ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Multi-Round SR2C Encryption & Decryption

Jan Mohd Najar[1], Ashish Sharma[2]

M. Tech Student, Dept. of CSE, BIMT, Mehli, Shimla, H.P, India[1]

Assistant Professor, Dept. of CSE, BIMT, Mehli, Shimla, H.P, India[2]

ABSTRACT: Data is the raw form of information stored as columns and rows in our files, network servers and personal computers in a structured and unstructured manner. This may be a wide range of information from personal files and intellectual property to market analytics. However, some of this information isn't intended to leave the system as it is critical and cannot be shared with others. The unauthorized access of such data could lead to numerous problems for the larger enterprises or even the personal home user. Having your bank account details stolen is just as damaging as the system administrator who was just robbed for the client information in their database. However researchers are looking beyond traditional security aspects and are trying to evolve more secure mechanism for data security. In this research paper we propose a multi-round SR2C encryption algorithm, enhancing file and database security by implementing the same to encrypt files and certain sensitive information within the database. The credibility of this algorithm is tested and compared with existing encryption algorithms. The main aim of this kind of encryption is to provide security for student's academic transactional data that is critical, huge and changes and access to this data is frequent.

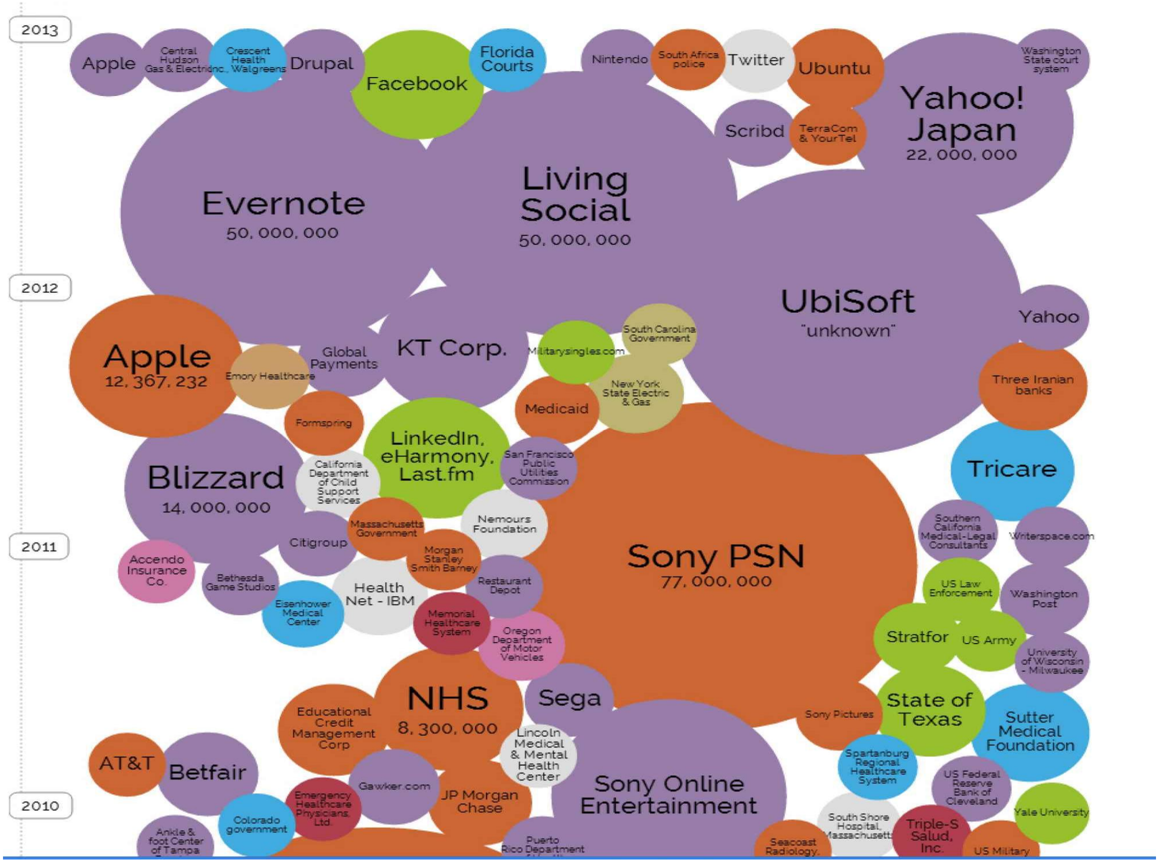
KEYWORDS: Encryption, Decryption, Cipher, Key, Rounds

