International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

DNA Based Cryptography

Durga Karapurkar[1], Veena Bhaskaran[2], Shreya Bale[3], Preeti Pednekar[4]

[1, 2, 3, 4]Student of Computer Department, Don Bosco College of Engineering, Goa India

Abstract: ***In the era of information technology, Security to the system is essential. With development in computer and network technologies, people's communication has changed greatly. Data security has become one of the significant issue in communication. This causes major concern for privacy, identity theft, social security numbers and many more. Cryptography provides way of making secure message for confidential message transfer. It is the standard way of transforming the sender's message to secret format called cipher text that only intended receiver will understand secret message. One of the efficient way to achieve this is DNA based cryptography. It is a technology of bio science to encrypt large message in compact volume. DNA is used as information carrier. Its computational logic can be used in cryptography for encrypting, storing and transmitting the information. The power of DNA computing strengthens the existing system by opening new possibility of hybrid cryptographic system. In this paper, a new cryptographic technique is proposed based on Advanced encryption standard. DNA has tremendous storage capacity, high parallelism and ability to synthesize DNA sequence of any desirable length.***

Keywords: Advanced encryption standard; AES; DNA, symmetric cipher, block cipher

1. Introduction

Information flows throughout the network that may be of local or of global scope. It is mandatory to secure that information to prevent from unauthorized access of it. Thus, to achieve security it is necessary to encode the data before sending it through the various unreliable communication channels available to make it unreadable. Cryptography provides a method for securing and authenticating the transmission of information over secure channels. Latest development on this field is DNA cryptography.

One of the most essential components required for the functioning of all living organisms is DNA. DNA stands for Deoxyribonucleic acid and it has many properties like vast parallelism, exceptional energy storage capability. There are four classes of nucleotides, Adenine, Guanine, Cytosine, Thymine (A, C, G, T). DNA is basically used to store genetic information. This information cannot be duplicated or copied. A strand contains a sequence of bases in specific patterns. This double helical structure is formed by the hydrogen bond between the T with C and G with A.

DNA cryptography provides greater security to knowledge, in this method plain text data is converted into DNA sequence. This Cryptographic scheme was introduced in the 1994 by Dr. Leonard M. Adelman of the University of Southern California. It provides two different fold securities through applying complex computation. It uses bio-molecular technique for encryption and decryption procedure, as the bio molecule has complex structure which is difficult to analyses simply.

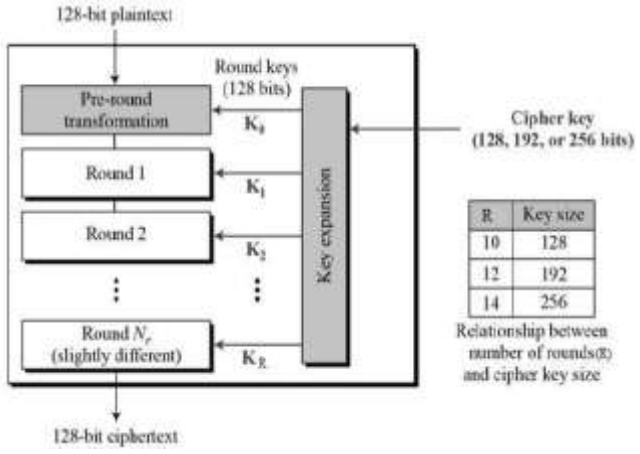
2. AES Design

AES is based on a design principle known as a substitution permutation network, and is fast in both software and hardware. The AES algorithm is symmetric block cipher that can encrypt and decrypt information. Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijndael. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits AES operates on a 4x4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special [mite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

The number of rounds are as follows:
• 10 rounds for 128-bit keys.
• 12 rounds for 192-bit keys.
• 14 rounds for 256-bit keys.

a) Operation of AES

AES is an iterative rather than Feistel cipher. It performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing a matrix *A*.



R	Key size
10	128
12	192
14	256

Figure: Key Expansion

b) Steps of key expansion

1) RotWord takes a word [a0, al, a2, a3] as input, performs a cyclic permutation, and returns the word [al, a2, a3, a0].

Licensed Under Creative Commons Attribution CC BY

2) SubWord is a function that takes a four-byte input word and applies the S-box to each of the four bytes to produce an output word.
3) The round constant word array, Rcon[i], contains the values given by [X_{i-1},{00}, {00}, {00}], with X_{i-1} being powers of X.
4) Last operation includes XOR with Rcon and then XOR with the temp to produce an output word (substitution).

3. Encryption Process

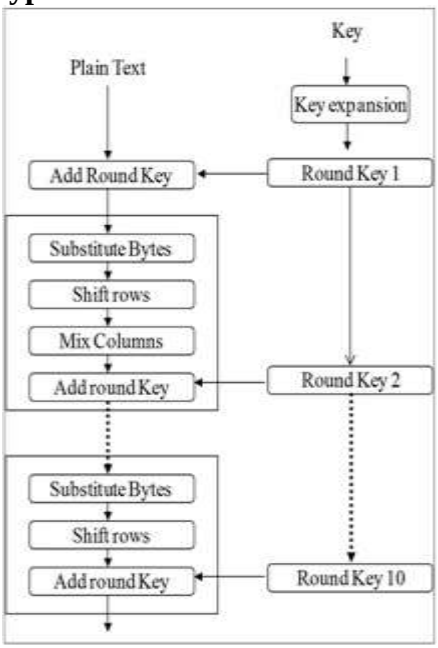


Figure: Encryption

a) AES Round operations

1) Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure: AES S-Box

2) Shift Rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

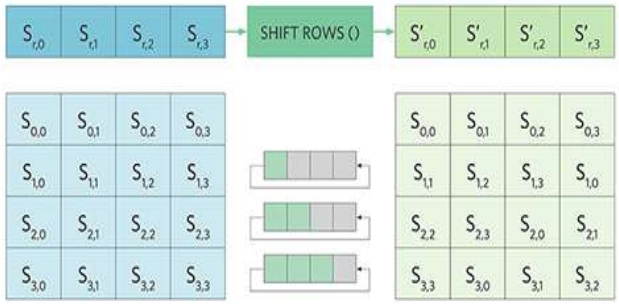


Figure: Shift Rows Operation

3) Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

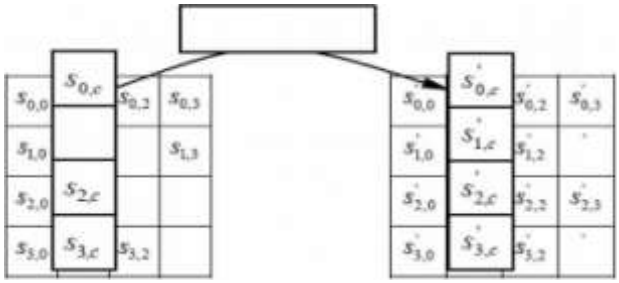


Figure: Mix column

4) Add Round Key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round, then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

4. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, the encryption and decryption algorithms need to be separately implemented.

5. The Proposed DNA-Based Advanced Encryption Standard

In our work, we are presenting the DNA based design and implementation to "Advanced Encryption Standard" [AES]. We built our algorithm with all its specifications (data, algorithms operations and used functions) on DNA basis instead of bits.

The proposed algorithm will encrypt the plain text using new encryption technique and decrypt the cipher text using

Licensed Under Creative Commons Attribution CC BY

decryption technique. It also proposes a unique cipher text generation in the form of DNA sequence as well as a new key generation procedure

a) Inputs and Outputs

The plaintext is to be introduced in the form of block each of 128 bits. Initial key is in lengths 128, 192 or 256 bits. Figure below shows how binary bits are converted to DNA streams. The result is input stream of size =64 DNA value-considered one block (128 bit). Key size is 64, 96, or 128 DNA. The ciphertext will be of the same size as the plaintext.

BIT 1	BIT 2	DNA
0	0	A
0	1	C
1	0	G
1	1	T

Figure: DNA representation of bits

b) Proposed DNA Functions

1) DNA XOR

The XOR operation using DNA inputs will result in output and can be implemented as follows:

1. Detect if the two inputs are the same
➔ output =A.
2. Detect if one of the inputs is the inverse of the other (A and T are complement, C and G are complement)
➔ output =T.
3. Detect if one of the inputs is 'A'
➔ output=the other DNA.
4. Detect if one of the inputs is 'T'
➔ output=the inverse of the other DNA.

2) DNA Substitute in the S-box

The idea depends on saving the S-box in the form of DNA. Standard s-box is modified such that value in s-box is converted to decimal and then to binary numbers. Binary values are written in corresponding DNA sequence. So we will have 16 DNA streams. The next table shows the DNS-based S-Box and the following figure shows how it is saved as DNA streams.

