENCRYPTED DATA

The primary purpose of encryption is to protect the data interface and stored on computer systems or transmitted over the internet or any other computer network. Encryption is often driven by the need to meet compliance regulations. A number of organizations and other symbolic recommend or require sensitive data to be encrypted in order to prevent unauthorized from intruders.

COLLECTION SURVEY DATA

We also examine the security aspects and processes involved in the design and implementation of most widely used symmetric encryption algorithms.
Data Encryption Standard (DES)
Triple Data Encryption Standard (3DES)
Advanced Encryption Standard (AES)
Hybrid Cubes Encryption Algorithm (HCSEA)



MIDDLE GAPS IN SECURE DATA

The number of cyber-attacks increase day to day. In order to do so we need to know where their weaknesses are, before implementing measures to plug those gaps.

During the webinar, we have observed the several gaps in cyber security that organizations face.

NON UNDERSTANDABLE

On the network increase in frequency and complexity of cyber incidents in the organizations cannot afford to be unknown for next. Organizations must test their protection before a breach occurs, and they to respond when required and captured.

THREAT WITHOUT KNOWLEDGE

organizations should know what the threats. Should known the intruders, keeping abreast of the latest developments, organizations and can also get from the unknown web to know where threats rise.

WEAK DETAILS

Intruders may have infiltrated an organization’s network and are just waiting for the right opportunity to attacks. It is recommended that organizations conduct active threat hunting to intercept these attempts, and stop attacks before they happen. Active threat can be done if proper monitoring systems are in place.

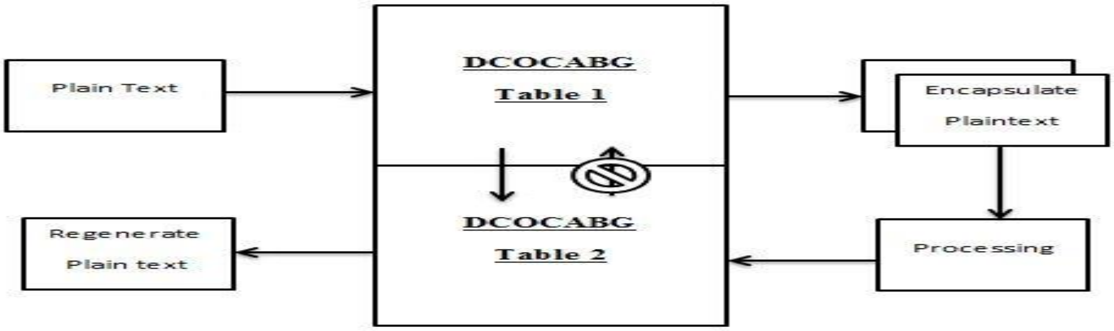
METHODOLOGY

The **Data Cryptography Optimizer Collaborative Autolysis Bit Generator(DCOCABG)** is one type off tools that protect encryption and decryption using dual separate methods. In middle of two byte code table used for processing your text and enroll up into new byte gen code while as in decryption processing another byte code table generate and used for decrypt.

The second decrypt table match the byte code decryption with encryption table. So generation new table have only to the receiver so sender don’t know the decryption code

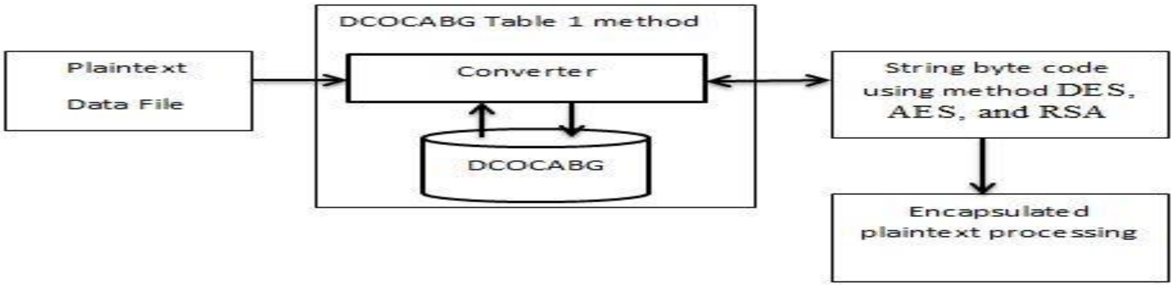
Flow Chart

Data Cryptography Optimizer Collaborative Autolysis Bit Generator



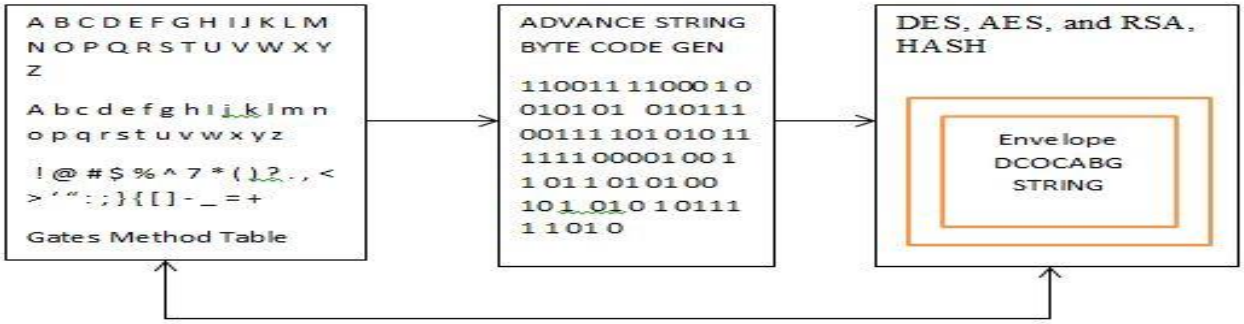
Data Cryptography Optimizer Collaborative Autolysis Bit Generator(DCOCABG) table 1 encode the plain text and convert un-meaningful(UM) byte code, the converted UM code envelope using the DCOCABG method table

DCOCABG TABLE 1 METHOD



DCOCABG convert plain text into AES, DES, RSA code , the coded string code reprocess and envelop using Data Cryptography Optimizer Collaborative Autolysis Bit Generator(DCOCABG) tables, Generation code reprocess it and encapsulate it for processing.

DCOCABG METHOD 1



Conclusion

AES has a very simple key schedule and simple encryption operations. Many (DCOCABG) attacks are based upon the simplicity of this key schedule and it is possible that one day an hackers will be created to break (DCOCABG) encryption.

Bibliography / References

Diffie, W., and Hellman, M. E., “New Directions in Cryptography,” *IEEE Trans. Inf. Theory,* vol. IT22, Nov. 1976, pp. 644–654

Ribeiro, C., A. Zuquete and P. Ferreira (2001a). SPL: An *access control language for security policies with complex constraints*. In Proceedings of the Network and Distributed System Security Symposium (NDSS’01), San Diego, California, February 2001

Ryan, V., S. Seligman and R. Lee (1999), *Schema for Representing Java (tm) Objects* in an LDAP Directory, RFC 2713, October 1999.

Sandhu, R., D. Ferraiolo and R. Kuhn (2000). *The NIST Model for Role-Based Access Control: Towards A Unified Standard*. In Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, pp. 47-61, 26-28 July 2000

Steen, M. W. A. and J. Derrick (1999). *Formalising ODP Enterprise Policies*. In Proceedings of the 3rd International Enterprise Distributed Object Computing Conference (EDOC '99), University of Mannheim, Germany, IEEE Publishing, September 1999

Strassner, J., E. Ellesson, B. Moore and R. Moats (2002), Policy Core LDAP Schema, IETF *Internet draft work in progress*, available from http://www.ietf.org, January 2002.

Sun (1999c) Microsystems, Inc, Remote Method Invocation Specification, available *from http://java.sun.com/docs/index.html*,September1999.Sun (1999d) Microsystems, Inc., Java Naming and DirectoryInterface,ApplicationProgrammingInterface, available from *http://java.sun.com/docs/index.html*, July 1999.