1. INTRODUCTION

21st century is all about data with every two days now we create as much information as we did from the dawn of civilization up until 2003, something like five Exabyte of data [1][2]. With this much of data around us we have become more vulnerable to data theft and our privacy is at high risk, thus focus behind data security is to ensure privacy while protecting personal or corporate data. There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down your data from software solutions to hardware mechanisms.

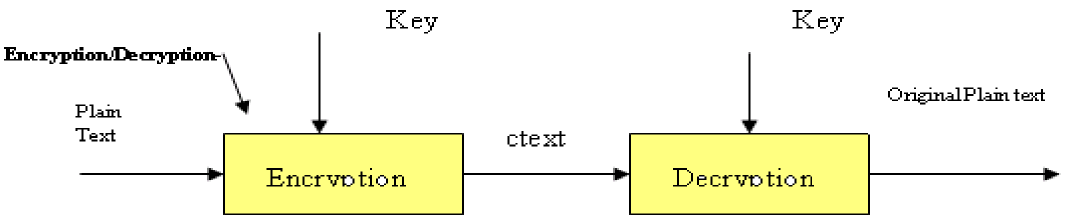
The internet is a giant vault where people store some of their most private information, trusting that the company holding on to it can keep it all safe [12[15]. That's not always the case, as this info graphic of data breaches in recent history reveals viruses, hacks, lost computers, accidental publishing, inside jobs and more have all been sources of major leaks over the last 9 years. The info graphic identifies breaches by amount of information stolen, type of organization that was breached, year of theft, and the sensitivity of information lost or stolen. An intriguing upshot: By showing major breaches over time, the info graphic illustrates how internet use has changed over the past decade [4][5]. AOL had the first major breach in 2004, healthcare providers dominate leaks around 2009, and gaming companies had the major data losses in 2012.

DOI: 10.15680/IJIRCCE.2015. 0309108



1.0 Encryption & Decryption

Data encryption is the act of altering electronic information into an unreadable state by using algorithms or ciphers so as to make it secure. Originally, data encryption was used for passing the government and military sensitive information electronically from one place to another. Over time as the public has begun to enter and transmit personal, sensitive information over the internet, data encryption has become more widespread. The procedure of hiding a communication in such a method/s as to conceal its matter is encryption. An encrypted data is cipher-text [1]. The procedure of whirling cipher-text back into plaintext is decryption. The below mentioned block diagram shows how encryption and decryption are carried out using a key which remain common in both the procedures.



Encryption Procedure

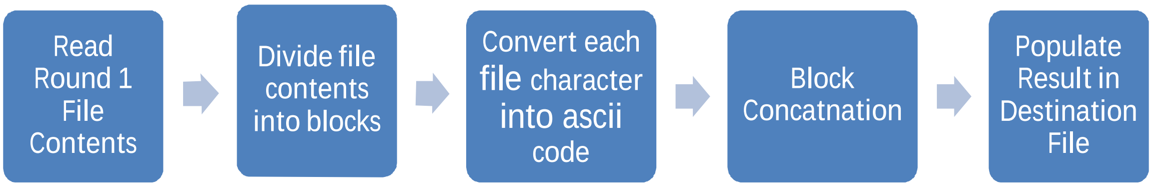
Encryption is used for protected transportations and data storage, mainly for verification of identifications and the communication of subtle data. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

II. PROPOSED ALGORITHM

The proposed research aims to perform an encryption technique for an examination data related students which could include the registration details, photograph and marks of a student in a faster and in a memory efficient manner. In this regard below is graphical description of Encryption/Decryption algorithm, this is multi round algorithm with each round converting the source data into crypt text and deleting source data.

