# Smart Network Algorithm

**Neha[1] Navya. V[2] Anusha[3] Munseera[4]**
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Shree Devi Institute of Technology, Mangaluru, India

*Abstract*— The internet today is being used by millions of users for a large variety of commercial and non-commercial purposes. It is mainly used as an efficient means for communication, entertainment and education. As the internet grows the existing security framework was not adequate for modern day applications. Cryptography plays a vital role in providing security. Lot of research is going on block cipher algorithms. The proposed system is more space and time efficient. The algorithm is implemented in .NET Framework. In this algorithm we will be working on to overcome all the drawbacks of the existing system. It is more secured and efficient. The length of both plain text and encrypted data will be of same length. Hence, it reduces the storage space and time consumption.

***Key words:*** Smart Network Algorithm

## I. Introduction

Cryptographic algorithm plays a vital role in the field of network security. There are two basic types of cryptosystems such as symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems are characterized by the fact that the same key is used in encryption and decryption transformations. In contrast to symmetric cryptosystems, asymmetric cryptosystems use complementary pairs of keys for encryption and decryption transformations. One key, the private key is kept secret like the secret key in a symmetric cryptosystem. The other key, the public key, does not need to be kept secret. This two key approach can simplify key management by minimizing the number of keys that need to be managed and stored in the network. The key distribution system is also much simpler as it can use unprotected medium for the distribution of the public keys. Data integrity and/or data origin authentication for a message can be provided as follows. The originator of the message generates, using all the data bits of the message contents and a secret key, an Integrity Check Value which is transmitted along with the message. The message recipient checks that the received message content and Integrity Check Values are consistent before accepting the message. A digital signature can be considered as a special case of Integrity Check Value. The digital signature may need to be used to resolve a dispute between the originator and recipient of a message. Symmetric encryption based or keyed hash algorithm based approach is usually inadequate for this purpose. Asymmetric cryptosystems provide more powerful digital signatures.

Many cryptographic algorithms are introduced day by day by many researchers all over the globe. But many algorithms have simple structures that can be breakable. The recent advances in cryptanalytic techniques are remarkable. A quantitative evaluation of security against powerful cryptanalytic techniques such as differential cryptanalysis and linear cryptanalysis is considered to be essential in designing any new block cipher.

In this paper a new algorithm for cryptography named Smart Network Algorithm (SNA) is proposed. The proposed algorithm is developed based on design principle known as Matrix cipher.

## II. Related work

Some of the commonly used algorithms are evaluated and implemented in C and Visual Basic to identify the weakness. Some of the block ciphers are taken into the consideration such as DES, 3DES, Blowfish and AES. Brief definitions of the most common encryption techniques are given as follows:

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher.

3DES: It is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods.

Blowfish: It is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to two fish.

AES: (Advanced Encryption Standard) is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

## III. Problem statement

The study shows that DES, 3DES have some security issues and performance issues. It is also found that AES and blowfish are highly secured than other encryption algorithms. The work stated that “According to academic papers and reports regarding the security evaluation for such algorithms, it is difficult to ensure enough security by using the algorithms for a long time period, such as 10 or 15 years, due to advances in cryptanalysis techniques, improvement of computing power, and so on. To enhance the transition to more secure ones, National Institute of Standards and Technology (NIST) of the United States describes in various guidelines that NIST will no longer approve two-key triple DES, RSA with a 1024-bit key and SHA-1 as the algorithms suitable for IT systems of the U.S. Federal Government after 2010”. Based on this study the statement of the problem is formulated and the new algorithm is proposed.

## IV. Proposed Algorithm

The proposed system is formulated on double encryption. Initially the data is encrypted using AES algorithm and then using proposed algorithm. The data is decrypted in the reverse order of encryption.

### A. *AES algorithm*

In cryptography the Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S government. AES is the first publicly accessible and open cipher approved by the NSA for top secret information. The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption as well as for decryption. The length of data blocks is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. AES algorithm is also an iterative algorithm. Each iteration can be called a round, and the total number of rounds is 10, 12, or 14, when key length is 128,192, or 256, respectively. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called the State, and all the internal operations of the AES algorithm are performed on the State.

