Pune Institute of Computer Technology
Dhankawadi, Pune

A SEMINAR REPORT
ON

ENCRYPTION OF PLAINTEXT USING MODIFIED AES

SUBMITTED BY

ADITYA JITENDRA SAWANT
Roll No. 31302
Class TE-3

Under the guidance of
Prof. S.H. PISEY

DEPARTMENT OF COMPUTER ENGINEERING
Academic Year 2020-21

DEPARTMENT OF COMPUTER ENGINEERING

Pune Institute of Computer Technology
Dhankawadi, Pune-43

CERTIFICATE

This is to certify that the Seminar report entitled

“ENCRYPTION OF PLAINTEXT USING AES”

Submitted by
Aditya Jitendra Sawant Roll No. 31302

has satisfactorily completed a seminar report under the guidance of Prof. S.H Pisey towards the partial fulfillment of third year Computer Engineering Semester II, Academic Year 2020-21 of Savitribai Phule Pune University.

Prof. S.H Pisey
Internal Guide

Prof. M.S.Takalikar
Head
Department of Computer Engineering

Place: Pune
Date: 21-05-2021

ACKNOWLEDGEMENT

I sincerely thank our Seminar Coordinator Prof. B.D.Zope and Head of Department Prof. M.S.Takalikar for their support.

I also sincerely convey my gratitude to my guide Prof. S.H Pisey, Department of Computer Engineering for her constant support, providing all the help, motivation and encouragement from beginning till end to make this seminar a grand success.

Contents

List of Tables

List of Figures

Abstract

Due to recent advancements in communication networks and computation, massive volumes of data has been flowing from one place to another. To prevent unauthorized access and manipulation of this data, many different cryptographic techniques have been employed. In this paper, we briefly discuss about need of cryptography, differences between symmetric and asymmetric key algorithms and some popular symmetric-key cryptosystems: AES, DES, and 3DES. After briefly touching on DES and its weaknesses, we move on to the main focus of this paper, the working of AES algorithm. AES is a symmetric key cryptographic algorithm proposed by Vincent Rijmen and Joan Daemen. This paper will provide an overview of AES algorithm and explain its working and several crucial features. Although AES supports 128, 192 and 256 bit key length, we will focus on 128 bit key. Then we conclude by comparing it against other symmetric key algorithms and see its advantages as well as disadvantages.

Keywords

AES, Cryptography, Decryption, Encryption, Hardware Encryption, RSA, DES

1 INTRODUCTION

Today, large amounts of data is transferred across various mediums. In this process, internet communication plays a major role. But this data, if sent through insecure channels may fall into wrong hands. It could be especially dangerous if this data happens to be sensitive details of a person or information related to net banking or of military data. To prevent this many methods have been developed by private and public sectors. Cryptography is one of the most significant and popular technique used to protect sensitive data. It involves two major steps: encryption and decryption. Encryption is the process of taking a plaintext (cleartext) and converting it into a ciphertext using a function known as encryption function. Decryption involves reverse operation of encryption ie. it takes ciphertext as input and returns plaintext. The encryption function also takes another parameter along with plaintext known as the key.

Today, we use cryptography on a daily basis to transfer vast amounts of data securely over the networks. Some common uses include:

- We use time stamping technique to certify that a certain document or communication existed or was delivered at a certain time. Time stamping uses blind signature scheme which allows the sender to get a message receipted by another party without revealing any information about the message to the other party.
- A stream cipher named A5/1 is employed to supply over-the-air communication privacy within the GSM mobile phone standard. It's one among seven algorithms that were specified for GSM use.
- Emails are encrypted in end to end fashion and are secured at every stage of delivery. They cannot be read even by the email servers.
- Hardware-based disk encryption is also becoming a feature on an increasing number of consumer and industrial SSDs.

2 MOTIVATION

With evolution of internet from a network used for military purposes to a consumer product with billions of users worldwide daily, it has become it has become critical that each user get secure access to it. Today people use internet for net banking, online transaction, communication, etc. Apart from these individuals, other organizations such as various companies, hospitals, educational institutes and government agencies heavily rely on the internet to send and receive bulks of data. This data in many cases can consist of sensitive information of the organization. If this data were to fall in the wrong hands, the organization could incur huge losses.

Security is a crucial factor in order to perform activities which require sensitive information. Not only these processes have to be secure, they have to be computationally efficient and available to each and every user. To provide security across the internet, various cryptography techniques are employed.

Thus with so many attackers trying to breach security services of the internet today, it has become crucial that we upgrade our existing security solutions. For this purpose a modified version of existing cryptography algorithm has been proposed.