A. MULTI-ROUND ENCRYPTION

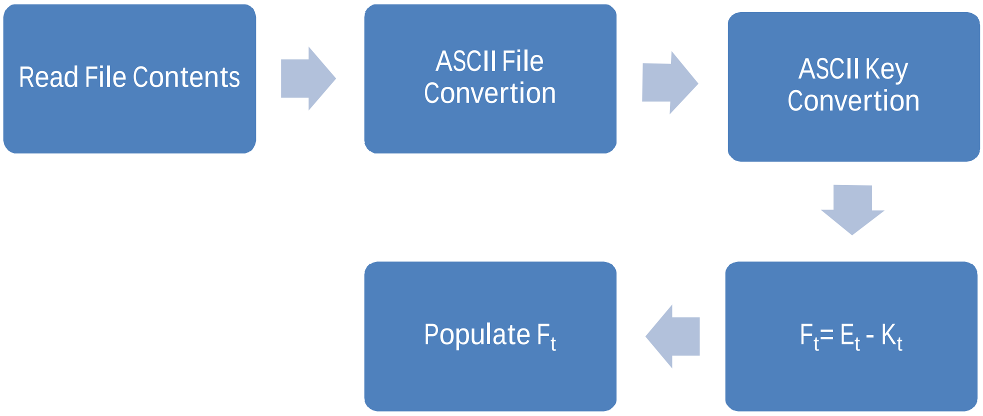
A.1. ENCRYPTION ROUND 1: SHUFFLE


Read Round 1 File Contents
Divide file contents into blocks
Convert each file character into ascii code
Block Concatination
Populate Result in Destination File

Steps Involved:

1. Read the contents of file to be encrypted
2. Divide the File Contents into blocks and Store each block in different linear structures.
3. Convert each key character into its ascii and and put the value in K_t
4. Concatenate characters between blocks
5. Write F_t into the Destination File and Delete the Soruce File

A.2. ENCRYPTION ROUND 2



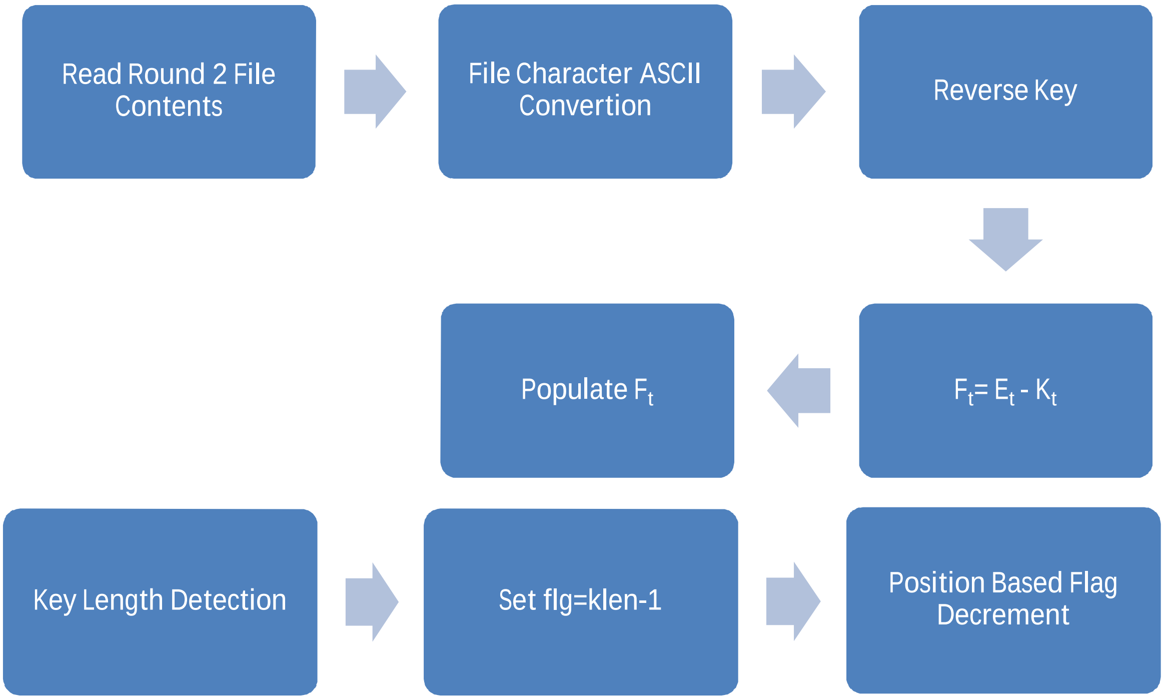
Steps Involved:

1. Read the contents of file created by round 1.
2. Convert each file character into its ascii code and store the value in E_t
3. Convert each key character into its ascii and and put the value in K_t

DOI: 10.15680/IJIRCCE.2015. 0309108

4. Perform a Random Mathematical Operation
5. Write F_t into the Destination File and Delete the Soruce File

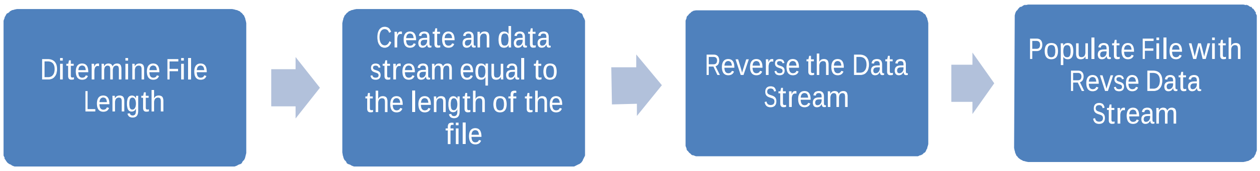
A.3. ENCRYPTION ROUND 3: REVERSE KEY


Read Round 2 File Contents
File Character ASCII Convertion
Reverse Key
F_t= E_t - K_t
Populate F_t
Key Length Detection
Set flg=klen-1
Position Based Flag Decrement

Steps Involved:

1. Read the contents of file created by round 2
2. Convert each file character into its ascii code and store the value in E_t
3. Reverse the key* Convert each key character into its ascii and and put the value in K_t
4. Perform a random Mathematical Operation
5. Write F_t into the Destination File and Delete the Soruce File
6. FInd the length of the key and store the value in K_{len}
7. Use the key from the flag position in the algorithm and decrement the flag after each iteration