The AES algorithm, a symmetric block cipher can encrypt as well as decrypt the data. Encryption translates data to a secret form called cipher-text. Encryption of the cipher-text then converts the data back into its original form, which is known as plain-text. AES is also reversible as most of the encryption algorithms. This helps us to understand that almost the same steps with some simple changes are performed to complete both encryption and decryption in reverse order.

For encryption, each round consists of the following four steps:

1) Sub Bytes
2) Shift Rows
3) Mix Columns
4) Add Round Key

For decryption, each round consists of the following four steps:

1) Inverse Shift Rows
2) Inverse Sub Bytes
3) Add Round Key
4) Inverse Mix Columns

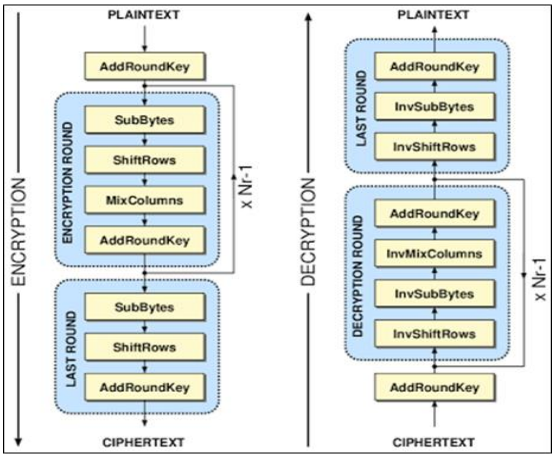

Fig. 1: AES Encryption/ Decryption process

#### 1) *SUB BYTES:*

Sub Bytes is the first transformation used at the encryption site. To substitute a byte, we have to represent the byte as two hexadecimal digits. The main aim of the substitution step is to reduce the correlation between the input bits and the output bits at the byte level. The bit scrambling part of the substitution step ensures that the substitution cannot be described in the form of evaluating a simple mathematical function.

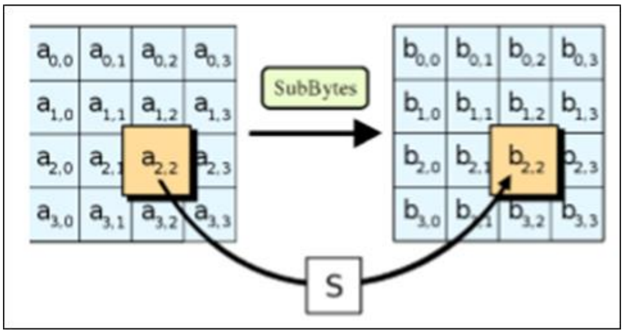

Fig. : Sub Bytes

#### 2) *SHIFT ROW*

The Shift Row transformation comprises of four basic steps as mentioned below:

1) Keeping the first row of the state array unchanged
2) Shifting the second row circularly by one byte to the left
3) Shifting the third row circularly by two bytes to the left
4) Shifting the last row circularly by three bytes to the left. The input block is written column-wise not row-wise.

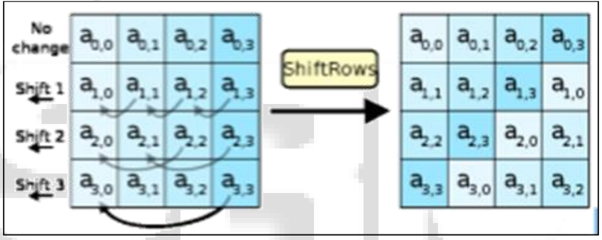

Fig. : Shift Row

#### 3) *MIX COLUMN*

The Mix Column transformation replaces each byte of a column by a function of all the bytes in the same column. More precisely, each byte in a column is replaced by two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows.

