

AES and Confidentiality from the Inside Out

Zilhaz Jalal Chowdhury, Davar Pishva, G. G. D. Nishantha

Ritsumeikan Asia Pacific University, Beppu City, Oita Prefecture, Japan

zilhch06@apu.ac.jp, dpishva@apu.ac.jp, gamagelk@apu.ac.jp

Abstract— Information Confidentiality has a prominent significance in the study of ethics, law and most recently in Information Systems. With the evolution of human intelligence, the art of cryptography has become more complex in order to make information more secure. There are arrays of encryption systems those are being deployed in the world of Information Systems by various organizations. However, for the wider use, we need to adapt to a particular encryption method and standard. This paper is intended to be an easy to follow tutorial on the principles of Information Security, Information Confidentiality and their underlying standards. This paper also thoroughly explains the inner working of an encryption standard known as Advanced Encryption Standard or AES.

Keywords— Information Systems, Information Confidentiality, Symmetric Encryption, AES, Rijndael Cipher

I. INTRODUCTION

Digital information has become a social infrastructure and with the expansion of the Internet, network infrastructure has become an indispensable part of social life and industrial activities for mankind. For various reasons, however, today's networks are vulnerable to numerous risks, such as information leakage and data corruption. As such Information Security has become vital for our modern life.

In the old days when everything was mechanical, people were mostly concerned with physical security. However, with our present technological progress, one can gain access to just about anything by breaking through Information Security gates. In this era of technology, financial institutions such as banks, perform their transactions and other highly important data exchange through computers and networks. This is where we can easily understand the importance of Information Security.

The basics of Information Security lies within the CIA triad; where C stands for Confidentiality, I for Integrity, and A for Availability. Confidentiality is not allowing the information to be accessed by people that are not allowed to. Integrity is restricting people from unauthorized modification of the information. Finally, Availability is the ability to get to the information when needed.

By following these main guidelines, Information Security continues to develop and improve to protect information from going to places where it shouldn't be. The National Institute of Standards and Technology (NIST) is a measurement

standards laboratory of U.S federal agency. In order to establish Information Security, NIST sets the encryption standards under Federal Information Processing Standards (FIPS). In 26th November, 2001 NIST announced the Advanced Encryption Standard (AES) in FIPS 197 [1]. AES adopted the Rijndael Cipher, which was proposed by Joan Daemen and Vincent Rijmen as the algorithm for AES.

AES is a 128 bit block cipher symmetric encryption system having sufficient key length of 128/192/256 bit [1]. Because of its secured algorithm and sufficient key length, AES provides satisfactory level of data confidentiality. AES algorithm is widely being used in the field of Information Technology for various security purposes.

II. INFORMATION CONFIDENTIALITY

Information means a set of data in an understandable form which contains some message. In the study of Information Systems (IS), Information Confidentiality refers to the protection of a set of data or information from any unauthorized access. Data confidentiality and privacy are the foremost concerns in Information Confidentiality [3]. In the present age of networking (most significantly the Internet), in a specific network, a certain piece of information is literally available everywhere within the network. Hence, Information Confidentiality becomes a serious issue, as taking any chance may result in information being leaked to unauthorized parties.

III. CRYPTOGRAPHY & SYMMETRIC ENCRYPTION

Information Security has long been equated with cryptography, whose historical connections with military applications and mathematical depth limited its exposure to the general public. As a result, most people had until recently very little knowledge and awareness of the ins and outs of Information Security. As such, this paper thoroughly explains the inner workings of Advanced Encryption Standard in an easy to follow manner.

Cryptography is an age old tool used for ensuring Information Confidentiality. In cryptography, during data transfer, the information is transformed into apparently meaningless data using certain encryption method, in order to protect the actual information from third party attack.

In a symmetric encryption method, there are five ingredients: Plain-text, Encryption Algorithm, Cipher-Key, Cipher-text and Decryption Algorithm. Both sender and receiver share the same secret key for encrypting and decrypting data [2].

IV. NIST AND AES

In regards to Information Security, institutions and organizations like the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are greatly involved in establishing security standards and protecting important information of the US government. In 2001, NIST announced the selected encryption standard after viewing all other presented encryption algorithms. In the process, AES was decided on the Rijndael Cipher, and will be explained in detail in this paper. This meant that the Rijndael algorithm would be the standard encryption method for the US Federal Administration [8]. Before describing the Rijndael Cipher in detail, we need to make sure that underlying principles of the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are understood.

The DES is a cipher, specifically a block cipher, which was used as an encryption standard in the past and uses a 56-bit key for symmetric encryption. In present days, the DES is mocked and in fact cannot be used anymore due to its lack of security. However, in the past when computing speed was slow, it was often used. AES is the present day encryption standard, which is far more secure than the DES. Unlike the DES, the AES has a fixed block size of 128 bits, and key sizes of 128, 192 and 256 bits. This ultimately provides far superior security [1].

V. IMPLEMENTATION OF AES

AES became effective from 26th May, 2002 [1]. Since then, the AES algorithm has been being implemented in software, hardware, firmware and various combinations of those. Up to 25th August, 1156 projects undertaken by numerous companies and organizations received AES validation for implementing AES in their respective programs [10]. This list includes well-known companies such as Motorola, Cisco Systems, Red Hat, Sun Microsystems and so on. AES validation test is performed in Cryptographic and Security Testing (CST) laboratories which are accredited by National Voluntary Laboratory Accreditation Program (NVLAP).

AES validation is certified under the Advanced Encryption Standard Algorithm Validation Suite (AESAVS). The AESAVS performs automated testing on Implementations Under Test (IUTs) in order to ensure proper implementation of the algorithm. In the validation process, the application system that implements AES has to go through 3 tests – 1. The Known Answer Test (KAT), 2. The Multi-Block Message Test (MMT), 3. Monte Carlo Test (MCT). After passing these 3 tests, the system has to claim conformance to the Advanced Encryption Standard as specified in Federal Information Standards Publications (FIPS)197 – Advanced Encryption Standard [2].

VI. RIJNDAEL CIPHER

On 12th September, 1997 NIST called for a new algorithm to be used for Advanced Encryption Standard (AES) and to replace Data Encryption Standard (DES). The given

requirements were – it had to be a block cipher, supporting a block size of 128 bits and having key sizes of 128, 192 and 256 bits. After the call, 15 algorithms were submitted in the next 9 months. In August 1999, NIST announced 5 finalists for the AES algorithm. They were – MARS, RC6, Rijndael, Serpent and Twofish. The winner was selected in AES2 conference from voting of the respected community. Rijndael won the selection process by having 86 positives and 10 negatives. The complete result is shown in Table 1.

Table1. Voting Result of AES2 Conference (Source: Wikipedia Page on Advanced Encryption Standard - AES [6])

Algorithm	Positive	Negative
Rijndael	86	10
Serpent	59	7
Twofish	31	21
RC6	23	37
MARS	13	83

In April of 2000, in AES3 conference, the competitors made presentation on their proposed algorithms to explain why their respective algorithm should be chosen. Finally in November 26, 2001 NIST announced that the Rijndael Cipher would be adopted as AES and it was approved under FIPS PUB 197 [6].

VII. WORKING MECHANISM OF RIJNDAEL CIPHER

By following the basic process of encryption method, AES simply uses encryption key to convert a given input (Plaintext) into a cipher-text. However, during encryption-decryption process, AES system goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text. In initial round, the plaintext is simply XORed with Cipher-key. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key.

In the final (10th) round, there is no Mix-column transformation [3]. Figure 1 shows the overall process and the following sections explain the details of AES encryption using a 128-bit key.

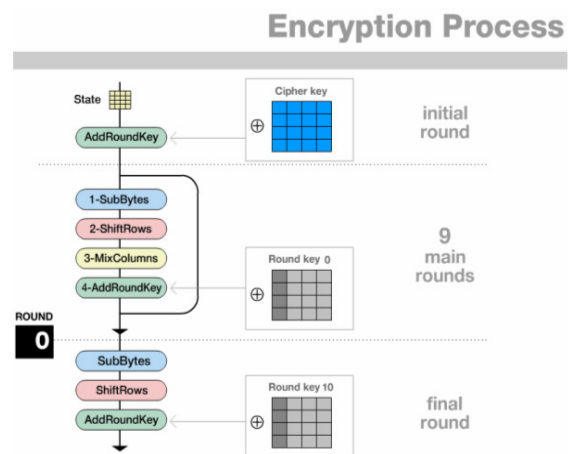


Figure 1. Encryption Process of AES

A. Sub-Byte Transformation

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael S-box. As can be seen from Figure 2, the S-box follows Hexadecimal numbering system; hence it has 16 rows and 16 columns (From Hexadecimal 0 to f or Decimal 0 to 15).

For instance, if we want to transform Hexadecimal 19, we will look into the row of S-box where we get the first digit 1 (1x Row in Figure 2), then in that particular row we search for the cell which intersects with the column containing 9 (i.e. x9 Column in Figure 2). In the S-box, this particular cell is Hexadecimal d4. This is how it can transform the bytes of entire block into another state using the S-box. The S-box is constructed using the functionalities of finite field mathematics. [3]

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 2. S-box for Sub-byte Transformation.

B. Shift-Rows Transformation

In AES, each of the blocks has 4 rows and 4 columns. In this transformation step, the 1st row of the block is kept as it is. Then for the 2nd row, 1 byte circular left shift is performed. That means after the transformation, the 1st cell (from left) of the 2nd row goes into 4th cell, 2nd cell goes into 1st cell, 3rd goes into 2nd and 4th goes into 3rd. In this manner, for the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively. [4] An example of Shift-rows transformation is given in Figure 3:

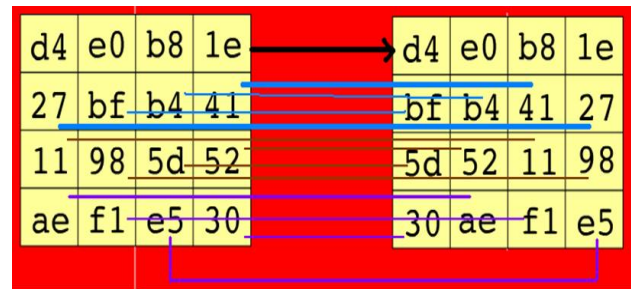


Figure 3. Shift-rows transformation.

The example shown in Figure 3, implements the following 4 steps of the transformation:

- The 1st row is not altered. (the cells of 1st row remain same in the right matrix as it was in left matrix)
- For the 2nd row, a 1-byte circular left shift is performed. (27, bf, b4 and 41 transformed into bf, b4, 41 and 27 respectively)
- For the 3rd row, a 2-byte circular left shift is performed. (11, 98, 5d and 52 transformed into 5d, 52, 11 and 98 respectively)
- For the 4th row, a 3-byte circular left shift is performed. (ae, f1, e5 and 30 transformed into 30, ae, f1 and e5 respectively)

C. Mix-Columns Transformation

According to Rijndael specification, each column is treated as a four-term polynomial over GF (2⁸) [8]. In this transformation, each column is multiplied by modulo $x^4 + 1$ with a fixed polynomial c(x), which is –

$$c(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\} \quad (1)$$

In other words, Mix-Columns step is performed by multiplying a coordinate vector of four numbers in Rijndael's Galois field by a particular circulant MDS matrix. It is to be mentioned that, calculation in this transformation is done in Rijndael's Galois field. The addition operation here is actually an Exclusive OR (XOR) operation, and multiplication is a complicated operation [5], [6]. The example given below will clarify this process. Let's perform the Mix-columns transformation of the right side matrix in Figure 3 which we derived by performing the Shift-rows transformation.

As shown in Figure 4, at first we separate the target column from the matrix and we multiply it using a fixed circulant MDS Matrix.

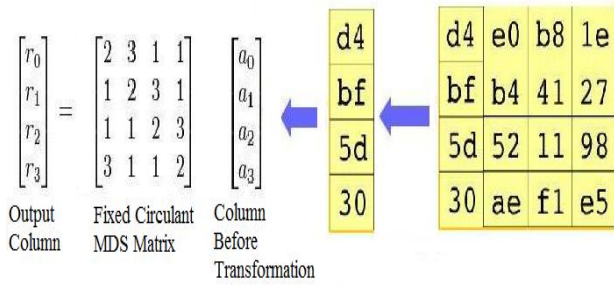


Figure 4. Mix-Columns Transformation (1).

We can represent this matrix multiplication with equations given below:

$$r_0 = 2a_0 + a_3 + a_2 + 3a_1 \quad (2)$$

$$r_1 = 2a_1 + a_0 + a_3 + 3a_2 \quad (3)$$

$$r_2 = 2a_2 + a_1 + a_0 + 3a_3 \quad (4)$$

$$r_3 = 2a_3 + a_2 + a_1 + 3a_0 \quad (5)$$

Now let's put the respective values of the variables in the above equations.

$$r_0 = 2a_0 + a_3 + a_2 + 3a_1 = (2*d4) + 30 + 5d + (3*bf) \quad (6)$$

$$r_1 = 2a_1 + a_0 + a_3 + 3a_2 = (2*bf) + d4 + 30 + (3*5d) \quad (7)$$

$$r_2 = 2a_2 + a_1 + a_0 + 3a_3 = (2*5d) + bf + d4 + (3*30) \quad (8)$$

$$r_3 = 2a_3 + a_2 + a_1 + 3a_0 = (2*30) + 5d + bf + (3*d4) \quad (9)$$

$$[a_0 = d4, a_1 = bf, a_2 = 5d, a_3 = 30]$$

The values are given in Hexadecimal numbering system. Before performing the arithmetic operation we have to convert the values in Binary numbering system for the comfort of calculation. In below, we convert the input values of r_0 into Binary numbering system.

$$\begin{aligned} r_0 &= (2*d4) + 30 + 5d + (3*bf) \text{ [Hexadecimal values]} \\ &= (10*110 \ 10 \ 100) + 110 \ 000 + 10 \ 111 \ 01 + \\ &\quad (11*101 \ 111 \ 11) \text{ [Binary Values]} \end{aligned} \quad (10)$$

Now, we have to perform the arithmetic operations according to Finite field/Galois field arithmetic system. The rules for addition and multiplication in finite field arithmetic are:

- Addition: XOR Operation
- Multiplication: Complicated Operation

Complicated operation means while doing arithmetic multiplication we need to perform XOR operation instead of normal addition. And, if the final result has more than 8 bits, the extra bits are not simply discarded. Instead, they're cancelled out by XORing the binary 9-bit string 100011011 with the final result (shifted right if necessary). The multiplication, performed for output r_0 will clarify the issue of complicated operation –

$$\begin{array}{r} 11010100 \\ * \quad 10 \\ \hline 00000000 \\ 11010100x \text{ (XOR)} \\ \hline 110101000 \text{ (More than 8 bits!)} \\ 100011011 \text{ (XOR)} \\ \hline 10110011 \end{array} \quad \begin{array}{r} 10111111 \\ * \quad 11 \\ \hline 10111111 \\ 10111111x \text{ (XOR)} \\ \hline 111000001 \\ 100011011 \text{ (XOR)} \\ \hline 011011010 \end{array}$$

Now, we will perform the addition which is actually XOR operation for finishing the calculation of “(10)”

$$r_0 = 10110011 \text{ XOR } 110000 \text{ XOR } 1011101 \text{ XOR}$$

$$011011010$$

$$= 100 \text{ (Binary)}$$

$$= 04 \text{ (Hexadecimal)}$$

In similar manner, we can derive r_1 , r_2 and r_3 . After performing the same operation for all 4 columns, we will come up with the following matrix shown in Figure 5:

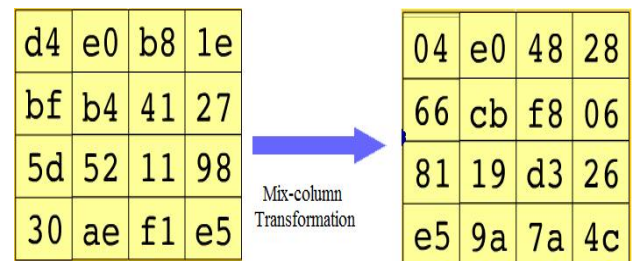


Figure 5. Mixed Column Transformation (2).

D. Add Round Key

In this step, the outcome state from Mix-columns transformation is XORed with a Sub-key or Round-key. Sub-key for each round is derived from the original Cipher-key following Rijndael Key Schedule which is also known as Key Expansion. The procedure for obtaining round key is described in the following paragraph.

E. Key Schedule or Key Expansion

In initial round, the input is simply XORed with Cipher-key. However, from Round 1, for each of the rounds a particular Sub-key is used for ‘Add round key’ step. The Sub-keys are generated from the original Cipher-key, following a particular method which is known as key schedule or key expansion.

As shown in Figure 6, the matrix in blue color is our original Cipher-key. For generating the Sub-key for Round 1, first of all we perform Sub-bytes transformation with the 4th column (from left) W_{i-1} of the original Cipher-key. (Sub-bytes Transformation is already discussed above). After performing the Sub-bytes transformation, we perform 1-Byte Circular Left Shift Operation. At this point, we XOR the obtained output with the 1st column (from left) W_{i-4} of the Cipher-key (Let's call this output as **Output₁**). For the next step, we take the 1st

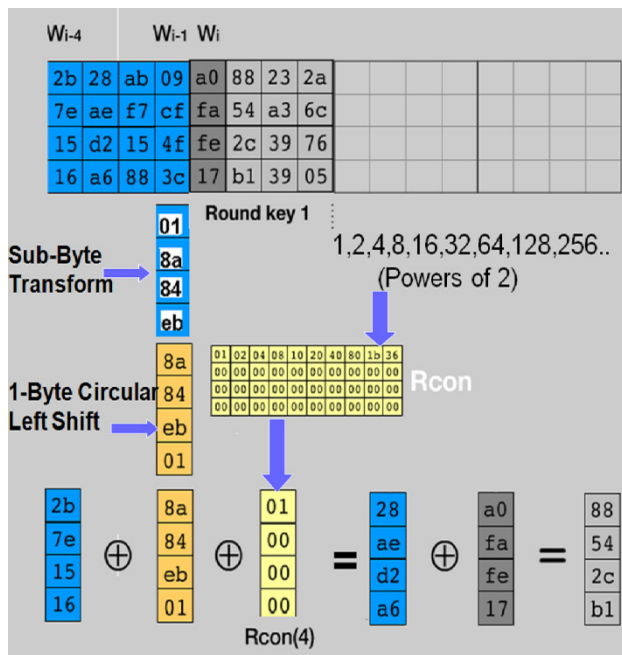


Figure 6. Key Schedule.

column from given Rcon table. Rcon table is a matrix of 4-rows which is constructed using exponentiation of 2 to a user-specified value. In our case, we have to generate 10 round keys for 10 rounds hence we use first 10 column of the Rcon table. Back to our 1st round key construction, after selecting the specific column from Rcon table, we XOR this column with our immediate previous output, which we defined as **Output₁**.

The outcome at this stage is the 1st column (W_i) of the Round Key 1 matrix. For achieving the 2nd column or W_{i+1} of the Round Key 1, we simply XOR W_{i-3} with W_i . In similar manner we can obtain W_{i+2} and W_{i+3} . For constructing, Round 2 Sub-key, we use the 2nd column of Rcon table. That's how we can construct 10 Sub-keys for all 10 rounds.

F. Decryption

Decryption method of AES is just the inverse of its encryption system. However, in the decryption process, the input is the Cipher-text which was obtained during the AES encryption process. Similar to encryption process, decryption starts with XORing Cipher-text with the Cipher-key. Then for next 9 rounds we have to go through 4 step transformations. The 4 transformations of AES Decryption are:

- Inverse Sub-bytes Transformation
- Inverse Shift-rows Transformation
- Inverse Mix-columns Transformation

- Inverse Add round key Transformation

In the final or 10th round, Inverse Add round key transformation is not performed. For inverse Sub-bytes transformation, a separate inverse S-box is available. And for inverse Sub-bytes transformation a different fixed circulant MDS matrix is used. As it was mentioned earlier, for decrypting a particular Cipher-text, the receiver has to use same cipher key which was used for encryption [3].

VIII. CONCLUSIONS

This paper has thus explained the principle of Information Security, Information Confidentiality, their underlying standards and the inner workings of AES in an easy to follow manner. Because of AES' dependable security, in 2003 US government announced that AES can be used to protect US government classified information [6]. So far there has been no evidence of any major attack on AES. Despite some academic and minor attacks (e.g. Side-channel attack) against AES, there has been no significant security loss or damage. AES has been performing a great task of securing information since its introduction in the information systems. Nevertheless, in parallel with the rapid pace of technology improvement, higher level of security is also required when making use of most advanced future technologies. At any rate, AES despite addressing present day security needs could also be used as a good model for future security standards.

ACKNOWLEDGMENT

Special thanks to Saif Al Mannaei for his contribution with information regarding NIST and importance of information security.

REFERENCES

- [1] Official NIST publication on AES: <http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [2] Official NIST document on AES/AVS: <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>.
- [3] STALLINGS, William & BROWN, Lawrie (2008); "Computer Security: Principles & Practice.", Pearson Prentice Hall, 2008.
- [4] AES Rijndael-Animation, Rijndael-Inspector: www.cryptool.org.
- [5] The Advanced Encryption Standard: <http://www.quadibloc.com/crypto/co040401.htm>.
- [6] Wikipedia page on AES: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Security.
- [7] Rijndael S-Box Figure: <http://edipermadi.files.wordpress.com/2008/03/sbox.png>.
- [8] DAEMEN, Joan & RIJMEN, Vincent, "The Design of Rijndael: AES – The Advanced Encryption Standard", Springer, 2002.
- [9] www.cryptool.org.
- [10] Advanced Encryption Standard Algorithm Validation List: <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>.
- [11] M. Morris Mano, Michael D. Ciletti, "Digital Design", Pearson/Prentice Hall, 2007.