A.4. ENCRYPTION ROUND 4: REVERSING FILE CONTENTS

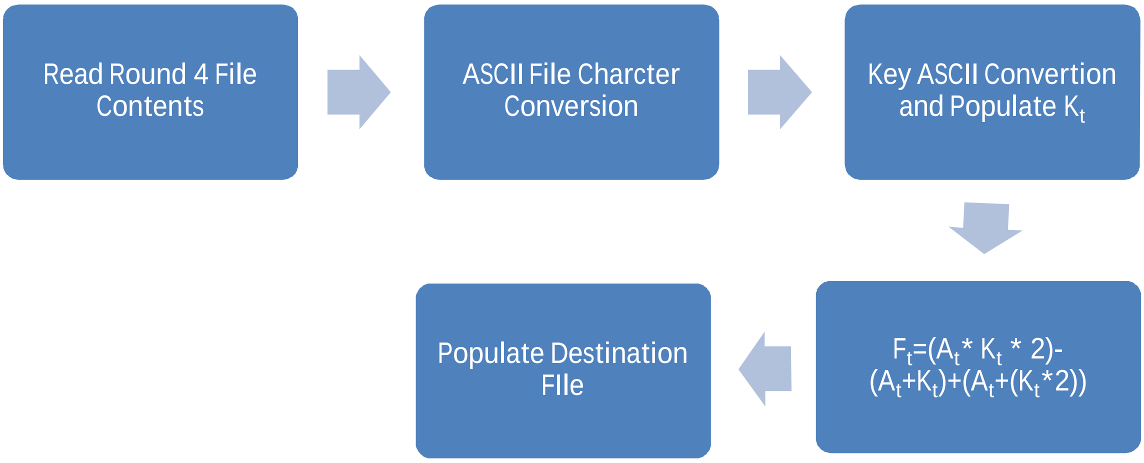

Ditermine File Length
Create an data stream equal to the length of the file
Reverse the Data Stream
Populate File with Revse Data Stream

Steps Involved:

1. Get the length of the file created by previous round and store the value in F_{len}
2. Create a Dynamic Array Based on File Content Length

3. Write array contents into the Destination File in reverse order and Delete the Soruce File.

A.5. ENCRYPTION ROUND 5: COMPLEX EQUATION


Read Round 4 File Contents
ASCII File Charcter Conversion
Key ASCII Convertion and Populate K_t
$F_t=(A_t* K_t * 2)-(A_t+K_t)+(A_t+(K_t*2))$
Populate Destination FIle

Steps Involved:

1. Read the contents of file created by round 4
2. Convert each file character into its ascii code and store the value in A_t
3. Convert each key character into its asciiand and put the value in Kt
4. Perform a Random and Complex Mathematical Operation.
5. Write F_t into the destination file and delete the source file

B. *Encryption Decryption Process for Data in Files*

B.1 Encryption Process

a. the source file is a.doc
b. a.doc is encrypted and saved as en1_a.txt with a.doc is deleted
c. en1_a.txt is encrypted and saved as en2_a.txt with en1_a.txt is deleted
d. en2_a.txt is encrypted and saved as en3_a.txt with en2_a.txt is deleted
e. en3_a.txt is encrypted and saved as en4_a.txt with en3_a.txt is deleted
f. en4_a.txt is encrypted and saved as en5_a.txt with en4_a.txt is deleted

In each level source file is encrypted and deleted, each level adds to complexity. At the time of decryption user has to provide key & file format e.g. .doc, .pdf, .exe etc. This adds to the complexity of the algorithm. The server does not retain key nor source file, rather all intermediate files are also deleted.

