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. 4, Issue 8, August 2016

Study on Generation and Re-Generation of Alpha-Numeric Security (GRAS)

Abhisek Sharma, Gaurav Kumar Roy

MCA Student, Department of Computer Application, Lovely Professional University, Punjab, India

MCA Student, Department of Computer Application, Lovely Professional University, Punjab, India

ABSTRACT: Information security is now-a-days one of the prime concern and the messages need encryption as they pass through the internet. So Information Security is the technique of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. Much of the messages transferred and stored via internet is highly confidential and not for public viewing. In this paper I have developed a new cryptography algorithm which is based on block cipher concept. In this algorithm we have proposed a 4-keys encryption technique. Experimental results show that proposed algorithm is very efficient and secured. To write this paper we have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, we are presenting our proposed work. This algorithm is based on modern cipher.

KEYWORDS: Information security, Encryption, Decryption, Cryptography, Cryptosystem, Algorithm

I. INTRODUCTION

BASIC TERMINOLOGIES -

What is Cryptography: Cryptography is the art of writing text or data in secret code. It is used to encrypt plain text data (which is in human readable form) to a whole new unreadable form, which is called the cipher text. The mechanism of encryption and decryption is based on mathematical algorithms. These algorithms use secret key(s) for the secure transformations. With the increase in the size of the key, the security increases and the probability of breaking the cipher text back to plain text by hackers or criminals become lesser.

It is the most effective way to achieve data / message security. To read an encrypted file, you must have to access to the secret key that enables you to decrypt it.

Plain-Text: Unencrypted data or message which is easily readable by human and which is not in scrambled form is known as Plain-text.

Cipher-Text: Encrypted Data which is unreadable in by human intelligence and holds no meaning (because it is in scrambled form) is known as Cipher-text.

What is Encryption and Decryption?

Encryption is the process or technique of altering data which is in plain-text to cipher-text or secret message using algorithms or specially written programs. On the other hand, decryption is the process or technique of altering data which is in cipher-text or secretly written data back to its plain-text or human readable form.

Encipher and Decipher:

Converting a message or piece of text into coded form is known as encipher whereas converting a message or piece of text which is in crypted form back to plain-text is known as decipher.

What is Key in Cryptography: - A key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message. To prevent a key from being guessed, keys need to be generated truly randomly and contain sufficient entropy.

Why Cryptography technique is used?

Cryptography is used to protect confidential data such as email messages, conversations, chat sessions, web transactions, personal data, corporate information, e-commerce applications, etc.

Objective of Cryptography:

The major objective of cryptography is to maintain –

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

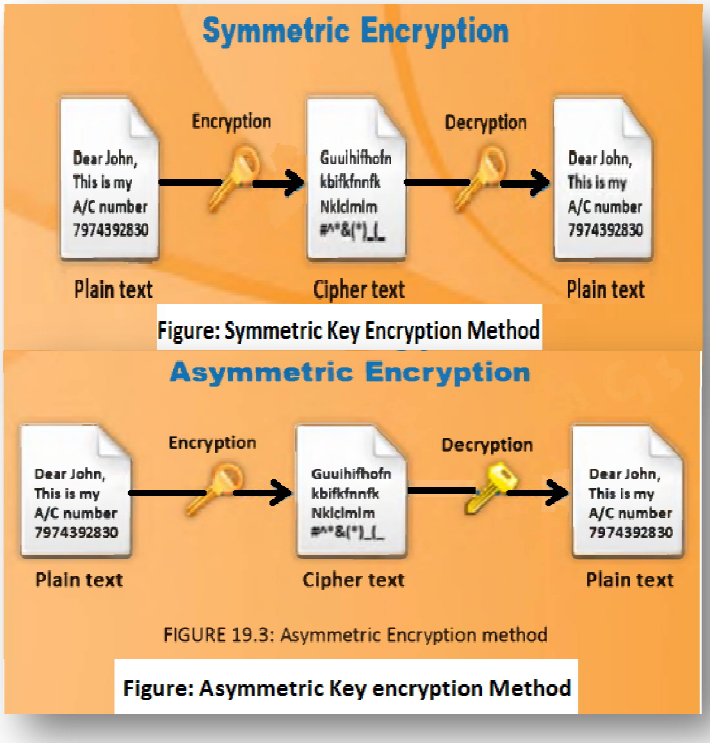
Vol. 4, Issue 8, August 2016

- ✓ Message Confidentiality
- ✓ Message Integrity
- ✓ Authentication
- ✓ Non-Repudiation

Types of Cryptography: -

The type of cryptography depends on the three different specifications. These are –

