International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-7, Issue-6)

Research Article

June 2017

Encryption of Data Using Radix-64 and Symmetric Key Encryption

Madem Nageswara Rao*
M.Tech (CSE) Student, Sri Vasavi Engineering College
Tadepalligudem, W.G.Dt, Andhra Pradesh, India

M R Raja Ramesh
Associate Professor, Sri Vasavi Engineering College
Tadepalligudem, W.G.Dt, Andhra Pradesh, India

DOI: 10.23956/ijarcsse/V7I6/0239

Abstract— Nowadays providing security for data in a personal computer has become the biggest problem, due to availability of high capability cracking tools in the market. In general people will store their data in hard disks and removable disks. Even if they are password protected they can be easily cracked. So, providing security for hard disks and removable disks has become cumbersome. Existing system uses TrueCrypt technique for encrypting text files data. But, using TrueCrypt is not secure as it may contains so many unfixed security issues like it data may loses and includes garbage after decrypt. So, that we are proposing another new technique Radix-64 with symmetric key encryption for encrypting text files. The Radix64 is also called as Base64, is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation and symmetric key encryption is a technique for encrypting data by using a single key.

Keywords— Encryption, Decryption, TrueCrypt, Radix-64, Base64, Symmetric Key Encryption

I. INTRODUCTION

The TrueCrypt is a special type of software for encrypting and decrypting of files in a personal computer. But it contains so many unfixed security issues. TrueCrypt independent audit conducted by iSEC Partners Company showed in total 11 threats to users' information security in its code. 4 of which have a middle level of threat, other 4 – a low level, the others are difficult to classify in principle through their insignificance. Hence Microsoft terminates the support to the TrueCrypt. Radix64 or base64 is an encoding method that converts binary data into ASCII text and vice versa. It is commonly used to send non-text files via the Internet's e-mail system.Base64 divides each set of three bytes of the original data into four 6-bit units, which it represents as four 8-bit ASCII characters. This typically increases the original file by about a third. Base64 or Radix64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as cipher text, while unencrypted data is called plaintext. Symmetric key cryptography is useful if you want to encrypt files on your computer, and you intend to decrypt them yourself.

Cipher text = encrypt (plain text, key)
Plain text = decrypt (cipher text, key)

Advantages of Symmetric Key algorithm:

- When it uses a secure algorithm, symmetric key encryption can be extremely secure.
- Encrypting and decrypting symmetric key data is relatively easy to do, giving you very good reading and writing performance.

Advantages of Radix-64 algorithm:

Implementations may have some constraints on the alphabet used for representing some bit patterns. This notably concerns the last two characters used in the index table for index 62 and 63, and the character used for padding which may be mandatory in some protocols, or removed in others.

II. PROBLEM DEFINITION AND PROPOSED SYSTM

In general people will store their data in hard disks and removable disks. Even if they are password protected they can be easily cracked. So, providing security for hard disks and removable disks has become cumbersome. We are proposing a new technique called RadiCrypt. That is Radix-64 with symmetric key encryption for encrypting text files. The Radix64 is also called as Base64, is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation and symmetric key encryption is a technique for encrypting data by using a single key.

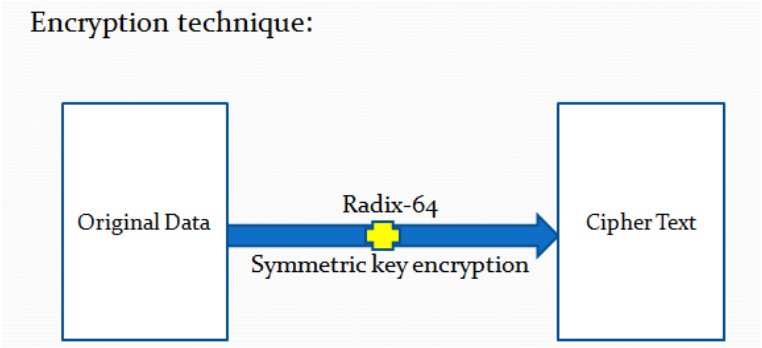
Advantages of Proposed System:

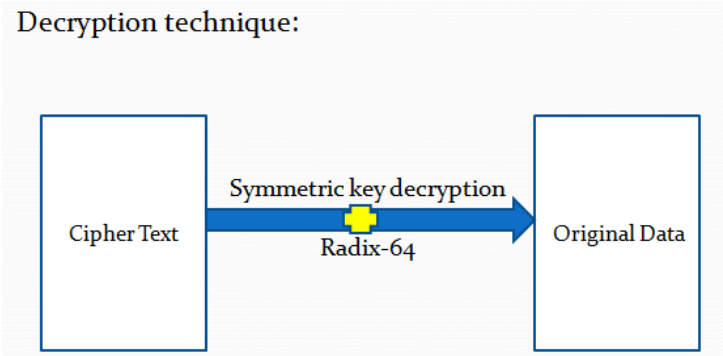
It is easy to implement and provides more security compare to others software's. There are no combination algorithms are present in the Market. So we introduced a new technique called RadiCrypt. It is a combination of Radix-64 and Symmetric key encryption.

III. METHODOLOGY

Symmetric key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations share this property but differ in the symbols chosen for the last two values.