3 LITERATURE SURVEY

The Following table shows the literature survey by comparing techniques propose in various references:
s

Table 1: Literature survey

No.	PAPER NAME	AUTHOR NAME	CONCLUSION
1	A Survey on Cryptography Algorithms	Omar G. Abood , Shawkat K. Guirguis	This paper gives high level overview of most popular cryptography algorithms and explains cryptography terminology and comparision of these algorithms.
2	Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data	Ako Muhamad Abdullah	Encryption and decryption using AES has been explained with detailed diagrams and examples. Key schedule of AES has also been explained in depth.
3.	A Study of Encryption Algorithms AES, DES and RSA for Security	Dr. Prerna Mahajan, Abhishek Sachdeva	This paper gives detailed comparison between asymmetric encryption algorithm and symmetric encryption algorithms. Here RSA algorithm implementation has been explained and is compared against AES and DES across parameters such as power consumption, scalability and simulation speed.

Table 2: Literature survey

No.	PAPER NAME	AUTHOR NAME	CONCLUSION
4.	A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security	R. Sivakumar, B. Balakumar, V. Arivu Pandeeswaran	DES algorithm, predecessor of AES algorithm has been explained in detail. Architecture and implementation of DES along with its short comings have been listed down.
5.	Development of modified AES algorithm for data security	Puneet Kumar, Shashi B. Rana	This paper explains in detail, architecture, methods and functioning of AES algorithm. It also extends current AES algorithm to provide mode security over the standard one.

4 PROBLEM DEFINITION AND SCOPE

4.1 Problem Definition

To understand in-depth working of AES algorithm and to implement a modified version of AES for improved security.

4.2 Scope

Although there are no practical cryptanalytical attacks against AES algorithm, AES can still be attacked using side-channel attacks. We limit our implementation to be resistant against the well known attacks. Implementation bugs, side-channel attacks, presence of malware and social engineering attacks are beyond the scope of the report.

5 CLASSIFICATION OF CRYPTOGRAPHY ALGORITHMS

5.1 Symmetric Key Cryptography

Symmetric Key Cryptography also known as Symmetric Encryption is when a common secret key is applied at both ends of a channel. In this method both the sender and the receiver have a unique key for encryption and decryption functions. During this process, data is converted to from plain text to a format which cannot be read by a person without the secret key.

Today, symmetric key cryptography is widely used across the Internet. Some examples of symmetric encryption algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). This technique is generally faster than its counterpart Asymmetric Encryption and are also more efficient, hence preferred when large data amounts of data is to be exchanged.

Modern symmetric key cryptography is further divided into Stream ciphers and Block ciphers.

5.1.1 Stream Ciphers

Stream cipher works by individually encrypting each bit. This is done by adding a key stream bit to a plain bit. Stream ciphers are of 2 types: synchronous and asynchronous stream cipher. In synchronous stream ciphers the key stream depends only on the key. In asynchronous stream ciphers the key stream is dependent on the key as well as the cipher text.

5.1.2 Block Ciphers

Block cipher encrypts an entire block of plain text bits at a time with the same key. In this encryption technique a plain text bit in a given block depends on every other plain text bit in the same block. AES has a block length of 128 bits and DES of 64 bits.

5.2 Asymmetric Key Cryptography

Asymmetric Key Cryptography is an encryption technique which is uses one key to encrypt the plain text and a different key to decrypt it. In this encryption, each party taking part in communication has 2 distinct, but related keys. One of the key is a secret key of the user and is known as Private key. The other key is distributed to the public and is freely available. This key in referred to as Public key.

These algorithms are mainly for key establishment over an insecure channel, identifying entities using using challenge-and-response protocols and digital signatures and for encrypting plain text. Some of the popular algorithms in this category include RSA and Diffie-Hellman.

6 Advanced Encryption Standards (AES)

In 1999 the US National Institute of Standards and Technology (NIST) suggested that DES be used only for legacy systems and instead triple DES (3DES) should be used for other applications. Although, that suggests 3DES is safe, it had some problems. One drawback of 3DES is its inefficiency in regards to software implementation. Software implementation of DES in inefficient and 3DES is 3 times slower than DES.

Hence, in 1997 NIST called for proposals for a new Advanced Encryption Standard (AES). In this call for proposals, some requirements had been set that every candidate had to follow. These were:

- block cipher with 128 bit block size
- three key lengths must be supported: 128, 192 and 256 bit
- security relative to other submitted algorithms
- efficiency in software and hardware

After subsequent evaluation of the entrees, an algorithm was selected. The algorithm was called Rijndael algorithm and was proposed by Joan Daemen and Vincent Rijmen. AES has been a dominant symmetric key algorithm. After its adoption, US National Security Agency (NSA) announced it has allowed AES-128 encryption for documents upto level SECRET and AES-192 or AES-256 for documents of level TOP SECRET. This implies even top government agencies believe AES to be a highly secure encryption standard.