- Based on the Type of operations used for transforming plain-text to cipher-text: Most of the encryption algorithms are based on two fundamental principles – i) *Substitution*, where each element is in a plain-text is mapped into another element and ii) *transposition*, where the elements in the plain-text are rearranged.
- Based on the number of keys used: If both sender and receiver use the same key, the encryption-decryption technique is termed as *symmetric key*, single key or secret key or conventional encryption. But in case the sender and the receiver uses a different key, the technique is termed as *asymmetric key encryption*, two-key or public key encryption.
- Based on the way in which plain-text is processed: There are two sub-categories under this category. First is the *block cipher* that processes the input one block at a single time and produces an output block for each input block. Second is the *stream cipher*, which processes the input element continuously, producing the result one element at a time as it goes on.



The main feature of the encryption/decryption technique using algorithms or programs is to implement and generate the encryption key. Now-a-day, cryptography has many commercial grounds also. If we are concentrating on protecting confidential message or information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to gives solutions for other problems like: data integrity, authentication, and non-repudiation. Cryptography is the methods which allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches are being going on for creating new cryptographic algorithms having anti-brute-force capabilities and larger key length which makes it difficult to crack any message or password. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

So here we introduced a new cryptographic algorithm which encrypts and decrypts messages written in plain-text and then repeating the algorithm making the cipher again another cipher and continued this four times. This algorithm and program will provide 4-keys each having 104 characters. At the time of encryption, the program will be having two 104-bytes length key which will then get mixed up altogether within the algorithm to create random cipher-text.

Security Services: If we are taking about security of message or information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)

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. 4, Issue 8, August 2016

- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

IV. PROPOSED WORK

Here we have developed a new technique which is a combination of symmetric key cryptography plus substitution cipher together named it as GRAS Cipher (Generation and Regeneration of Alpha-numeric Security :: Cipher). In this proposed algorithm, two keys will be generated in the algorithm itself, and rest two keys will be given by the sender of the message. The sender will input two keys having length 104 bytes length x 2 (number of keys) = 208 bytes length key. So there will be 4 keys each having 104 bytes long so the total possible key combinations will be 104 (bytes length) x 4 (keys) = 416! Combinations (factorial of 416) possible combinations.

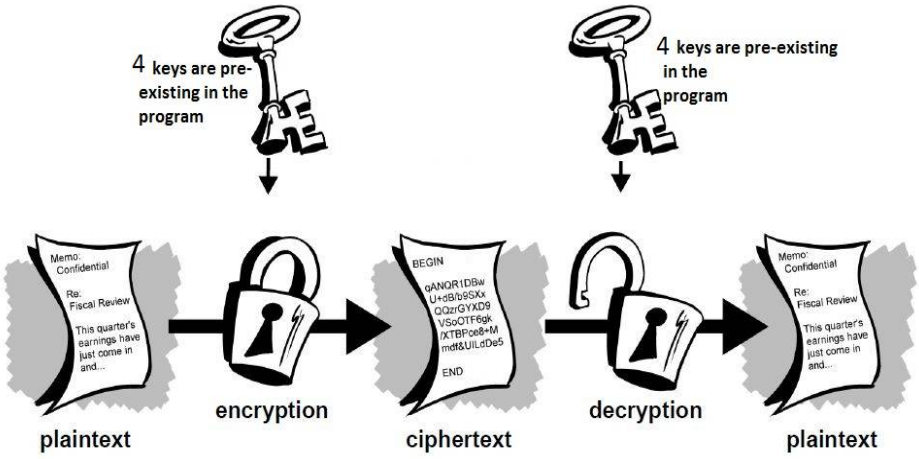


Figure: This is how the whole encryption decryption works

Steps for Proposed Algorithm (For Encryption):-

Step1: Start

Step2: Initially, plain text entered by Sender

Step3: If plainText[i] between 'a' – 'z' Then

If (i mod 4 == 1) then

{

cryptedText[i] = ((plainText[i] + key1[k]) – 2 x ASCII_Value('a')) mod 26 + ASCII_Value('a')

}

If (i mod 4 == 2) then

{

cryptedText[i] = ((plainText[i] + key2[k]) – 2 x ASCII_Value('a')) mod 26 + ASCII_Value('a')

}

If (i mod 4 == 3) then

{

cryptedText[i] = ((plainText[i] + key3[k]) – 2 x ASCII_Value('a')) mod 26 + ASCII_Value('a')

k=k+1

}

else

{

cryptedText[i] = ((plainText[i] + key4[k]) – 2 x ASCII_Value('a')) mod 26 + ASCII_Value('a')