System Design:





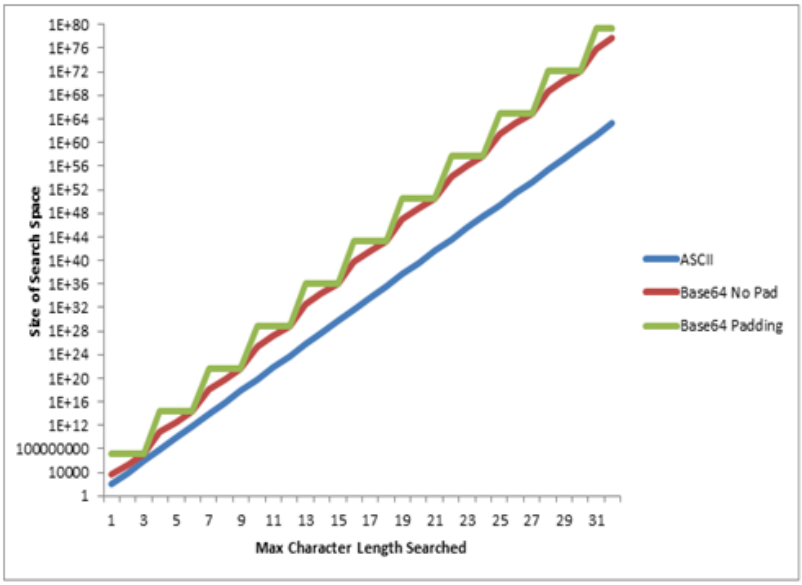
Algorithm: Encryption

Step 1: Start
Step 2: Select text file name for encryption
Step 3: Append selected filename ASCII numbers to the output file
Step 3: Finding ASCII numbers for selected data in a file
Step 4: Finding Binary equivalent of each ASCII number and check weather binary length is 8
Step 5: If binary length is less than 8 then appending 0's to the left of the binary data.
Step 6: Split the above 8 bits of overall binary data in to 6 bit of binary data
Step 7: Find out that 6 bit binary data equivalent Decimal number
Step 8: Get characters from Radix-64 table that are decimal equivalent number.
Step 9: Stop

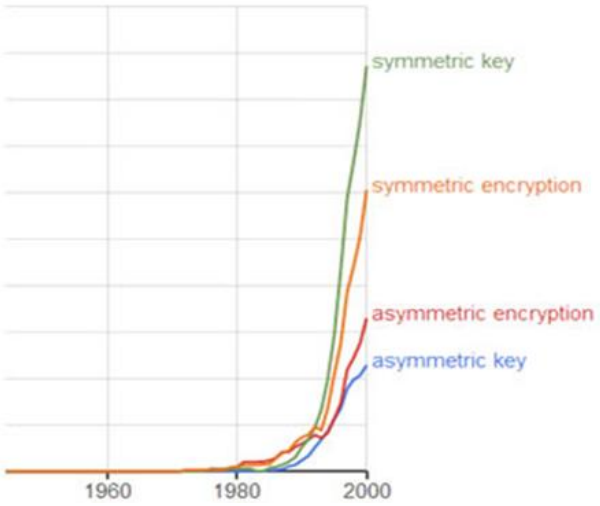
Algorithm: Decryption

Step 1: Start
Step 2: Select text file name for decryption
Step 3: Find out decimal equivalent numbers for decrypting from selected file
Step 4: Find out that 6 bit binary data equivalent Decimal number
Step 5: Split the above overall binary data in to 8 bits of binary data
Step 6: Find out the decimal equivalent for the above 8 bit of data
Step 7: Find the ASCII characters for the above 8 bit data
Step 8: Remove file name from the above data
Step 9: Finally we get Original data
Step 10: Stop

Radix-64 Comparison:



Symmetric Key Encryption:



IV. CONCLUSION

The existing technique TrueCrypt for encrypting and decrypting the text data is having so many unfixed bugs. So, we have proposed a new encryption and decryption technique called RadiCrypt. RadiCrypt is a combination of both Radix64 and Symmetric key encryption technique. In which Radix 64 uses 8 bits ASCII binary data by splitting into 6 bits where as symmetric key encryption encrypts the data by using a single key. The main advantage of using this technique is, it is simple and powerful at the same time it provides more security for our text data while reducing the complexity.

In future the same technique will be applicable for providing security to all types of data like image, audio, video and for different types of documents.

REFERENCES

[1] Program-technical aspects of encryption protection of users' data- URL: ttp://ieeexplore.ieee.org/document/7452083/
[2] Fakty: skolko tsiklov zapisi u fleshki? [Electronic resource]. – URL:http://hi-news.ru/periferiya/fakty-skolko-ciklov-zapisi-u-fleshki.html.
[3] Zaschischaem informatsiyu na s'yomnyih diskah. [Electronic resource]. – URL:http://wd-x.ru/protect-info-on-removable-drives/.
[4] «TrueCrypt»— programma dlya shifrovaniya. [Electronic resource]. – URL: https://te-st.ru/tools/truecrypt/.
[6] What is the Performance Impact of System Encryption With TrueCrypt. URL:http://www.digitalcitizen.life/what-performance-impact-system-encryption-truecrypt.
[7] CipherShed. [Electronic resource]. – URL: https://ciphershed.org.
[8] https://truecrypt.sourceforge.net/
[9] https://en.wikipedia.org/wiki/TrueCrypt
[10] https://en.wikipedia.org/wiki/Base64

[11] https://www.cse.ust.hk/faculty/cding/CSIT571/SLIDES/Radix-64.pdf
[12] https://en.wikipedia.org/wiki/Symmetric-key_algorithm
[13] http://www.webopedia.com/TERM/S/symmetric_key_cryptography.html
[14] https://docs.microsoft.com/en-us/sql/t-sql/statements/open-symmetric-key-transact-sql
[15] https://xakep.ru/2011/03/14/54794/
[16] http://en.wikipedia.org/wiki/denial_encryption
[17] https://digitalguardian.com/blog/what-data-encryption

