Advanced Encryption Standard (AES) and It's Working

Shripal Rawal

Undergraduate Final year, Department of Computer Science & Engineering,
DRIEMS, Mumbai University,
Mumbai, Maharashtra, India
Email- rawalshreepal000@gmail.com

---***---

Abstract - *Encryption is an interesting piece of technology that works by scrambling data so it is unreadable by unintended parties. The Advanced Encryption Standard (AES), which is also known as Rijndael (its original name), is a specification for the encryption of electronic data. Encryption is a process of encoding messages or vital information in such a way that only canonical parties can read it. Encryption does not of itself prevent the interception, but denies the information to the interceptor. Encryption in simple words means generating a cipher text which can be only read by the one having decryption key. One such encryption technique used for protecting online data from any malicious threat is Advanced Encryption Standard (AES). Generally Encryption uses symmetric key encryption schemes or public key encryption schemes. These schemes are discussed later.*

Key Words: **Rijndael, Cipher, Decryption, Encryption, Data, Encoding, Canonical, Malicious, Symmetric key, Public key.**

1. INTRODUCTION

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths.

1.1. What is Symmetric or Secret key?

Symmetric key cryptography systems use the same key for both to encrypt the plain text and to decrypt the cipher text. Symmetric key systems have the advantage of being simple and fast. However, the important factor to be considered is that the parties involved must exchange the key in a secured way.

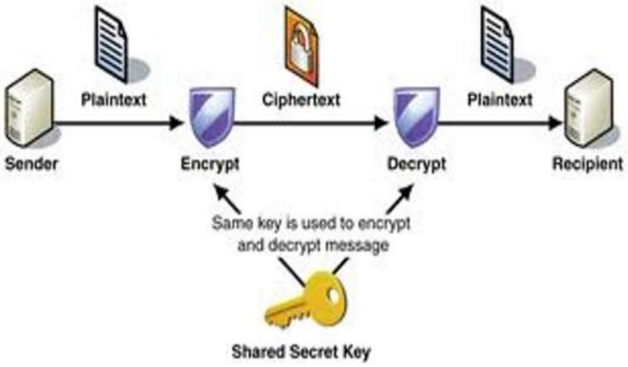


Fig -1: Secret key scheme

The above figure demonstrates Symmetric or Secret key scheme.

1.2. What is Public Key?

In comparison to symmetric key, public key cryptography systems use different keys to encrypt to plaintext and to decrypt the cipher text.

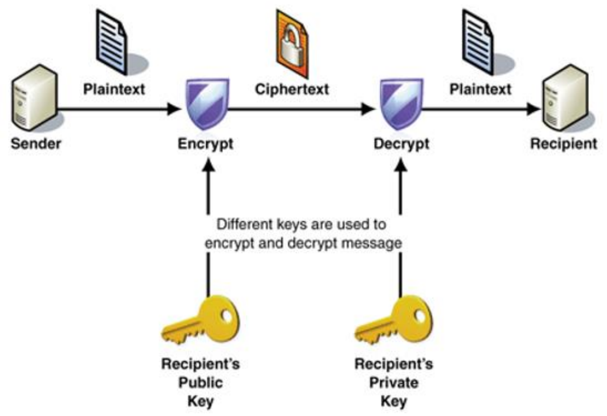


Fig -2: Public key scheme

Public key uses 2 different keys – a public key for encryption and a private key for decryption. Using this encryption system, the public key can be distributed in a non-secure way. The private key is never transmitted and is only available at the recipient's side. As the keys are different, the decryption of the cipher text computationally is assumed to be not feasible without the private key.

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. 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.

AES operates on a 4 × 4 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 finite field.