}

else If plainText[i] between 0 – 9 Then

If (i mod 4 == 1) then

{

times[i] = ((plainText[i] + key1[k]) – ASCII_Value('a') – ASCII_Value(0))/10

cryptedText[i] = ((plainText[i] + key1[k]) – ASCII_Value('a') – ASCII_value(0)) mod 10 + ASCII_Value(0)

}

If (i mod 4 == 2) then

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. 4, Issue 8, August 2016

```
                {
        times[i] = ((plainText[i] + key2[k]) – ASCII_Value(‘a’) – ASCII_Value(0))/10
        cryptedText[i] = ((plainText[i] + key2[k]) – ASCII_Value(‘a’) – ASCII_value(0)) mod 10 + ASCII_Value(0)
                }
If (i mod 4 == 3) then
                {
        times[i] = ((plainText[i] + key3[k]) – ASCII_Value(‘a’) – ASCII_Value(0))/10
        cryptedText[i] = ((plainText[i] + key3[k]) – ASCII_Value(‘a’) – ASCII_value(0)) mod 10 + ASCII_Value(0)
k=k+1
                }
        else
                {
        times[i] = ((plainText[i] + key4[k]) – ASCII_Value(‘a’) – ASCII_Value(0))/10
        cryptedText[i] = ((plainText[i] + key4[k]) – ASCII_Value(‘a’) – ASCII_Value(0)) mod 10 + ASCII_Value(0)
                }
        else
        If (i mod 4 == 1) then
                {
        cryptedText[i] = ((plainText[i] + key1[k]) – (ASCII_Value(‘a’) – ASCII_Value(‘A’)) – 2 x
ASCII_Value(‘A’)) mod 26 + ASCII_Value(‘A’)

                }
If (i mod 4 == 2) then
                {
        cryptedText[i] = ((plainText[i] + key2[k]) – (ASCII_Value(‘a’) – ASCII_Value(‘A’)) – 2 x
ASCII_Value(‘A’)) mod 26 + ASCII_Value(‘A’)
                }
If (i mod 4 == 3) then
                {
        cryptedText[i] = ((plainText[i] + key3[k]) – (ASCII_Value(‘a’) – ASCII_Value(‘A’)) – 2 x
ASCII_Value(‘A’)) mod 26 + ASCII_Value(‘A’)
k=k+1
                }
        else
                {
        cryptedText[i] = ((plainText[i] + key4[k]) – (ASCII_Value(‘a’) – ASCII_Value(‘A’)) – 2 x
ASCII_Value(‘A’)) mod 26 + ASCII_Value(‘A’)
                }
```

Step4: Repeat Step 3, Until plainText become cipherText, where i = Index of plainText and k = Index of key
Step5: Print: cryptedText
Step6: End

Steps for Proposed Algorithm (For Decryption):-
Step1: Start
Step2: Initially, cipher text entered by Receiver
Step 3: Declare value (int)
Step4: If cryptedText[i] between ‘a’ – ‘z’ Then

```
        If (i mod 4 == 1) then
                {
        Value = ((cryptedText – ASCII_Value (‘a’)) + 26 + ASCII_Value (‘a’)) – key1[k]
dcryptText[i] = (value mod 26) + ASCII_Value(‘a’)
                }
If (i mod 4 == 2) then
                {
```

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. 4, Issue 8, August 2016

```
        Value = ((cryptedText – ASCII_Value(‘a’)) + 26 + ASCII_Value(‘a’)) – key2[k]
dcryptText[i] = (value mod 26) + ASCII_Value(‘a’)
                }
If (i mod 4 == 3) then
                {
        Value = ((cryptedText – ASCII_Value(‘a’)) + 26 + ASCII_Value(‘a’)) – key3[k]
dcryptText[i] = (value mod 26) + ASCII_Value(‘a’)
k=k+1
                }
        else
                {
        Value = ((cryptedText – ASCII_Value(‘a’)) + 26 + ASCII_Value(‘a’)) – key4[k]
dcryptText[i] = (value mod 26) + ASCII_Value(‘a’)
                }
        else If plainText[i] between 0 – 9 Then
If (i mod 4 == 1) then
                {
        value = ((cryptedText[i] – ASCII_Value(0)) + (10 x times[i]) + ASCII_Value(‘a’)) – key1[k]
        If value < 0 Then
                value = 10 + value
dcryptText[i] = (value mod 10) + ASCII_Value(0)
                }
If (i mod 4 == 2) then
                {       value = ((cryptedText[i] – ASCII_Value(0)) + (10 x times[i]) + ASCII_Value(‘a’)) –
key2[k]
        If value < 0 Then
                value = 10 + value
dcryptText[i] = (value mod 10) + ASCII_Value(0)
                }
If (i mod 4 == 3) then
                {
                value = ((cryptedText[i] – ASCII_Value(0)) + (10 x times[i]) + ASCII_Value(‘a’)) – key3[k]
        If value < 0 Then
                value = 10 + value
dcryptText[i] = (value mod 10) + ASCII_Value(0)
k=k+1
                }
        else
                {
                value = ((cryptedText[i] – ASCII_Value(0)) + (10 x times[i]) + ASCII_Value(‘a’)) – key4[k]
        If value < 0 Then
                value = 10 + value
dcryptText[i] = (value mod 10) + ASCII_Value(0)
                }
        else
        If (i mod 4 == 1) then
                {
        value = ((cryptedText[i] – ASCII_Value(‘A’)) + 26 + ASCII_Value(‘A’)) – (key1[k] – {ASCII_Value(‘a’) –
ASCII_Value(‘A’)})
        dcryptText[i] = (value mod 26) + ASCII_Value(‘A’)
                }
If (i mod 4 == 2) then
                {
```