As mentioned before, 3 key lengths must be supported by AES. Those are 128 bits, 192 bits and 256 bits. For each of these, there are different number of internal rounds.

Key Length	No. of rounds
128	10
192	12
256	14

Table 3: Key lengths and number of rounds for AES

In AES the finite field contains 256 elements and is denoted as GF(28). This field was chosen because each of the field elements can be represented by one byte. For the S-Box and MixColumn transforms, AES treats every byte of the internal data path as an element of the field GF(28) and manipulates the data by performing arithmetic in this finite field.

7 METHODOLOGY

7.1 Encryption

AES algorithm operations are divided into so-called layers. These layers manipulate 128 bits of data path at a time. The data path is also known as the state matrix. It is a column-major ordering of the bytes in 4 rows. The 3 layers in algorithm are Byte Substitution layer, Diffusion layer and Key Addition layer. The encryption starts by adding the initial key to the input value. This first round is called the initial round. Following this, 9 more iterations take place and ending with a special round. The number of rounds are dependent on key size being used. One round of AES encryption contains the following steps: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The last round of AES differs from the rest as it skips Mix Columns operation.

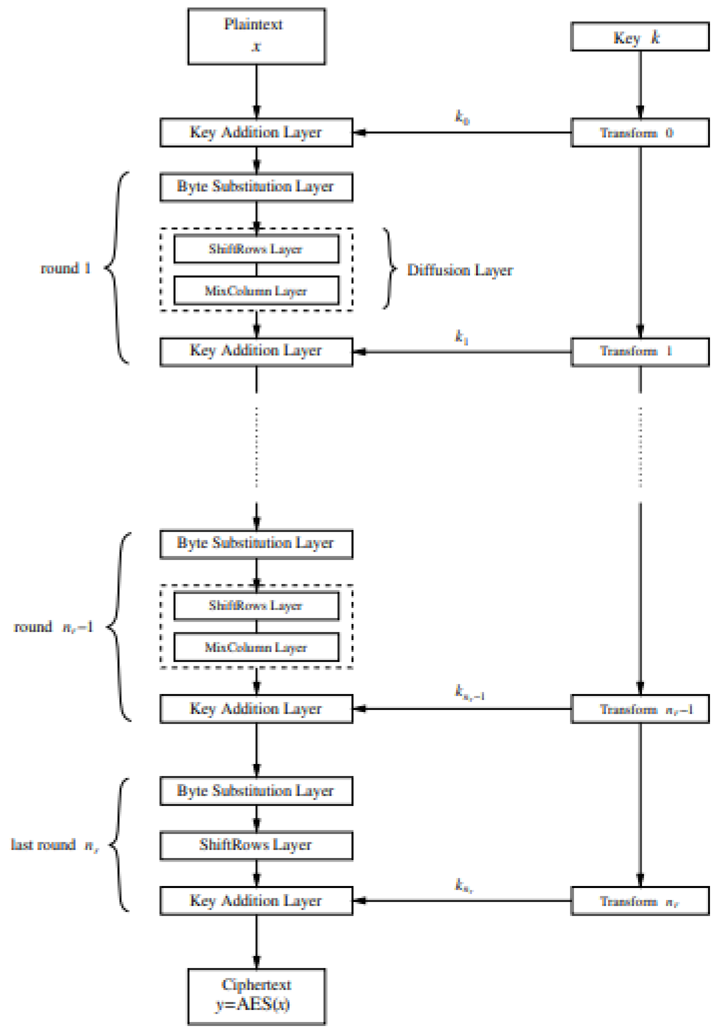


Figure 1: AES encryption block diagram

7.2 Byte Substitution Layer

In byte substitution operation, we substitute the value of each byte A_i with another byte B_i. To calculate the byte to be substituted, 2 operations are performed. The first operation is a Galois field inversion. For each input A_i, the inverse element $B_i^{'}$ is computed as $B_i^{'} = A_i^{-1}$, where both A_i and $B_i^{'}$ are elements of $GF(2^8)$ with fixed irreducible polynomial P(x) $= x^8 + x^4 + x^3 + x + 1$. The second operation is called Affine mapping. It requires each byte $B_i^{'}$ be multiplied by a constant bit-matrix then added to a constant 8-bit vector.