For instance, if there are 16 bytes b_0, b_1... b_{15}, these bytes are represented as this matrix:

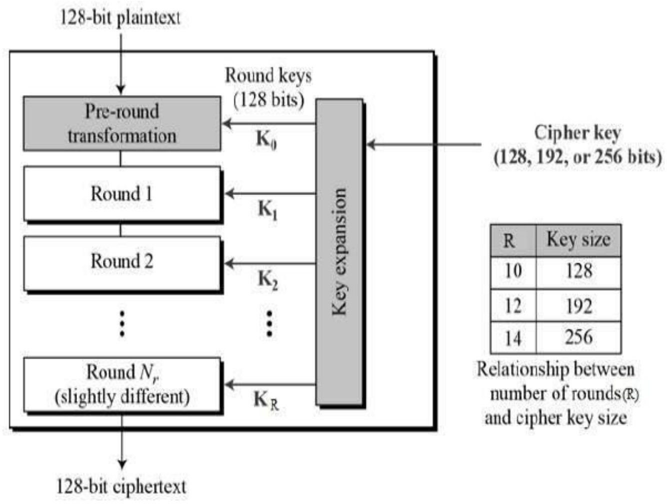
$$\begin{pmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{pmatrix}$$

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 cipher text. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

The schematic of AES structure is given in the following illustration –



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig -3: AES structure

2. ENCRYPTION PROCESS

Data encryption using AES consists of several rounds, depending on the cipher blocks, i.e. AES-128, AES-192 and AES-256. A typical round in AES encryption comprise of four sub-processes. The first round process is depicted below-

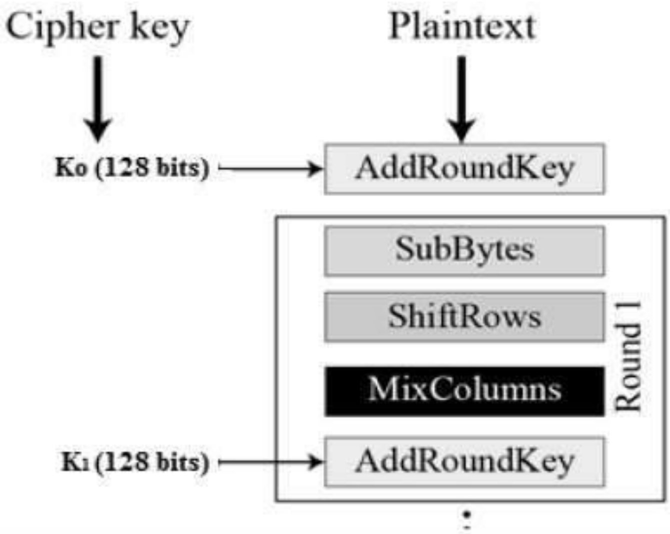


Fig -4: Sub processes in round 1

The above figure illustrates the sub processes of the intermediate rounds, the initial and final rounds comprise of subtle different process.

AES works on the following 4 steps:

1. KeyExpansions
2. InitialRound
   - 2.1. AddRoundKey
3. Rounds
   - 3.1. SubBytes (Bytes Substitution)
   - 3.2. ShiftRows
   - 3.3. MixColumns
   - 3.4. AddRoundKey
4. FinalRound
   - 4.1. SubBytes
   - 4.2. ShiftRows
   - 4.3. AddRoundKey

1. KeyExpansions.

Round keys are derived from the cipher key using Rijndael's key schedule.

2. InitialRound.

2.1. AddroundKey.

In the AddRoundKey step, the subkey is combined with the state. This step is explained in detail in further in the context.

3. Rounds.

3.1. SubBytes.

In the SubBytes step, each byte $a_{i,j}$ in the state matrix is replaced with a SubByte $S(a_{i,j})$, using an 8-bit substitution box, the Rijndael S-box. This operation provides non-linearity in the cipher. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation.

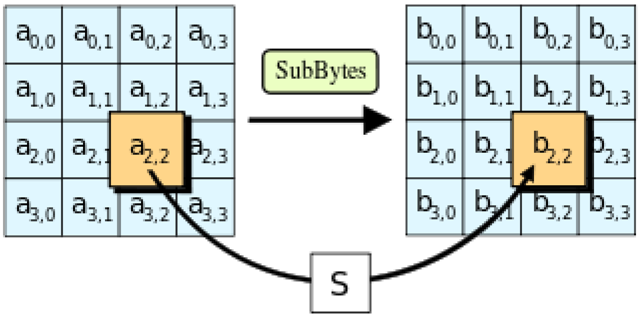


Fig -5: SubBytes process

3.2. ShiftRows.

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks.

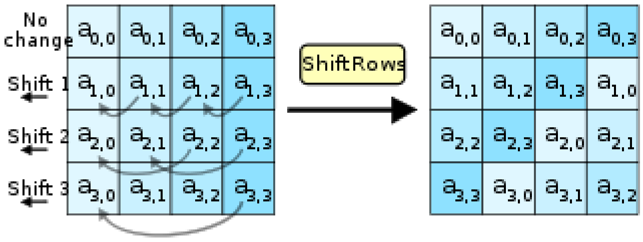


Fig -6: ShiftRows process

3.3. MixColumns.

In the MixColumns step, the four bytes of column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. During this operation, each column of state is transformed by multiplying with a fixed polynomial c(x).

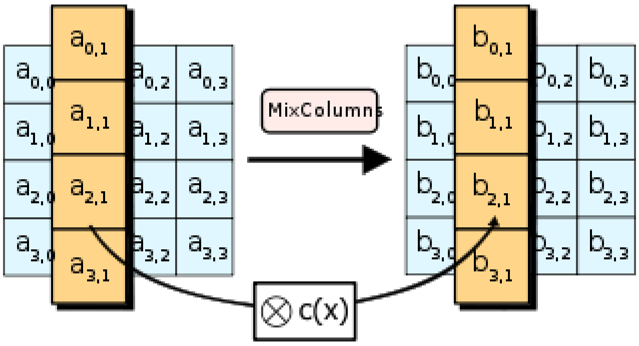


Fig -7: MixColumns process

3.4. AddRoundKey.

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

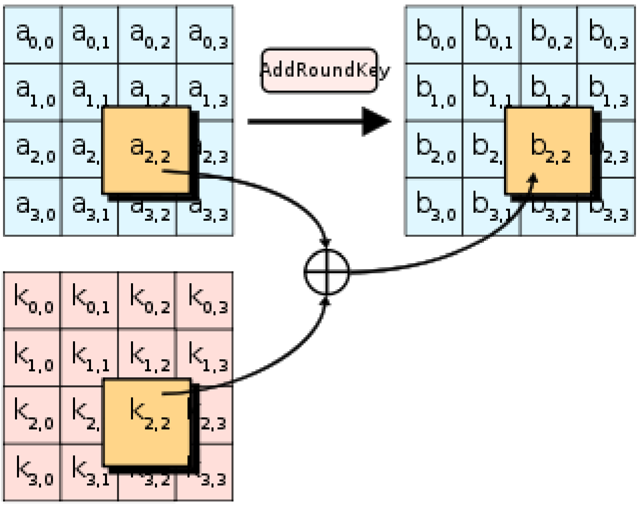

AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$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

Fig -8: AddRoundKey process

4. FinalRound.

The FinalRound comprise of all the sub processes of rounds, except the MixColumns step. Rest of the process is entirely similar to that of Rounds.

3. 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, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

4. CONCLUSION

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

5. REFERENCE

[1]. Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". Pp267–287, ASIACRYPT 2002.

[2]. Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.

[3]. Christof Paar, Jan Pelzl, "The Advanced Encryption Standard", Chapter 4 of "Understanding Cryptography, a Textbook for Students and Practitioners". (Companion web site contains online lectures on AES), Springer, 2009.

[4]. Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology.

[5]. "Efficient software implementation of AES on 32-bit platforms". Lecture Notes in Computer Science: 2523. 2003

[6]. "ISO/IEC 18033-3: Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers".

[7]. Biryukov, Alex; Khovratovich, Dmitry (2009-12-04). "Related-key Cryptanalysis of the Full AES-192 and AES-256".