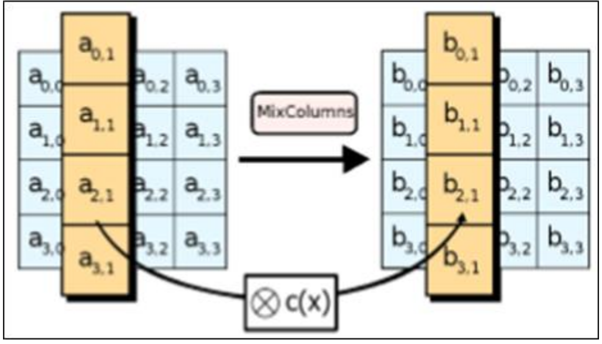

Fig. : Mix Columns

#### 4) *ADD ROUND KEY*

In the Add Round Key step, the sub key is combined with the state. Each round has its own round key that is derived from the original 128-bit encryption key. For each round a sub key is derived from the main key. The sub key is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.

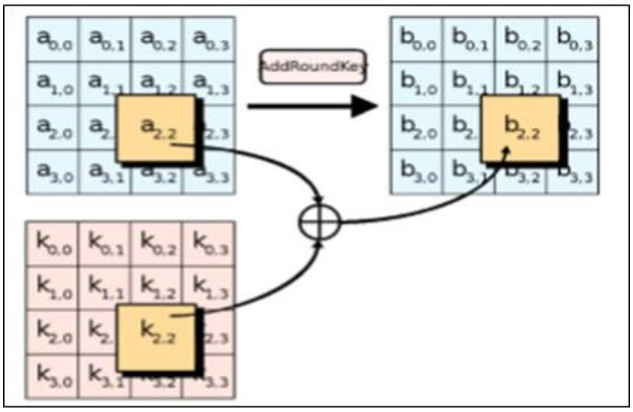
AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig. : Add Round Key

Decryption process is just the reverse of encryption process which inverse round transformations to computes out the original plain text of an encrypted cipher text in reverse order. Add Round Key is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order. Inverse Mix Columns needs a different constant polynomial than Mix Columns does. Inverse Shift Rows rotates the bytes to the right instead of to the left. Inverse Sub Bytes takes place by an inverse transformation followed by the same inversion over which is used for encryption.

### B. *Smart Network Algorithm*

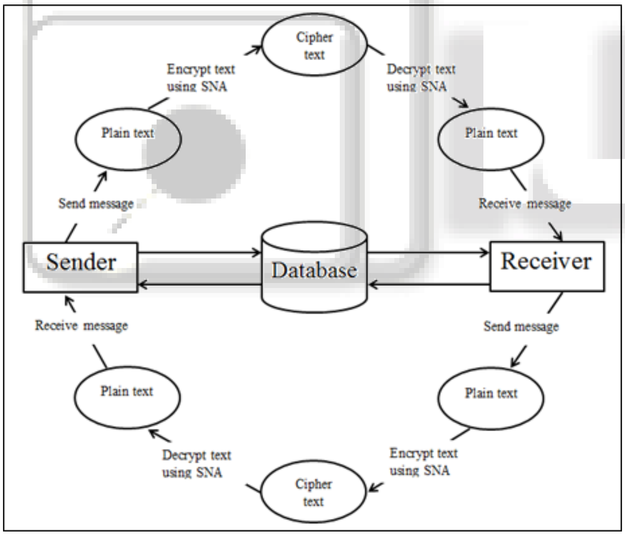

Fig. 2: Architectural diagram of SNA

Considering a sender and a receiver as end systems, a server is placed at the centre. Server is used for the storage purpose. When a sender sends a message it travels through the transmission path and the message is stored as encrypted format in server. Here the encrypted format is 32bits long. Further the encrypted data is routed towards the receiver. The decrypted data is displayed as a message at the receiver side.

In this proposed system we are trying to reduce the length of encrypted data that has to be stored in the server which in turn reduces the storage space and is more efficient. The following steps are involved in this algorithm.