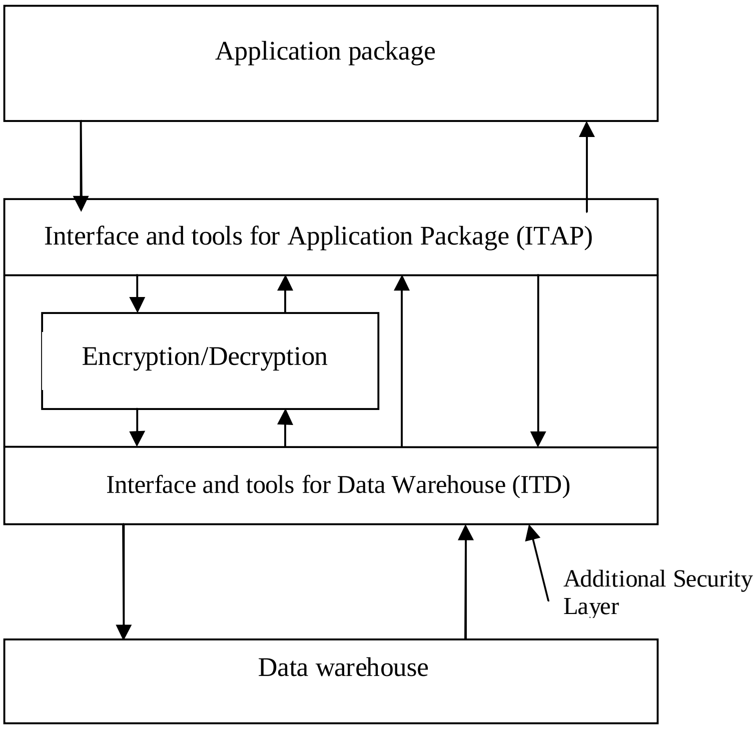
B.2 Decryption Process

a) User is asked for source file, format, & Key
b) En5_a.txt is decrypted and saved as dc5_a.txt, with en5_a.txt is not deleted and is treated as source file for all decryptions process.
c) dc5_a.txt is decrypted and saved as dc4_a.txt with dc5_a.txt is deleted
d) dc4_a.txt is decrypted and saved as dc3_a.txt with dc4_a.txt is deleted
e) dc3_a.txt is decrypted and saved as dc2_a.txt with dc3_a.txt is deleted
f) dc2_a.txt is decrypted and saved as a.txt with dc2_a.txt is deleted
g) As soon as file is decrypted, it is downloaded and deleted.
h) Source file is not retained with the server.

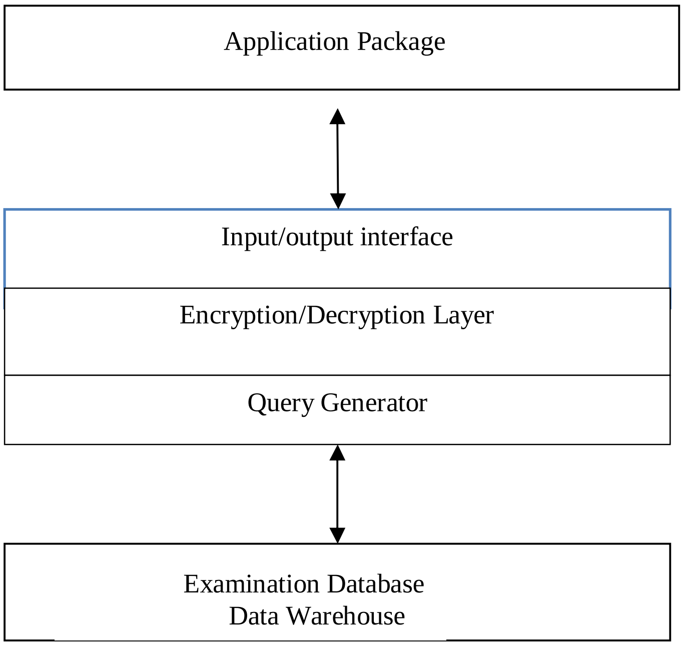
C. *Encryption Decryption Process for Data in Databases*

The Implementation part of the system pertains to the layer of software installed between the Application Package and Data Warehouse [1][14][16]. The interface between the Application Package and Encryption/Decryption software is such that Application package interacts with the software as if it is interacting with the database itself, and same is the case between the Encryption/Decryption software and Database[9][10][11], however they have used one of the following algorithms

- DES
- Blowfish
- Triple DES


Application package
Interface and tools for Application Package (ITAP)
Encryption/Decryption
Interface and tools for Data Warehouse (ITD)
Additional Security Layer
Data warehouse

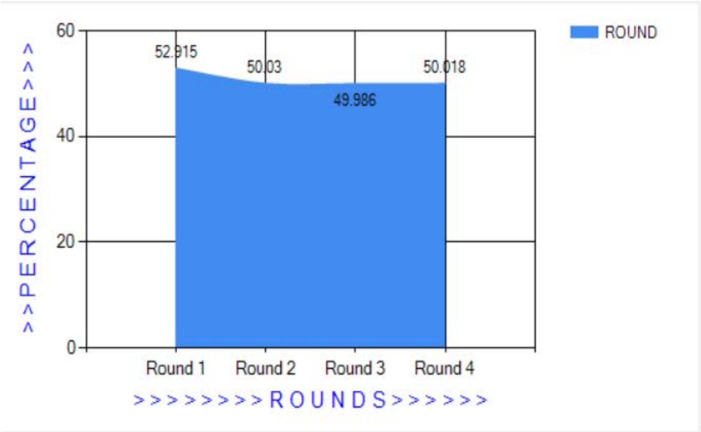
The architecture proposed by Mehraj, Majid & Muheet [1] is implemented with modification and algorithms in university examination system as diagrammatically represented below.



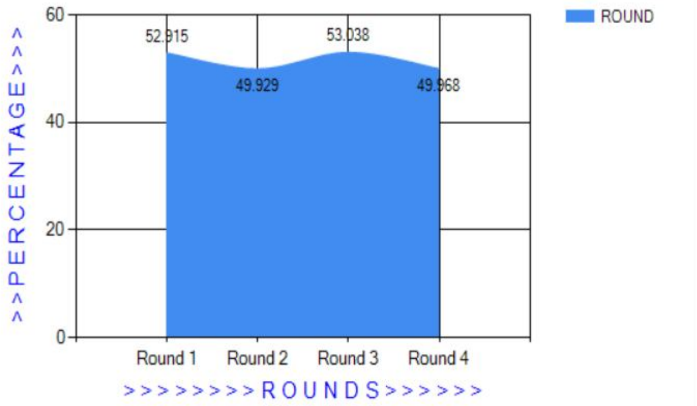
In order to safe guard sensitive information, extra layers are added to encrypt and decrypt information. Once the user enters say marks, these marks are collected and forwarded to encryption/decryption layer [5][6][8]. Encryption/Decryption layer encrypts/decrypts based on key as the case may be. Query generator is used to save and retrieve information from the database [1] and adds layer of security for sensitive information.

1V. CRYPT-ANALYTICS FOR SR2C ALGORITHM

The crypt analytics for the said algorithm is carried out by comparing the encrypted files at various rounds. Two main techniques were carried out as comparative and cumulative and it was observed that at each time 51.6% average bit manipulation took place at each round. This Crypt analytics gives us an insight of the variations that have taken place at bit level which could be only reversed at the time of decryption. The byte streams also convey the amount of security present in information transformation resulting in a byte pattern which is not readable. The analysis was carried out on above dataset in a Dot Net Platform and the graphs plotted comparative and cumulative encryption comparison are shown below in Graph 1 and 2 respectively.



Graph 1: Comparative Crypt Analytics for SR2C Encryption



Graph 2: Cumulative Crypt Analytics for SR2C Encryption

V. COMPARISION WITH OTHER ENCRYPTION ALGORITHMS

The following comparison was carried out between various encryption algorithms and SR2C based on Key Length, Block Size, Rounds, Encryption Speed, Security Level, Attacks Found, Data Build-up [7][13] in structured and unstructured format and cost and following results were recorded in the Table shown below.

Parameter Type	**DES**	**AES**	**3DES**	**RSA**	**BLOWFISSH**	**SR2C**
Key Length	64 (56 Usable)	128,192,256	168,112	Depends on Bits in Module	32-448	Variable Key Length
Block Size	64	18	64	Variable Block Size	64	Variable Block Size
Rounds	16	10,12,14	48	1	16	Need Based Multi Round 1 to n
Encryption Speed	Very Slow	Faster	Very Slow	Average	Faster	Variable
Level of Security	Secure	Secure	Secure	Good Secure	Highly Secure	Secure
Attack Found	Differential Attack Related Key Attack	Correlation Attack, Timing Attack	Improved Related Key Boomerang Attack	Doubling Attack	Linear Attack	No Impact of these Attacks. (Tried on Simulators)
Data Build-Up	Low	Low	Low	Moderate	Moderate	High
Cost	Less	Little More	Less	More	Most	Least

VI. CONCLUSION

With massive infusion of data, information is vulnerable and at risk of being stolen. Users cannot rely upon traditional means of security and have to integrate multiple solutions in order to increase over-all strength of the system. From the proposed work in this paper it is observed that that the strength and versatility of the any encryption algorithm depends upon the key management, type of cryptography used, number of keys and rounds, Key Length and Data to be encrypted. Longer the key length and data length more will be the workload. In this research paper we proposed multidisciplinary encryption solution, algorithm was developed using open source technology and was tested on two formats i.e. files and databases. While traditional encryption techniques have worked well with files however applicability of encryption techniques have grown substantially for other applications including cloud, mobile services , databases etc. Accordingly in this research paper we have successfully tested encryption technique and proposed modified applicability of secure database system based on encryption technique.

The proposed SR2C algorithm is mostly implemented for transaction data where we need custom based rounds and keys for efficient and fast encryption. In general we have concluded that using very small data sequence and key lengths are not good to use. The keys having more number of bits requires more encryption computation time and vice versa. We believe that encryption will drastically change its direction- from being traditional key based to multi discipline thing; future will be to create new algorithm architectures those will be developed on open source technologies, that cost less, and that provide a higher level of assurance to the enterprise user as well as to common man

REFRENCES

1. Kale, Karbhari Viswanath,” Advances in Computer Vision and Information Technology”, IK International Pvt Ltd, 2008 [Book Chapter]
2. Denning, D. E., Denning, P. J., Schwartz, M.D. 1979. The tracker: a threat to statistical database security. ACM Trans. Database Syst. 4(1): 76-96
3. Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).
4. D.Ferraiolo, R.Chandramouli, R.Kuhn “Role Based Access Control”, Artech House, 2003
5. S.Oliveira, O. Zaiane “Privacy Preserving Frequent Itemset Mining”, Proc. IEEE ICDM Workshop, 2002
6. MaqboolRao, Nouman, et al. "Distributed Data Warehouse Architecture: An Efficient Priority Allocation Mechanism for Query Formulation."
7. Dr. Prerna Mahajan & Abhishek Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security” Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013
8. Butt, Muheet Ahmed. "Implementing ICT Practices of Effective Tourism Management: A Case Study." Journal of Global Research in Computer Science4.4 (2013): 192-194.
9. Zaman, Majid, and Muheet Ahmed Butt. "Warehouse Creator: A Generic Enterprise Solution." International Journal of Engineering Science (IJES) 2.11.
10. Butt, Muheet Ahmed. "COGNITIVE RADIO NETWORK: SECURITY ENHANCEMENTS." Journal of Global Research in Computer Science 4.2 (2013): 36-41.
11. Butt, M. A., and M. Zaman. "Data Quality Tools for Data Warehousing: Enterprise Case Study." IOSR Journal of Engineering 3.1 (2013): 75-76.
12. Butt, Er Muheet Ahmed, and Er Majid Zaman. "Data Quality Tools for Data Warehousing: Enterprise Case Study."
13. Mr. Gurjeevan Singh, Ashwani Singla, K S Sandha, “Cryptography Algorithm Comparison for Security Enhancement In Wireless Intrusion Detection System”, International Journal Of Multidisciplinary Research Vol.1 Issue 4, August 2011, Issn 2231 5780
14. Zaman, Majid, S. MK Quadri, and Muheet Ahmed Butt. "Generic Search Optimization for Heterogeneous Data Sources." International Journal of Computer Applications 44.5 (2012): 14-17.
15. Zaman, Majid, and Muheet Ahmed Butt. "Enterprise Data Backup & Recovery: A Generic Approach." International Organization of Scientific Research Journal of Engineering (IOSRJEN) (2013): 2278-4721.
16. Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).