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. 4, Issue 8, August 2016

value = ((cryptedText[i] – ASCII_Value(‘A’)) + 26 + ASCII_Value(‘A’)) – (key2[k] – {ASCII_Value(‘a’) – ASCII_Value(‘A’)})
dcryptText[i] = (value mod 26) + ASCII_Value(‘A’)
}
If (i mod 4 == 3) then
{
value = ((cryptedText[i] – ASCII_Value(‘A’)) + 26 + ASCII_Value(‘A’)) – (key3[k] – {ASCII_Value(‘a’) – ASCII_Value(‘A’)})
dcryptText[i] = (value mod 26) + ASCII_Value(‘A’)
k=k+1
}
else
{
value = ((cryptedText[i] – ASCII_Value(‘A’)) + 26 + ASCII_Value(‘A’)) – (key4[k] – {ASCII_Value(‘a’) – ASCII_Value(‘A’)})
dcryptText[i] = (value mod 26) + ASCII_Value(‘A’)
}
Step4: Repeat Step 3, Until cipherText become decryptedText (to obtain the sender’s plainText)
Step5: Print: dcryptText
Step6: End

V. MATHEMATICAL EXPRESSION

For Encryption:
C.T. = ((P.T. + key[i][k]) -ASCII_Val (‘a’) – ASCII_Val (INITIAL-Value of set) mod n + ASCII_Val (INITIAL-Value of set)
For Decryption:
P.T. = ((((cryptedText – ASCII_Value(INITIAL-Value of set)) + (n * m) + ASCII_Value(‘a’)) – key1[k]) mod n) + ASCII_Value(INITIAL-Value of set)
Here, ‘n’ represents specific set size and ‘m’ represents the multiplier which is used to regenerate the set size value.

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs and secures in much better way with the total number of keys and its length. The proposed algorithm provides energy efficient path for message security and maximizes the time duration to more than $10^{4 \text{ to } 5}$ years to creak using Brute force attack and decrypt the message.As the performance of the proposed algorithm is analyzed, we will put flavor in future with some modifications in design considerations, the security with 4 - 6rounds, inclusion of symbols and increasing the keys and key length to a more secured state, along with the performance of the proposed algorithm.

REFERENCES

[1] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
[2] T Morkel, JHP Eloff “ ENCRYPTION TECHNIQUES: A TIMELINE APPROACH” published in Information and Computer Security Architecture (ICSA) Research Group proceeding.
[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.
[5] Neal Koblitz “A Course in Number Theory and Cryptography” Second Edition Published by Springer-Verlag.

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. 4, Issue 8, August 2016

BIOGRAPHY

Gaurav Kumar Roy is a CEO and founder of ITHubSchool, also a Certified Ethical Hacker (C|EH), Computer Hacking Forensic Investigator (CH|FI), EC-Council Certified Security Analyst (EC|SA), CCNA, OWASP10, software developer and pursuing Masters in Computer Application (MCA). He has keen interest in programming, web development and security and currently works as Technical Writer at www.w3schools.in. *Linkedin Link:* https://in.linkedin.com/in/gaurav-roy-119221110

Abhisek Sharma is a computer enthusiast and security expert, software developer and has HP & Microsoft certification on C#, Java, Python and many more programming languages. Currently, he is pursuing Masters in Computer Application (MCA). He has keen interest in solving problems with programming and is a Vulnerability Penetration Tester (VAPT) also. *Linkedin Link:* https://in.linkedin.com/in/abhisek-sharma-27884a49