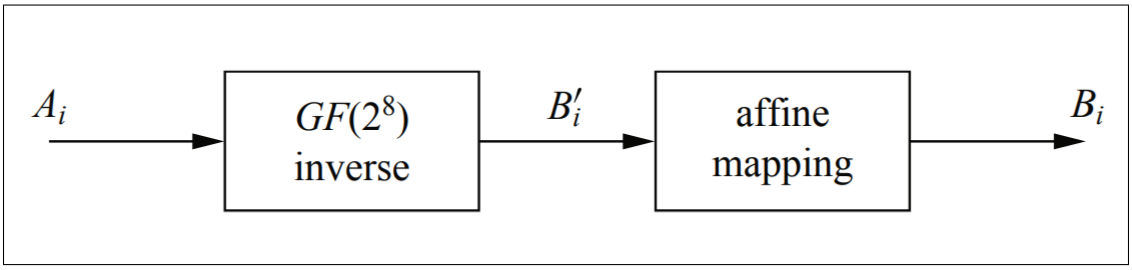


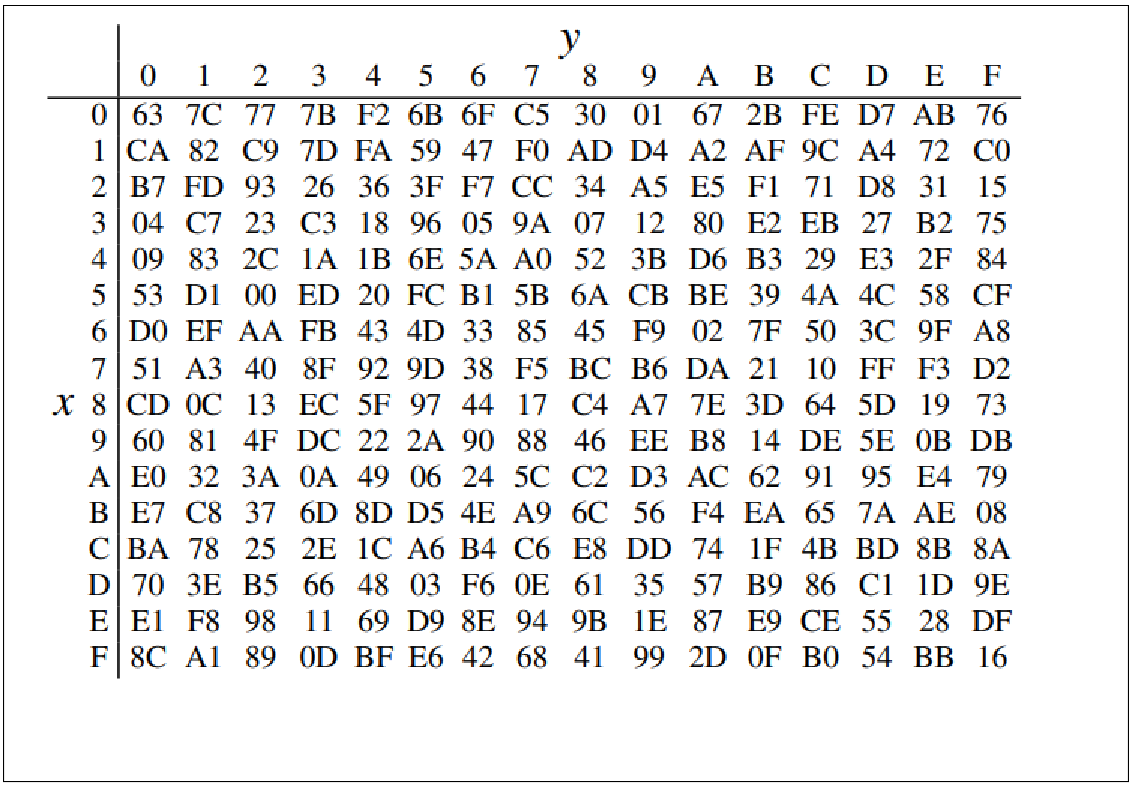
Figure 2: The two operations within the AES S-Box which computes the function $B_i = \mathrm{S}(A_i)$

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2.$$

Figure 3: Affine mapping operation

To save computation time during this process, one can calculate output for all 256 possible input elements and store it as a table in the memory. This table is called S-Box. Most software implementations of AES use the S-Box lookup table, but for hardware implementations it is sometimes advantageous to realize the S-Boxes as digital circuits which actually compute the inverse followed by the affine mapping. The S-Box is the only non-linear element of the AES algorithm and is also easy to uniquely reverse when decrypting cipher-text.

The advantage of using inversion in $GF(2^8)$ as the core function of the Byte Substitution operation is that it provides a high degree of non linearity and prevents some of the strongest known analytical attacks. The affine mapping step disrupts the standard algebraic structure of the Galois field. This helps thwart the attacks that would exploit the finite field inversion.



		y															
		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
x	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 4: AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

7.3 Diffusion Layer

In AES encryption, the diffusion layer is further divided into 2 sub-layers: Shift Rows Transformation and Mix Column Transformation. These operations are performed to spread the influence of individual bits over the entire state.

7.3.1 ShiftRows Sublayer

The ShiftRows operation transforms the state matrix by cyclically shifting the rows of the matrix. In this operation, the second row of the state matrix is shifted by one position to the left, the third row by two positions to the left and the fourth row by three positions to the left. The first row is not shifted during this operation.

B0	B4	B8	B12
B1	B5	B9	B13
B2	B6	B10	B14
B3	B7	B11	B15

Table 4: Before ShiftRows Transformation

B0	B4	B8	B12
B5	B9	B13	B1
B10	B14	B2	B6
B15	B3	B7	B11

Table 5: After ShiftRows Transformation

7.3.2 MixColumns Sublayer

This operation is used to mix all the columns in the state matrix. In this operation, since each input byte influences the other four bytes, it is a major diffusion element in AES. The input to this operation is the output of the shift row operation (B). Then, each 4-byte column is considered as a vector and multiplied by a fixed 4x4 matrix. The matrix contains constant entries. Multiplication and addition of the coefficients is done in $GF(2^8)$.

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}.$$

Figure 5: Computation of first four bytes in MixColumn Operation

7.4 Key Addition Layer

Inputs to this operation are the output of the mix column layer, i.e. the current state matrix and the 128-bit subkey. A bitwise XOR operation is performed to combine the inputs. These subkeys are derived using a key schedule. A key schedule is an operation that takes the original input key and computes the subkeys recursively. This process is typically referred to as key whitening. We require a total of 11 keys in 128-bit AES encryption. The general idea being that the total number of subkeys is equal to total rounds in AES plus one, where we require an extra key for key whitening in the first key addition layer.

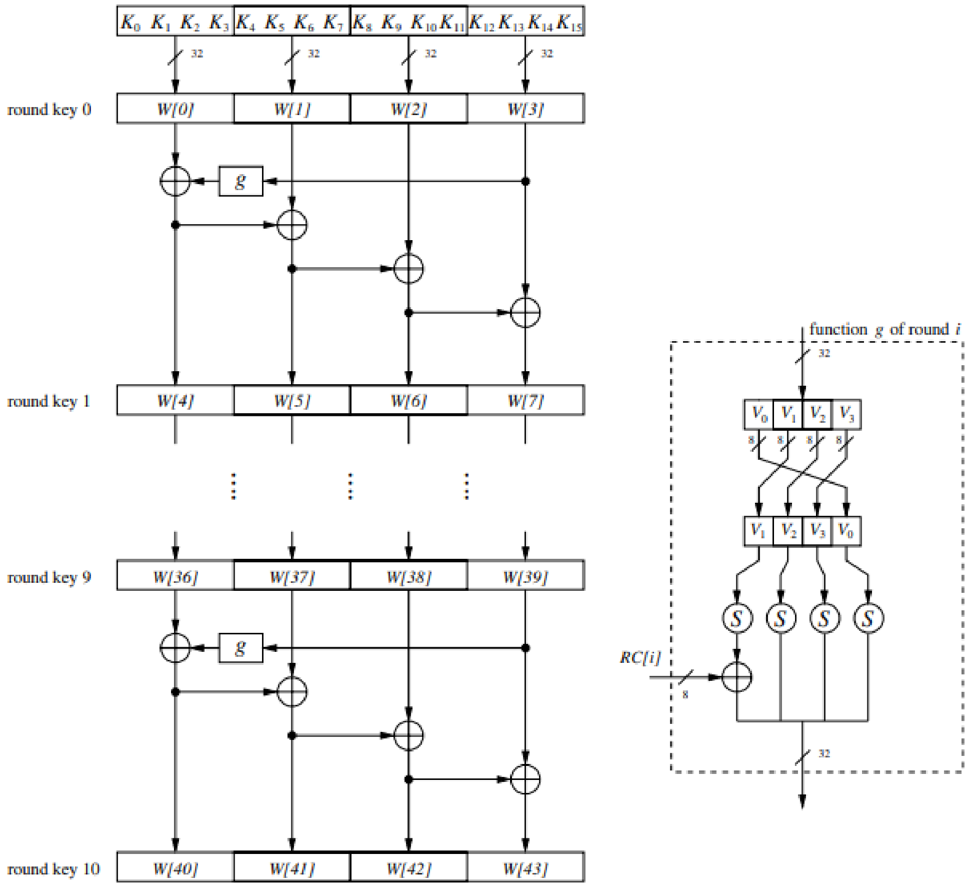


Figure 6: Key schedule in AES for 128-bit key size

Subkeys are stored in a key expansion array W that consists of words where 1 word is equal to 32 bits. For 128 bit key length, 10 rounds are performed during encryption which generates a total of 11 subkeys. These are stored in a key expansion array as W[0] to W[43]. The subkey k_i is calculated using k_{i-1} by first rotating its input bytes, performing byte-wise S-Box substitution and then adding round coefficient RC to it. These combined operations have 2 purposes: adding non-linearity to the key schedule and thwarting certain block cipher attacks.

Formula for computing leftmost word of subkey W[4i] is given as:

$$\mathrm{W[4i] = W[4(i1)]+g(W[4i1])}$$

7.5 Decryption

The decryption process involves operations that are inverse of operations performed during the encryption process. These are referred to as Inverse Byte Substitution, Inverse Shift Row and Inverse Shift Row and so on. These operations are fairly similar to their corresponding encryption counterparts. Decryption also involves a reversed key schedule.

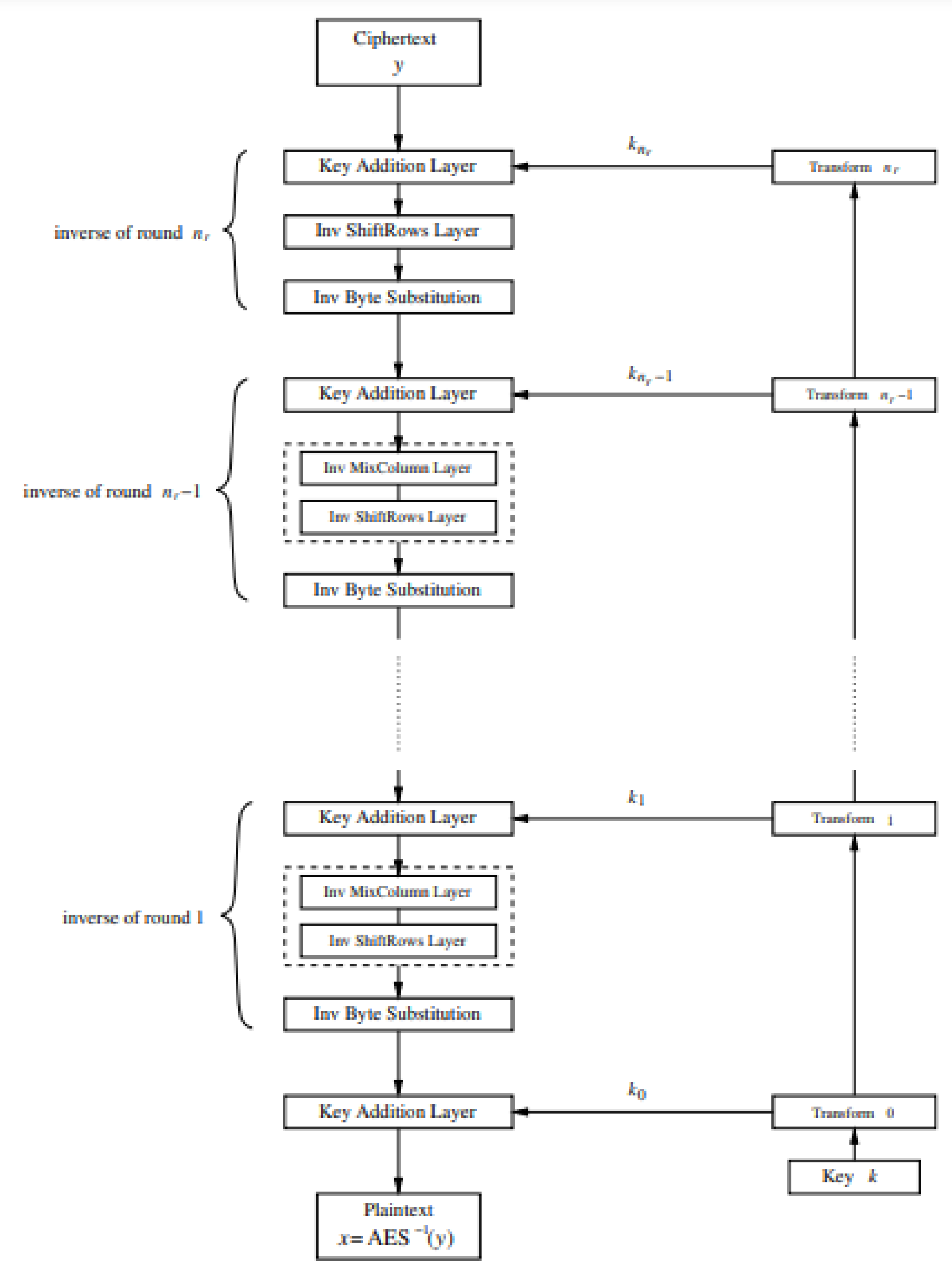


Figure 7: AES decryption block diagram

Since last encryption iteration skips Mix Column operation, first iteration of decryption skips corresponding Inverse Mix Column operation.

7.5.1 Inverse MixColumn Sublayer

Decryption of ciphertext proceeds in opposite direction of encryption process. After the addition of the subkey, the inverse MixColumn step is applied to the state. Note that this was step during encryption process. For this, the inverse of matrix used during MixColumn operation is used. Multiplication and addition of the coefficients is done in $GF(2^8)$.

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

Figure 8: Computation in Inverse MixColumn Operation

7.5.2 Inverse ShiftRows Sublayer

In order to reverse the ShiftRows operation of the encryption algorithm, we must shift the rows of the state matrix in the opposite direction. In this operation, the second row of the state matrix is shifted by one position to the right, the third row by two positions to the right and the fourth row by three positions to the right. The first row is not shifted.

B0	B4	B8	B12
B1	B5	B9	B13
B2	B6	B10	B14
B3	B7	B11	B15

Table 6: Before Inverse ShiftRows Transformation

B0	B4	B8	B12
B13	B1	B5	B9
B10	B14	B2	B6
B7	B11	B15	B3

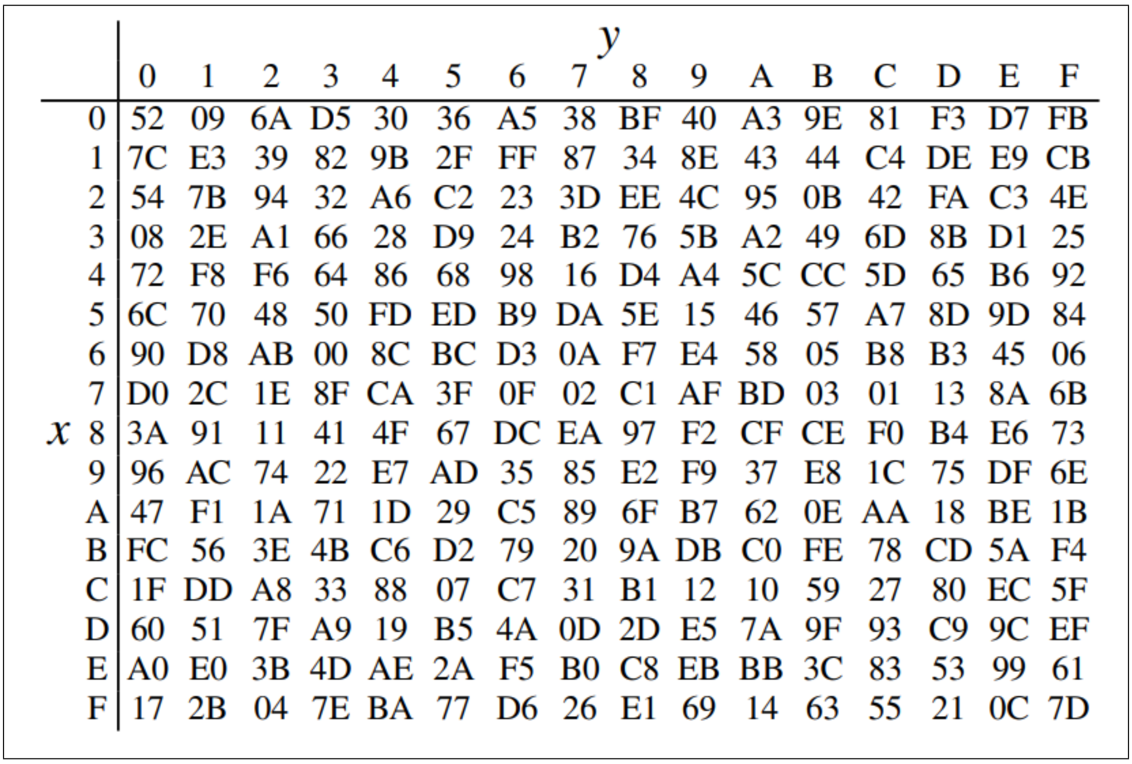
Table 7: After Inverse ShiftRows Transformation

7.6 Inverse Byte Substitution Layer

During decryption process, we use an inverse S-Box to get inverse of each byte. This is possible due to S-Box being bijective i.e. it has one-to-one mapping. Inverse of an input byte is calculated as:

$$A_i = S^{-1}(B_i) = S^{-1}(S(A_i))$$

where A_i and B_i are elements of the state matrix.



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

Figure 9: Inverse AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

8 MODIFIED AES

8.1 Methodology

When we see AES algorithm, we usually find three different key sizes: 128, 192 and 256 bits. These sizes were part of requirements laid down by NIST for AES. But Rijndael algorithm works with other key sizes as well. For this proposed model, we will choose key size as 320 bits. The number of rounds for this key are increased from 10 to 16. This configuration improves the security of encryption and makes it harder for attackers to decrypt.

For encryption, we follow the steps used in standard AES. We start by performing Byte Substitution operation followed by Diffusion operation and ending with Key Addition Layer. The model consists of 16 iterations instead of 10, but similar to standard AES, we skip MixColumn operation.

Decryption is the process of converting ciphertext to plaintext using a secret key. Our model follows standard AES decryption process. This process includes AddRoundKey, InvMixColumns, InvShiftRows and InvSubBytes operations. Note that these operations are carried out in reverse order of encryption process.

8.1.1 Key Generation

For this model, we will use Polybius square for generating the initial secret key. Polybius square is 6x6 matrix containing alphabets and numerals without repetition.

-	0	1	2	3	4	5
0	A	B	D	E	Y	4
1	E	F	G	H	Z	5
2	I	J	K	L	0	6
3	M	N	O	P	1	7
4	Q	R	S	T	2	8
5	U	V	W	X	3	9

Table 8: Polybius Square used for generating keys

9 RESULTS

The encryption computational time is defined as the time required by algorithm to completely convert an input file text from plaintext format to ciphertext format The encryption time is used to calculate the throughput of an encryption algorithm. We performed encryption of files of various sizes using our model, calculated encryption time and compared it against other algorithms, namely DES, 3DES and AES.

Input file size (kb)	DES	3DES	AES	Proposed
15	20	22	21	23
42	63	71	60	65
90	134	142	129	137
157	272	289	253	263
303	451	479	439	471
412	654	691	612	684

Table 9: Encryption execution time for different file size

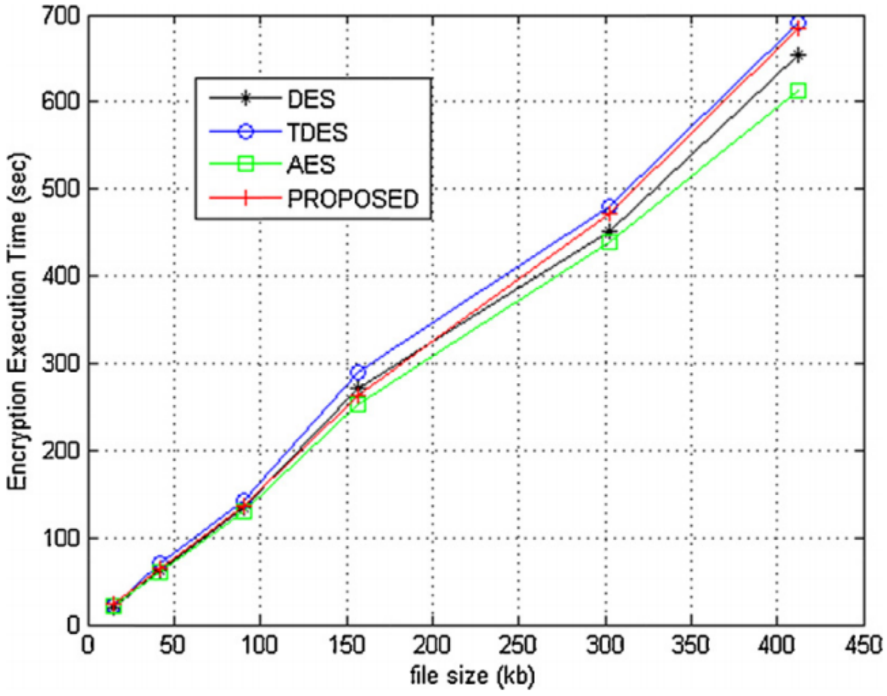


Figure 10: Encryption execution time of different file sizes

10 CONCLUSION

Encryption is an important tool to keep sensitive data from falling into the wrong hands. For that purpose, we discussed cryptography, its principles, classification and its uses. We also learned the in-depth working of AES and studied its implementation. Then, we proposed an AES based encryption model which has 16 rounds as opposed to 10 in standard AES. This model is proven to be more resistant to attackers. With increase in number of rounds, it becomes significantly difficult for an attacker to break the system, thus improving the overall security.

References

[1] Omar G. Abood, Shawkat K. Guirguis, ”A Survey on Cryptography Algorithms”, International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018

[2] Ako Muhamad Abdullah “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”, Publication Date: June 16, 2017

[3] 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

[4] R. Sivakumar, B. Balakumar, V. Arivu Pandeeswaran “A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security” International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 04 — Apr-2018

[5] Puneet Kumar, Shashi B. Rana, ”Development of modified AES Algorithm for Data Security”, Publication Date: 24 November 2015

attach your review and visit log here......

attach plagiarism report here.....