Substitution to reach the right output includes two sub operations:

1) Finding the right DNA stream (row) which is one of 16 streams.
2) Finding the right sequence in this stream(column)

		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
		AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
0	AA	CGAT	CTTA	CTCT	CTGT	TTAG	CGGT	CGTT	TACC	ATAA	AAAC	CGCT	AGGT	TTTG	TCCT	GGGT	CTCG
1	AC	TAGG	GAAG	TAGC	CTTC	TTGG	CCGC	CACT	TTAA	GGTC	TCCA	GGAG	GGTT	GCTA	GGCA	CTAG	TAAAA
2	AG	GTCT	TTTC	GCAT	AGCG	ATCG	ATTT	TTCT	TATA	ATCA	GGCC	TGCC	TTAC	CTAC	TCGA	ATAC	ACCC
3	AT	AACA	TACT	AGAT	TAAT	ACGA	GCCG	AACC	GCGG	AACT	ACAG	GAAA	TGAG	TGGT	AGCT	GTAG	CTCC
4	CA	AAGC	GAAT	AGTA	ACGG	ACGT	CGTG	CCGG	GGAA	CCAG	ATGT	TCCG	GTAT	AGGC	TGAT	AGTT	GACA
5	CC	CCAT	TCAC	AAAA	TGTC	AGAA	TTTA	GTAC	CCGT	CGGG	TAGT	GTTG	ATGC	CAGG	CATA	CCGA	TATT
6	CG	TCAA	TGTT	GGGG	TTGT	CAAT	CATC	ATAT	GACC	CACC	TTGC	AAAG	CTTT	CCAA	ATTA	GCTT	GGGA
7	CT	CCAC	GGAT	CAAA	GATT	GCAG	GCTC	ATGA	TTCC	GTTA	GTCG	TCGG	AGAC	ACAA	TTTT	TTAT	TCAG
8	GA	TATC	AATA	ACAT	TGTA	CCTT	GCCT	CACA	ACCT	TACA	GGCT	CTTG	ATTC	CGCA	CCTC	ACGC	CTAT
9	GC	CGAA	GAAC	CATT	TCTA	AGAG	AGGG	GCAA	GAGA	CACG	TCTG	GTGA	ACCA	TCTG	CCTG	AAGT	TCGT
a	GG	TGAA	ATAG	ATGG	AAGG	CAGC	AACG	AGCA	CCTA	TAAG	TCAT	GGTA	CGAG	GCAC	GCCC	TGCA	CTGC
b	GT	TGCT	TAGA	ATCT	CGTC	GATC	TCCC	CATG	GGGC	CGTA	CCCG	TTCA	TGGG	CGCC	CTGG	GGTG	AAGA
c	TA	GTGG	CTGA	AGCC	AGTG	ACTA	GGCG	GTCA	TACG	TGGA	TCTC	CTCA	ACTT	CAGT	GTTC	GAGT	GAGG
d	TC	CTAA	ATTG	GTCC	CGCG	CAGA	AAAT	TTCG	AATG	CGAC	ATCC	CCCT	GTGC	GACG	TAAC	ACTC	GCTG
e	TG	TGAC	TTGA	GCGA	ACAC	CGGC	TCGC	GATG	GCCA	GCGT	ACTG	GACT	TGGC	TATG	CCCC	AGGA	TCTT
f	TT	GATA	GGAC	GAGC	AATC	GTTT	TGCG	CAAG	CGGA	CAAC	GCGC	AGTC	AATT	GTAA	CCCA	GTGT	ACCG

Figure: DNA S-box

c) The proposed D-AES algorithm implementation

1) DNA-Based Key Expansion

Suppose we take the key size = 128 bits with 10 rounds. The DNA key stream (64 DNA) is divided into smaller streams of size = 16 DNA resulting in 4words (W[i], I =0, 1, 2, 3). Key expansion should expand from 4 words to 44 words. So we need to generate from W[4] to W[43] through the following steps:

- **Rotation by 4 DNA (DNA RotWord):**

This step includes left rotation of 16 DNA (equivalent to 32 bits) by 8 bits or 4 DNA. So input is 16 DNA and output is16 DNA after rotation. It is implemented through the following algorithm steps:

○ Take the first 4 DNA and save them in stream l
○ Remove the first 4 DNA from Input
○ Output = Input+ stream

2) Substitute in S-box

This step includes taking as input the output of the rotation step (16 DNA), and then we substitute each 4 DNA in the s-box and return the result 16 DNA.

○ Take 4 by 4 DNA from input
○ Search the s-box streams.
○ Return an output 4 DNA
○ Collect all outputs to give 16 DNA

3) XOR with Rcon

Get Constant (Rcon) which is stored in streams for each iteration. Then the result of the previous step is XORed with RCON according to the round number.

Licensed Under Creative Commons Attribution CC BY

```
private void f_gen_RCon()
{
    RCon=new string[NRounds+1];
    //for(int i=0;i<NRounds;i++)
    RCon[1] = "AAAC AAAA AAAA AAAA"; //01
    RCon[2] = "AAAG AAAA AAAA AAAA";//02
    RCon[3] = "AACA AAAA AAAA AAAA";//04
    RCon[4] = "AAGA AAAA AAAA AAAA";//08  0000 1000
    RCon[5] = "ACAA AAAA AAAA AAAA";//10  0001 0000
    RCon[6] = "AGAA AAAA AAAA AAAA";//20  0010 0000
    RCon[7] = "CAAA AAAA AAAA AAAA";//40  0100 0000
    RCon[8] = "GAAA AAAA AAAA AAAA";//80  1000 0000
    RCon[9] = "ACGU AAAA AAAA AAAA";//1B  0001 1011
    RCon[10] = "AUCG AAAA AAAA AAAA";//36 0011 0110
}
```

Figure: RCON

4) XOR with W[i-4]
The output from the previous step is XORed with W[i-4] which is also 16 DNA. Note that the generated keys have 4<= i<=43.

B) DNA based AES Plaintext Encryption
The plaintext in the form of DNA is divided into separate streams of size 64 DNA (128 bit). If the last stream is less than 64, then it is concatenated by 'A' till reaching the 64 DNA size. Each stream is put in the form of STATE. The STATE consists of 4 streams (rows), each row contains16 DNA. Each step will go through following rounds:

- **Sub Bytes**

In this step, each 4 DNA in STATE streams will be an input to the function substitute in the S-Box.

- **Shift Rows**

It is a transformation that operates row by row on STATE. It is basically a function separating each row in separate stream then left rotation by 4 DNA characters according to each row number. The row number ranges from 0 and 3.

- **Complement of DNA matrix**

Each column of STATE array is processed separately to produce new column. It involves taking compliment of each DNA.

- **Add Round key**

It is a simple operation that involves XOR of elements of the STATE with the corresponding Round key. Thus the cipher text is obtained when key is XORed with DNA sequence.

C) DNA based Decryption

All the steps of AES encryption are performed in reverse order once receiver gets the key. Key generated by key expansion algorithm is transferred using secure medium (TCP and SSL protocols)

- **Add round key**

Operation involves XORing key with cipher text.

- **Complement of matrix**

Each column of STATE array is processed separately to produce new column. It involves taking complement of each DNA

- **Shift rows**

Perform right rotation according to number of row.

- **Sub bytes:**

STATE streams are substituted using inverse SBOX.
Covert the resulting DNA sequence in binary format. Binary values are then converted to hexadecimal.
Plain text is thus obtained from cipher text.

A. Application

It can be used in different fields like **private companies,** government organization like **aeronautical agencies**, **research area** etc.

- To protect **military messages**.
- Securing conference papers from intruders.
- Secure private files and documents.

6. Future Scope

This proposed idea can not only overcome the existing network security but also has edge over the computational time. However, in this paper only text files are encrypted, in future messages can be in form of images or audio as well as video which are equally important to be protected against intruders and cryptanalysts.

References

[1] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa “Design of DNA-based Advanced Encryption Standard (AES)” Faculty of Computer Science and Information Systems, Ain Shams University, Cairo, Egypt.
[2] Tausif Anwar, Abhishek Kumar, Sanchita Paul “DNA Cryptography Based on Symmetric Key Exchange” Dept. of Computer Science & Engineering, Birla Institute of Technology, Mesra Ranchi, India.
[3] Suvajit Dutta, Tanumay Das, Sharad Jash, Debasish Patra, Dr.Pranam Paul “A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions”
[4] Xing Wang, Qiang Zhang “DNA computing-based cryptography” Key laboratory of advance design and intelligent computing (Dalian University) Ministry of Education, Dalian, China.
[5] Atanu Majumder, Abhishek Majumdar, Tanusree Podder, Nirmalya Kar, Meenakshi Sharma “Secure Data Communication and Cryptography Based on DNA Based Message Encoding” Dept. of Electronics and Information Technology, NIC Tripura State Centre, Agartala, India, Dept. of Computer Science & Engineering, SSCET, Badhani, Punjab, India
[6] Souhila Sadeg, Mohamed Gougache, Nabil Mansouri, Habiba Drias “An encryption algorithm inspired from DNA” Computer Science Department, USTHB, LRIA, Algeria.
[7] Gurpreet Kour Sodhi and Gurjot Singh Gaba “DNA and Blum Blum Shub Random Number Generator Based Security Key Generation Algorithm” Discipline of Electronics &Communication Engineering, Lovely Professional University, Jalandhar, India.
[8] Amritha Thekkumbadan Veetil “An Encryption Technique Using Genetic Operators” MTech, Computer Science Invertis University, Bareilly, Uttar Pradesh, India

Licensed Under Creative Commons Attribution CC BY