Analysis on AES Encryption Standard and Safety

Zhengyi Lu[1,*]
[1]Shanghai Jiao tong University, Joint Institute, Shanghai, China
windlll@sjtu.edu.cn
[*]Corresponding author email: windlll@sjtu.edu.cn

Abstract

AES has replaced DES to become a widely-used encryption algorithm since 2000s. This paper may insight the basic theory of AES and safety analysis. In this paper, the whole process of AES encryption is described. The procedures of plaintext processing firstly, substituting bytes secondly, then shifting rows, mixing columns and adding round keys. AES-128 is taken as the study example in this paper to introduce the features and operating steps of AES. The construction and use of a simple S-box is also mentioned to help understand the procedure of substituting bytes. Safety analysis of AES is also taken into consideration to test AES's resistance against different kinds of attacks. The results show that AES is free from brute force attack with time security analysis. AES with 128 or more bits of key length can resist square attacks according to reviews on research. A way of differential cryptanalysis attack with concrete operating steps is introduced as a potential attack method against AES encryption standard. The paper also casts view on an improved AES algorithm to increase efficiency and security proposed by other researches.

Keywords: Encryption process; Transformation; Safety analysis.

1. INTRODUCTION

Cryptography is a common technology in information industry. It means methods of transforming significant data into meaningless and messy codes with encryption functions to hide the data from attackers during transmitting procedure. After reaching the target receiver, the massy codes can be recovered with specific decryption functions. To be more vivid, encryption is like an excellent combination of art and science with the function of transferring plain and readable information into un-readable format [1]. Cryptography has shown great value in various industries including password protection, bitcoin mining, bitcoin transaction and so on. Cryptography has many subs and AES is one of the most practical and widely-used encryption algorithms.

1.1 Background

The Advanced Encryption Standard is called AES for short. Before it appeared, Data Encryption Standard, which is shorted as DES, was used by programmers for encryption on the world scale. DES is a symmetric cryptosystem developed by IBM in 1972. In 1977, it was identified as the Federal Data Processing Standard by the Federal Government of the United States and authorized to be used in non-secret government communications. However, DES only has a key length of 64 bits. It began to fail to meet the security requirements of encryption algorithm over time.

In 1990s, NIST started to collect for AES scheme to replace DES. The requirements for this standard were that it should be faster than Triple DES and should have at least the same security with Triple DES. Another request is that the winner should be able to resist both practical attacks and theoretical attacks with academic cryptanalysis methods [2]. During that period, Rijndael algorithm, which is the predecessors of AES, is created by Joan Daemen and Vincent Rijmen. For the design of Rijndael algorithm, it has principles of pursuing simplicity, focusing on performance and using well-understood components [2].

By 1999, five algorithms had been included as final alternative solutions. They are MARS, RC6, Rijndael, Serpent and Twofish. In 2000, Rijndael algorithm won in the competition with other algorithms and became the final standard in early 2000s. In US, NIST withdrew DES in 2004, which is a significant symbol for the recognition of AES. Internationally, AES has been included in ISO, IETF and IEEE standard [2].

1.2 Features

AES is a symmetric encryption algorithm. It means that its encryption key and decryption key have the same length. The decryption process of AES is the inverse of its encryption process. As a symmetric encryption algorithm, AES has

Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022),
edited by Xianye Ben, Proc. of SPIE Vol. 12462, 1246215 · © The Authors. Published under a
Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2662564

advantages of relatively light computation requirements, fast encryption speed and high efficiency during the process of encryption.

What's more, AES is a block cipher algorithm in structure, which represents that the block length and key length are independent and the block length is fixed. Moreover, the plaintext and ciphertext are texts with the same bit length. For AES, it has a fixed block length of 128 bits. Its key length is not fixed and can be adjusted according to different demands. It can be 128 bits, 192bits and 256bits, which correspond to 10, 12 and 14 rounds of encryption.

2. PROCEDURE ANALYSIS AND PRINCIPLE

2.1 Overall Process

For more detailed study, the research contributes insight into AES-128, which has a key length of 128 bits and 10rounds of encryption. It contains universal procedures of plaintext processing, and four procedures for each round. A diagram for a typical 10 rounds encryption is shown in Figure 1.

As shown in this diagram, the origin message is blocked and has a length of 128 bits. The zero round only contains the operation of adding round key. During the next 9 rounds of encryption, each round has procedures of substituting bytes firstly, shifting rows secondly, then mixing columns and adding round keys. However, for the last round, the operation of mixing columns is removed.

Figure 1. Procedures

2.2 Plaintext Processing

Before rounds, operations should be done to transform plaintext to a matrix. The matrix is 4×4 bytes. The plaintext is fixed as 128 bits for one process. One letter takes up one byte (8 bits) of space. For example, Plaintext = "abcdefghijklmnop". The matrix is P_0, P_1, …, P_{15} from top to bottom and left to right. Then "a" corresponds to "P_0", and "p" corresponds to "P_{15}". Figure 2 provides a visualization of the concrete operation.

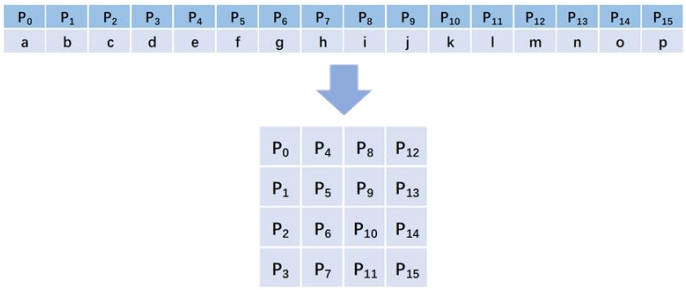

Figure 2. Text Processing

2.3 Substitute Bytes

After entering rounds, operation of substituting bytes should be first completed. A S-Box, which is constructed complicatedly, is used. It is a 16×16matrix. A S-box is shown below in Figure 3.

For example, for an 8-bit to 8-bit mapping, a = $a_0a_1a_2a_3a_4a_5a_6a_7$. Then the output should be S[$a_0a_1a_2a_3$] [$a_4a_5a_6a_7$]. For this S-Box, if a = 00000000_B, then the output should be S[0][0]=63_H.

x \ 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
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 3. S-box [3]

It comes to S-box and its structure. S-box provides mix functions for block key cipher and also serves as defender for different kinds of attacks. For AES-128, S-box is used for 160 times during processing and encryption. In consequence, the security of S-box is strongly associated to the safety of the whole cipher system [4].

To ensure the security of the whole system and make it able to withstand different attacks, the design of S-box should take differential cryptanalysis analysis and linear analysis into consideration. The process of designing one specific S-box is kept secret and should match several requirements. The S-box should be reversible to deal with encryption and decryption demands and should have complexity based on GF (2^8) [5]. GF (2^8) has a field of 256 elements and it is constructed according to the polynomial that $f(x) = x_8+x_4+x_3+x+1$ is irreducible in the ring $Z_2[x]$ [6]. An algebraic interpretation of a S-box is started with one byte (eight bits) with each bit representing 0 or 1. Its S-box entry can be found applying GF (2^8) and computing algebraically [6].

2.4 Shift Rows

This procedure is a transformation of bytes in a 4×4 matrix (the data matrix). The first row on the top remains unchanged. The second row is shifted left for 8 bits (one byte) circularly. The third row is shifted left for two bytes circularly. The last row on the bottom is shifted left for three bytes circularly. The initial matrix and the result matrix obtained after row-shifts are shown in Figure 4.

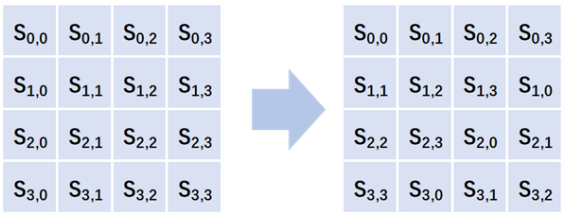

Figure 4. Shift Rows

2.5 Mix Columns

In this procedure, a left multiplication is applied by multiplying data matrix with a fixed mix matrix. The basic requirements of mixing columns are as follows. The process should be reversible and symmetric [7]. It should also on GF (2^8). A more specific process is shown in Figure 5 as below.

Different from common matrix multiplication, the calculation is based on GF (2^8) and the XOR calculation is applied.

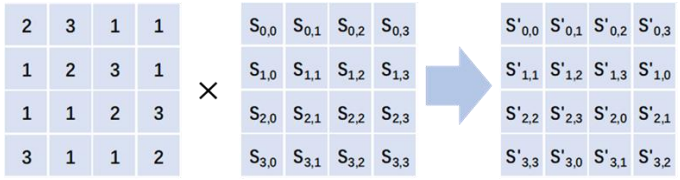

Figure 5. Mix Columns

2.6 Add Round Keys

For AES-128, key length is equal to 128 bits. By applying Key-generating function, 44 elements can be generated with each having a length of 4: W[0], W[1],….,W[43].

Among them, the elements from W[0] to W[3] are the original key. Others are divided into 10 groups and serve as round keys for 10rounds encryption.

For every round, XOR calculation is done with the data and the round key. Restoring the text of this round is available by doing the XOR calculation with the round key again.

3. SAFETY ANALYSIS AND IMPROVEMENTS

AES has been widely used since it is authorized. When it comes to advantages, AES can resist many known attacks. It can be put into practical use on different kinds of platforms. What's more, it is fast and has a relatively simple structure for users and programmers to adapt to. Since AES's applications are numerous, for example, the development of accounting information system with AES, these industries and systems need high security assurance along with their development [8]. Thus, safety analysis of AES is necessary and meaningful.

The safety analysis is an important part for an algorithm to evaluate its usability and stability. The meaning of safety analysis is to judge the algorithm with the requirement that the potential attackers are still unable to break the key though they get to know the structure and procedures of the algorithm [9]. The attackers should consume more time on key attacks than exhaustive methods on this algorithm. For the safety analysis of AES, the resistance capacity towards different kinds of key attacks should be taken into consideration.

3.1 Brute Force Attack Analysis and Time Security

Brute force attack means applying exhaustive methods to figure out the key of the encryption. The time complexity of brute force attack is mainly decided by the block length and the key length of the algorithm. For this study, AES-128 has key length of 128 bits. After careful calculation, the results show that brute force attack has to try 3.403×10^{38} key combinations in the worst condition. This number of possible keys means that even for the fastest computer in the world, it will need about 3.19×10^{14} years to find that correct key [10]. This computation result shows a barely imaginable time demand for brute force attack, which verifies the time safety. What's more, the block size for plaintext and key length are both 128-bit for AES-128 and it has an additional random key size of 8 bits. For the additional bits, the attacker needs to

try 8.712×10^{40} key combinations in the worst condition. It will still need about 8.165×10^{16} years in maximum to crack the AES-128 algorithm even with the currently fastest computer in the world [10]. To be brief, it is totally impossible for human to try all the key combinations in a short time with current computation capacity.

3.2 Differential Cryptanalysis Analysis

Differential cryptanalysis is an effective method for block key analysis. It is proposed by Bihamand Shamiin in 1991 as a branch of chosen-plaintext attack. The fundamental idea of differential cryptanalysis is to acquire as many key bits as possible through the method of analyzing the effect of chosen plaintext changes on the ciphertext. This method is useful to attack block ciphers and ciphers constructed by iterating over a fixed round function.

For AES, the differential cryptanalysis is based on S-box attacks. Since the security of one encryption system is mainly dependent on the keys rather than the system. The keys of AES are the round keys generated by S-box. As a result, S-box is studied in every round to figure out part of the key. Linear analysis is applied for finding the most suitable linear functions among bits to try to find all bits [8]. For X, X' $\oplus$ $\{0, 1\}^n$, the differential of X, X' can be expressed as $\Delta X = X \oplus X'$. For input pair (X, X') and the output cipher pair (Y, Y'), the differential pair is (α, β), which satisfies $\alpha = X \oplus X'$ and $\beta = Y \oplus Y'$.

To generate differential distribution table of S-box, IN_s is defined. As S-box is a mapping of $F_2^m \rightarrow F_2^n$, IN_s refer to the assemble of (α, β) which satisfies $S(X \oplus \alpha) \oplus S(X) = \beta$. It means that $IN_s(\alpha, \beta)=\{x \in F_2^m : S(X \oplus \alpha) \oplus S(X) = \beta\}$.The attacker can only get several plaintext pairs, but he can observe the differential from different cipher pairs. Then the attacker should follow these steps:

- The attacker can select an input differential α and compute the plaintext pair (x_1, $x_1 \oplus \alpha$), (x_2, $x_2 \oplus \alpha$) and so on. With these pairs, the output differential δ_{y1}, δ_{y2}, … can be obtained.
- Afterwards, the attacker computes $\cap IN_s(\alpha, \delta_{yi})$ in order to get the possible key k.
- To get the actual key, the attacker has to choose more input differential and follow the step a & b until there only remains one possible key, which is the actual key.

3.3 Square Attack Analysis

Square attack is an attack based on the A set balance and is also a kind of chosen-plaintext attack. The designer of AES recommends that the method of using the square algorithm to calculate passwords based on byte structures is called Persistent Threat. Since AES algorithm integrates the byte-structure-oriented feature of square algorithm, the square attack can also be applied to AES [11]. According to analysis of basic attacks of square attack, there's no successful square attack towards the complete AES algorithm. There're several methods for solving AES with the reduced rounds, which are 4~6 rounds in detail [9]. This means that the attack is only possible for AES with less than 6 rounds. To avoid the square attack and ensure the security, the number of rounds must be equal to or greater than 7 [11]. Therefore, after taking this condition and other features into consideration, the AES algorithm requires 10 rounds of operations, which correspond to 128-bit key.

3.4 Improvements

As the AES algorithm is a widely used cipher system currently, the potential risks as mentioned above need to be faced and solved. Continually being open to attacks will leave the practical users and platforms unsecure. To face up these attacks, divisions of them should be made. The differential cryptanalysis attack and square attack are both chosen-plaintext attacks. Besides, side channel attack and energy analysis attack are all methods that are likely to break the algorithm.

For improvements, a lot of researches and optimizations have been carried out. In Mouna's research, an improved method for AES implementation is discussed [12]. It uses temporal redundancy and adjusts the AES cycle to make it able to perceive fault attacks that may appear during runtime execution. This change can improve working frequency because pipelined registers are used. According to the research results and statistics, the detection of single fault attacks and multiple fault attacks becomes possible reality with its efficient fault detection system.

4. CONCLUSION

This paper introduces the basic theory and concrete procedures of AES algorithm. AES as a widely-used cryptography technology shows the typical process and the significant points of a symmetric and block cryptography function.AES-128 is taken as an example for research in this paper. Starting by plaintext processing, the message needed to be transformed is turned into data matrix for later procedures. Substituting bytes is applied with a S-box to further handle the data matrix. Shifting rows and mixing columns are continued with matrix transformation in two certain different ways to help the cipher data to become massy gradually. To add round key part, the original key is expended with key generation functions. The keys obtained from the function are separately work for ten rounds of encryption. For the decryption part, an inverse of the encryption function will successfully work to help get the original plaintext provided with the ciphertext.

Safety analysis is applied for AES algorithm. Its resistance against brute force attack, differential cryptanalysis attack and square attack is taken into consideration. For brute force attack, AES shows perfect time security after computation of time consumption for exhaustive methods. The differential cryptanalysis attack provides a potential attack method against AES. Basic steps are shown for a typical differential cryptanalysis attack. The square attack turns out to be not effective against AES as AES has rounds of more than ten to resist such kind of attacks. To optimize attacks mentioned before and other potential attacks, improvements are continually raised for better security and performance of AES. A method of using temporal redundancy and changing the AES cycle is mentioned, which can effectively detect single and multiple fault attacks and increasing working efficiency. Obviously, more measures and improvements will be figured out and help AES to become more and more comprehensive and secure in nearing future.

References

[1] A. Hamza and B. Kumar, “A Review Paper on DES, AES, RSA Encryption Standards,” 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 333-338.

[2] J. Daemen and V. Rijmen, "The First 10 Years of Advanced Encryption," in IEEE Security & Privacy, vol. 8, no. 6, pp. 72-74, Nov.-Dec. 2010.

[3] ReadingLover. 2015. Detailed explanation of cryptographic algorithm—AES. https://www.cnblogs.com/luop/p/4334160.html.

[4] Wang peifen, “S-box design analysis and improvement of AES encryption algorithm [J],” in Journal of huaihai institute of technology (natural science edition), 2014, pp. 18-21.

[5] Liu Yufeng, Xu Xiangyang, Su Hao, Geng Yanxiang and Liu Ting, “Optimization and design of block cipher AES [J],” in Computer applications and software, 2020, pp. 267-270+297.

[6] Aiden A. Bruen, Mario A. Forcinito and James M. McQuillan, "Modes of Operation for AES and Symmetric Algorithms," in Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century, Wiley, 2021, pp.109-123.

[7] Guo Yanzhen, Han Wenbao, Zhao Long and Liu Jiaxiao, “AES column hybrid transformation [J],” in Journal of PLA university of science and technology (natural science edition), 2009, pp. 232-236.

[8] Qing-Xiang Zhu, Lu Li, Jing Liu and Nan Xu, "The analysis and design of accounting information security system based on AES algorithm," in 2009 International Conference on Machine Learning and Cybernetics, 2009, pp. 2713-2718.

[9] Dongli Zhang and Wenchen Jiao, “AES algorithm and Safety Analysis,” in Proceedings of the 2011 International Conference on Future Computer Science and Application, 2011, pp.237-239.

[10] Al-Mamun A , Shawon S M R , Ahmed Shaon T , et al, “Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte[J],” in International Journal of Computer Networks and Communications, 2017, pp. 69-88.

[11] Wei Baodian, Liu Dongsu and Wang Xinmei, “A New Square Attack [J],” in Journal of Xidian University,2003, pp. 473-476.

[12] Mouna Bedoui, Hassen Mestiri, Belgacem Bouallegue, Belgacem Hamdi and Mohsen Machhout, “An improvement of both security and reliability for AES implementations,” Journal of King Saud University - Computer and Information Sciences, 2022.