- Step 1: A 9x9 matrix is considered which is further divided into 9 blocks of 3x3 matrices each that is numbered from block 0 to block 8.
- Step 2: The matrix is randomly filled with upper case and lower case alphabets, numeric and special characters.
- Step 3: When a text message is sent, the algorithm automatically search for the position of the first character in the matrix and similarly the position of remaining characters.
- Step 4: Depending upon the character position in the matrix, the block number is noted and also the character position within the block is checked and that is also noted.
- Step 5: Counting from the next position of the character, the number of places to be shifted within the block depends on the position of the character in that block.
- Step 6: The new character that is obtained after shifting the places will replace the original character. Hence, the replaced character is called the encrypted data of the original message.

For example: Let us consider a chat engine as the example to show the encryption using the proposed algorithm. If the message sent is say “We”, then the encrypted data for this can be obtained as follows:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A | 0 | R | U | 3 | S | H | z | M |
| . | B | , | ; | h | x | y | N | 6 |
| s | v | C | q | w | p | o | : | I |
| c | t | X | V | ! | W | Y | 7 | G |
| % | Q | 1 | @ | g | 4 | / | P | * |
| a | u | b | d | # | E | F | ( | Z |
| m | 2 | D | r | 5 | T | J | - | j |
| & | e | [ | = | i | + | 8 | K | ) |
| f | ] | n | l | 9 | O | k | _ | L |

Fig. 3: Matrix Cipher

‘W’ is in the position {4, 2}, so moving forward 2 places from the position of ‘W’ we get ‘g’. Hence, ‘W’ will be replaced by ‘g’.

Similarly, ‘e’ is in the position {6, 4}, so moving forward 4 places from the position of ‘e’ we get ‘n’. Hence, ‘e’ will be replaced by ‘n’.

Finally, the encrypted data for the message “We” is “gn” and this will be stored in the server for security purpose.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A | 0 | R | U | 3 | S | H | z | M |
| . | B | , | ; | h | x | y | N | 6 |
| s | v | C | q | w | p | o | : | I |
| c | t | X | V | ! | g | Y | 7 | G |
| % | Q | 1 | @ | W | 4 | / | P | * |
| a | u | b | d | # | E | F | ( | Z |
| m | 2 | D | r | 5 | T | J | - | j |
| & | n | [ | = | i | + | 8 | K | ) |
| f | ] | e | l | 9 | O | k | _ | L |

Fig. 4: Encrypted Data Stored in Matrix Cipher

## V. ADVANTAGES

1) The proposed system requires comparatively less storage space than the existing system.
2) In this system it is difficult to obtain the key; hence the data cannot be gained.
3) The encrypted data will be in same length as that of plain text hence, it takes less time for transmission.

## VI. Conclusion

In this paper, various cryptographic algorithms are reviewed. From the literature review, it is identified that the block cipher with 128 bit keys and 128bit block size will not be suitable for IT systems and banking sectors due to the advances in the computing technologies and cryptanalysis techniques. So in order to overcome this problem, we propose a new algorithm named as Smart Network Algorithm(SNA) which is capable of encrypting data of similar length as that of original data. Cryptanalysis is carried out in the encrypted file. It was found that the encrypted file with this algorithm is difficult to break. In this work, AES algorithm is initially used to encrypt the data. Once the data is encrypted it uses SNA for double encryption.

## References

[1] A New 512 Bit Cipher for Secure Communication M. Anand Kumar and Dr.S.Karthikeyan

[2] Design and Simulation of AES algorithm for cryptography, Radhika D Bajaj, Dr U M Gokhale.

[3] Alaa, T., A.A. Zaidan and B.B. Zaidan, 2009. New framework for high secure data hidden in the MPEG using AES encryption algorithm. Int. J. Comput. Electr. Eng., 1: 566-571.

[4] Matin, M.A. Hossain, M.M. Islam, M.F and Islam, M.N,2009. Performance evaluation of symmetric encryption algorithm in MANET and WLAN.IEEE International conference for Technical Postgraduates, pp: 1-4.

[5] Rabah, K., 2004. Data security and cryptographic techniques: A review. Inform. Technol. J., 3: 106132.

[6] Rabah, K., 2005. Secure implementing message digest. Authentication and Digital Signature.

[7] Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

[8] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .