The AES Algorithm Explained

A Straight to the Point Overview of the Advanced Encryption Standard

Documentation made with dedication, by Mousa Emarah.

The Advanced Encryption Standard (AES), also known as Rijndael, is the most widely used symmetric encryption algorithm today. Adopted by the U.S. government in 2001, AES replaced the aging Data Encryption Standard (DES) and provides stronger security with key sizes of 128, 192, or 256 bits. Unlike DES, which uses a 56-bit key and became vulnerable to brute-force attacks, AES remains resistant to all known practical cryptanalytic attacks when implemented correctly.

Brief: How AES Works

AES is a block cipher that processes 128-bit blocks of data (16 bytes) using a series of mathematical transformations. The number of rounds (transformation steps) depends on the key size:

10 rounds for 128-bit keys

12 rounds for 192-bit keys

14 rounds for 256-bit keys

Each round consists of four main operations:

1. SubBytes – A non-linear substitution using a predefined S-box.
2. ShiftRows – A transposition step that shifts rows of the state matrix.
3. MixColumns – A mixing operation that combines bytes in each column.
4. AddRoundKey – An XOR operation with a round-specific subkey.

So, we have 2 main steps:

A) Key Expansion

Before encryption begins, AES expands the original key into a series of round keys, This ensures confusion where the cipher text now depens on multiple parts of the key as each round uses a unique subkey derived from the original key.

B) MSG Encyption

We have 2 important things:

Data and Key.

First, the data is transformed into hexadecimal [Block to state “Maxtrix”]

Then, the Hexa is turned into binary to enter the following process:

Initial Key Addition (AddRoundKey)

(Where The plaintext is XORed with the first round key.)

After that, 10 Rounds of Transformation happen.

Each round applies:

SubBytes (S-box substitution)

ShiftRows (cyclically shifting rows)

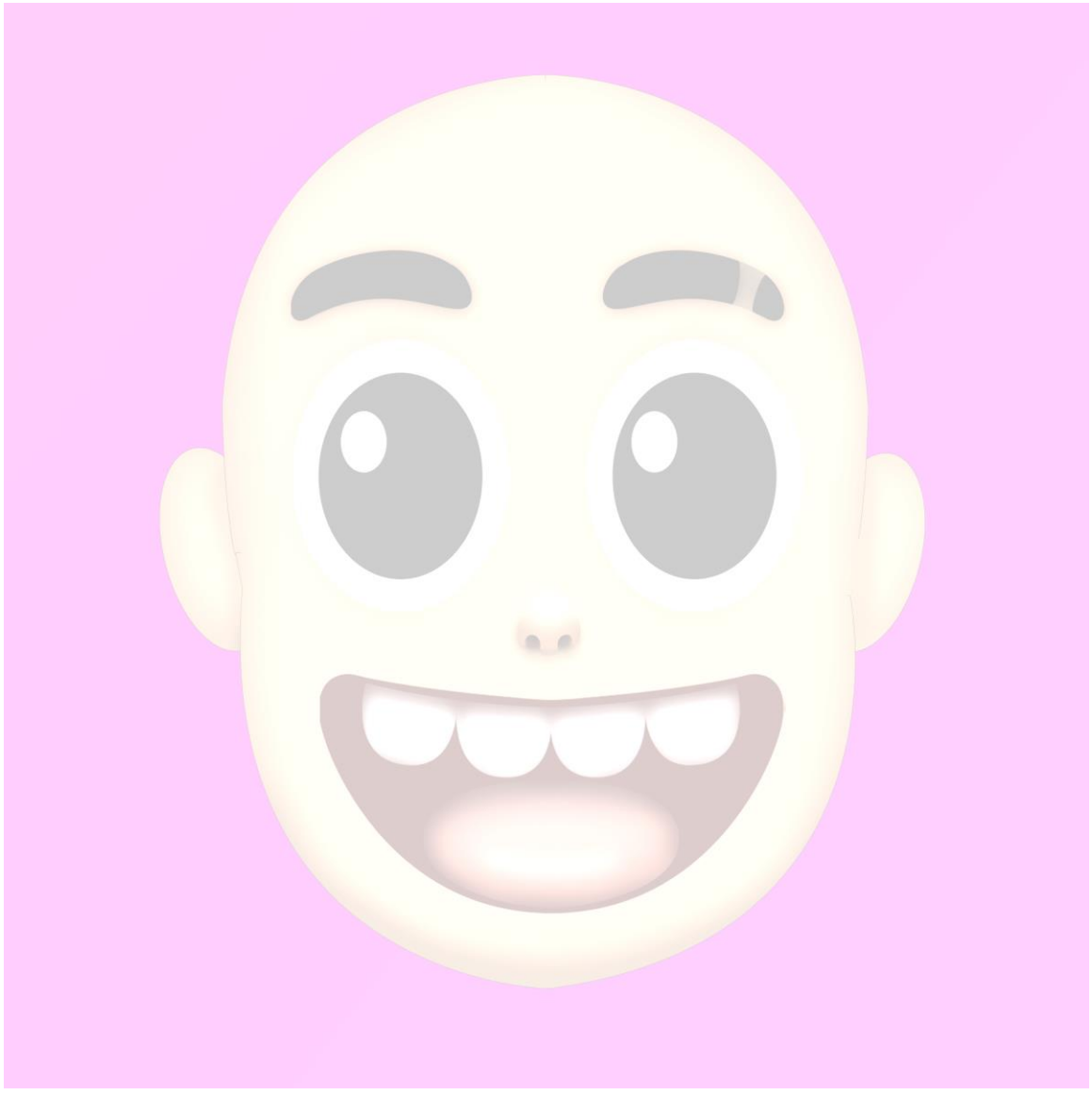
MixColumns (matrix multiplication, except last round)

Then **repeat** again, AddRoundKey (XOR with round key)

https://www.linkedin.com/in/mousa123/

Ready to dive into more details?

Don’t worry man, it’s fun!



1. Key Expansion Process

Before encryption begins, AES expands the original key into multiple round keys using the Rijndael key schedule.

1.1 Key Preparation

The 128-bit (16-byte) key is arranged in a 4×4 byte matrix (called the key state).

For 192-bit and 256-bit keys, the matrix is extended accordingly.

1.2 Round Key Generation

AES generates 10, 12, or 14 round keys (for 128, 192, and 256-bit keys, respectively).

Key Expansion Steps:

1. SubWord – Each byte in a word is substituted using the AES S-box.
2. RotWord – A 1-byte left rotation is applied to a 4-byte word.
3. Rcon (Round Constant) – A predefined XOR operation is applied to introduce non-linearity.
4. XOR Combination – The previous round key is XORed with the transformed word to generate the next round key.

2. Message Encryption Process

AES encrypts 128-bit (16-byte) blocks through multiple rounds of substitution and permutation.

2.1 Initial Setup

Plaintext Conversion – The input message is converted into a 4×4 byte matrix (called the state matrix).

Initial AddRoundKey – The state matrix is XORed with the first round key.

2.2 Round Operations (10/12/14 Rounds)

Each round (except the last) consists of four main operations:

1. SubBytes (Non-linear Substitution)

Each byte in the state matrix is replaced using the AES S-box.

Provides confusion by breaking linearity.

2. ShiftRows (Row-wise Rotation)

1. Row 0: No shift.
2. Row 1: Left-shifted by 1 byte
3. Row 2: Left-shifted by 2 bytes.
4. Row 3: Left-shifted by 3 bytes.

Now, with the diffusion, where we spread out info from plain text to cipher.

3. MixColumns (Column Mixing)

Each column is multiplied by a fixed matrix in Galois Field (GF(2^8)).

-Provides diffusion by spreading changes across the entire block.-

4. AddRoundKey (Key XORing)

The state matrix is XORed with the current round key.

2.3 Final Round (No MixColumns)

The last round skips MixColumns and only performs:

1. SubBytes
2. ShiftRows
3. AddRoundKey

3. Decryption Process

AES decryption reverses the encryption steps:

1. Inverse AddRoundKey (using round keys in reverse order).
2. Inverse ShiftRows (right shifts instead of left).
3. Inverse SubBytes (using the inverse S-box).
4. Inverse MixColumns (applying the inverse matrix).

Why AES is Secure

1. Larger Key Sizes (128/192/256 bits) – Resistant to brute-force attacks.
2. Strong Diffusion & Confusion – Every bit affects the entire ciphertext.
3. Efficient Implementation – Works well in both hardware and software , optimized for speed.

AES vs. DES

Feature	DES (1977)	AES (2001)
Key Size	56 bits	128/192/256 bits
Block Size	64 bits	128 bits
Rounds	16	10/12/14
Security	Broken (brute-force)	Still secure

Modes of Operation

Like DES, AES supports different encryption modes:

1. ECB (Electronic Codebook) – Encrypts each block independently (weak for patterns).
2. CBC (Cipher Block Chaining) – Each block depends on the previous (better security).
3. GCM (Galois/Counter Mode) – Provides authenticated encryption (used in TLS).

Is AES Crackable?

1. Brute-force attacks on AES-128 are impractical (would take billions of years).
2. Side-channel attacks (timing/power analysis) are possible but require physical access.
3. Quantum computers could theoretically break AES-256, but practical quantum attacks are still far off.

Conclusion

AES remains the gold standard for symmetric encryption, trusted by governments, banks, and cybersecurity experts worldwide. Its mathematical foundations ensure security, while its efficiency allows fast encryption on everything from smart cards to supercomputers.

Good Resources:

Simulation:

https://www.formaestudio.com/rijndaelinspector/

https://www.youtube.com/watch?v=C4ATDMIz5wc

https://www.youtube.com/watch?v=gP4PqVGudtg

https://www.youtube.com/watch?v=FLszAz7gRqM