International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 574-576
e-ISSN:2278-621X

UNIVERSAL STRENGTH ASSESSMENT OF ENCRYPTION ALGORITHM (USAEA)

Ruben Anthony D'Costa[1], Noah JonesGomindes[2] & Mr.Santhosh B[3]

Abstract: In this paper we introduce a new method for assessment of encryption algorithms strength – USAEA , which does not require the knowledge of working of the algorithm. Using this it is possible to determine strength of any encryption algorithm. Here the concept of correlation coefficient is applied to the plaintext and cipher text pairs and its strength is determined.
Key words: DES, Encryption, cipher text, plain text, correlation, Karl pearsons coefficient of correlation.

1. INTRODUCTION

Encryption is the process of converting a plaintext message into acipher text which then can be decoded back into its normal formof original message. An encryption algorithm along with the support of a key is used in the encryption and decryption of information/data. There are many types of data encryptions which provide the basis of network security. Encryption depends on block or stream ciphers.

1.1 Asymmetric encryption algorithm.

A modern and new branch of cryptography. also called the open -key cryptography in which the algorithms implements a pair of keys (a public key and a private key) and use an alternative segment of the pair for different steps of the algorithm.

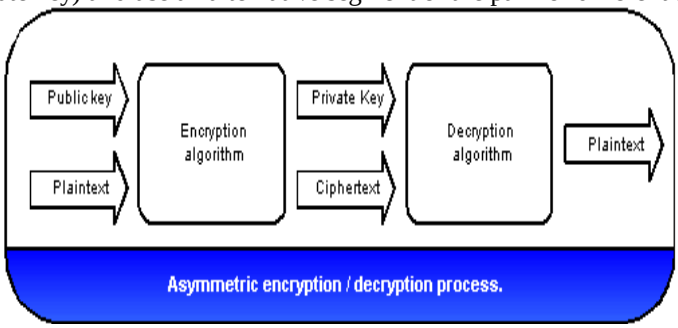

Fig 1.Asymmetric encryption/decryption process.

1.2 Symmetric encryption algorithm.

The encryption key and the decryption key are connected to each other internally and may even match.

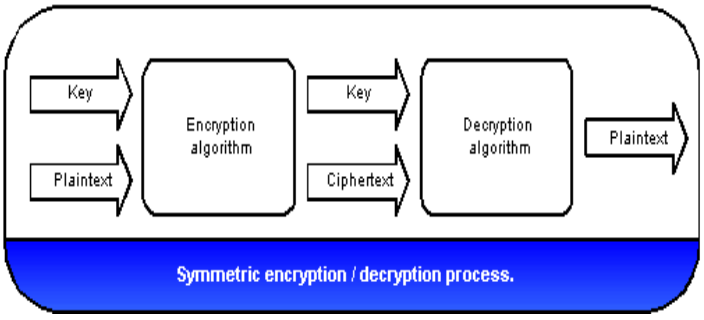

Fig 2 Symmetric encryption/decryption process.

[1] Department of MCA, St. Aloysius Institute of Management & Information Technology, Beeri, Kotekar, Mangalore, 575022, Karnataka, India
[2] Department of MCA, St. Aloysius Institute of Management & Information Technology, Beeri, Kotekar, Mangalore, 575022, Karnataka, India
[3] Department of MCA, St. Aloysius Institute of Management & Information Technology, Beeri, Kotekar, Mangalore, 575022, Karnataka, India

2. LITRATURE SURVEY

All Encryption algorithms are mostly evaluated by how much effort of (time, processing power) is required to crack them based under a number of assumptions. These incorporate the content of encrypted text available, regardless of whether the basic algorithm is known to the attacker, and whether encrypted text is corresponding with plaintext. In most of the cases, it is assumed that the attacker have access to all of these.

And normally, attacks can be made more time consuming by increasing the key length.Commonly, it is easy to increase key length as the attacker's power grows (due to faster computers); Maybe, if the encryption is done in hardware this is not feasible. Even if this is possible, increasing to build the key length requires that all users obtain new keys. The difficulties of key management are as shown below.

Because if proper time given a key will be found, the long term viability of an encryption requires that the key be changed periodically when time comes. The stronger the encryption, the less every now and again the keys must be changed to prevent attack form the hacker.

In general terms, because of an increasing computing power, it is safest to assume that a message is secure and not breakable only during a particular "time window" based on the current and projected computing technology. Keeping messages secure for quite a long time period is often sufficient because many messages are only important for a certain length of time. If repeatedly security is required, there are theoretically unbreakable encryptions based on "one time keys" that are very secure but have enormous key management issues associated with them.

3. PROPOSED SYSTEM

The Proposed system (USAEA) considers correlationcoefficient among plaintext and cipher text pairs to determine its strength. This is a measure of linear relationship between the two variables – that are plain text and cipher text. It points out to the degree of correlation between plain text and cipher text.

It is denoted by 'r'.

Interpretation Of Coefficient Of Correlation

a. A positive value of r indicates positive correlation
b. A negative value of r indicates negative correlation
c. r = +1 means, correlation is perfect positive and the algorithm is very week.
d. r = -1 means, correlation is perfect negativeand the algorithm is very week.
e. r = 0 (or low) means, the variables are non – correlated and the algorithm is very strong.

Karl Pearson's correlation co efficient between two variables (series) X and Y , usually donated by r , is a numerical measure of linear relationship between them and is defined as the ratio of the covariance between X and Y , written as Cov (x, y) to the product of standard deviation of X and Y . Here X represents message digest of Plain text and Y represents message digest of Cipher Text.

Procedure:

Step 1: Generate message digests X of Plain text with step value K and calculate corresponding Cipher text and its message digest Y .

Step 2: Use Karl Pearson's correlation co efficient between two variables – Message Digest of plain texts X and Message Digest of Cipher texts Y .

Step 3: if r =0 means the encryption scheme is very strong.

else If r is near to zero the encryption scheme is strong

else encryption scheme is week.

4. EVALUATION

To test the algorithm standard, most commonly used DES algorithm is considered. A sample test is as follows

Key := 3b3898371520f75e	
Ascii – plaintext	Hexadecimal-cipher text generated
11111111	922fb510c71f436e
11111112	d124ea66d65d7574
11111113	f7b33cbb35f114cc
11111114	b393c26b5c7e4e70
11111115	14609ae46045b0e5

11111116	2bd2c8baf0fb3174
11111117	60c56be2ca053219
11111118	0e54b4a46fda2ba5
11111119	b5529455270cfc99
11111120	532bc74a2c601c34

Here r= -0.479779114507535 and is negatively correlated means lower the values of one variable results in an higher the value of another variable. And the algorithm is for the given key is vulnerable to attacks.

5. CONCLUSION

This algorithm can be used to test any encryption algorithm, compare to the existing algorithm here tester need not understand the working of the encryption algorithm and the method is faster, accurate and efficient. Once the combinations of required plain text and cipher text is produced the time complexity of the algorithm is Big Theta (n^2)

6. REFERENCES

[1] Swarnendu Mukherjee , Debashis Ganguly "A New Generation Cryptographic Technique" International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009 pg no 284-287

[2] Book :S.P Guptha "statistical methods "

[3] Book: Williams stallings "cryptography and network security

[4] Q. Chai and G. Gong, "Differential Cryptanalysis of Two Joint Encryption and Error Correction Schemes," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston, TX, USA, 2011, pp. 1-6.

[5] H. Pang, J. Zhang and K. Mouratidis, "Enhancing access privacy of range retrievals over B^+-trees," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1533-1547, July 2013.