Report Title: The Advanced Encryption Standard (AES)

Module name: *Cryptography*

Module code: *IT302*

Semester: *Second Semester*

Supervision: *Dr/Ahmed Farouk*

Submission Date: *26/5/2024*

Word count:*1953 words*

Team members:

1- Hassanein Said Mohamed.
2- Nader Ahmed BhaaEldein
3- Mina Hany Ibrahim
4- Ismail Sherif Abdelfatah

Table of Contents:

Abstract:

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely adopted for securing digital data. Developed by the National Institute of Standards and Technology (NIST) in 2001, AES has become the de facto standard for data encryption across various applications, including secure communications, financial transactions, and data storage. This paper presents an overview of the AES algorithm, detailing its encryption and decryption processes.

AES operates on fixed block sizes of 128 bits and supports key lengths of 128, 192, and 256 bits, providing flexibility in security levels. The encryption process involves a series of transformations—Sub Bytes, Shift Rows, Mix Columns, and Add Round Key—repeated over multiple rounds, depending on the key size. The decryption process reverses these steps, employing inverse transformations to retrieve the original plaintext from the ciphertext. Central to both encryption and decryption is the key schedule, which generates a sequence of round keys from the original key.

Introduction:

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used for securing data. It operates on fixed block sizes and supports key sizes of 128, 192, or 256 bits. **Here is the structure of the AES algorithm:**

Key Features

- Block Size: 128 bits (16 bytes)

- Key Sizes: 128, 192, or 256 bits

- Number of Rounds:

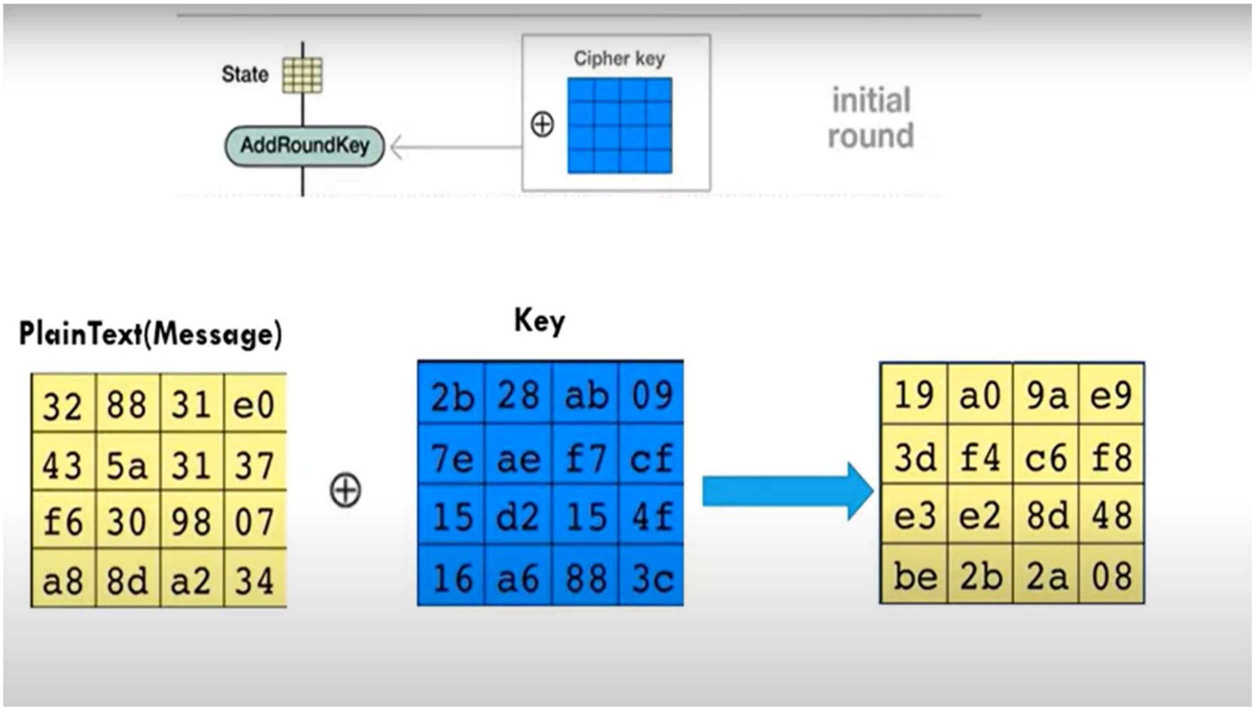
- 10 rounds for 128-bit keys
- 12 rounds for 192-bit keys
- 14 rounds for 256-bit keys

Steps in the AES Algorithm

1.Key Expansion: The AES key schedule generates a series of round keys from the initial key. This involves using a Rijndael key schedule to expand the initial key into multiple round keys, one for each round plus one more for the initial round.

2. Initial Round:

- Add Round Key: The input data (plaintext) is XORed with the first-round key.



PlainText(Message)

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

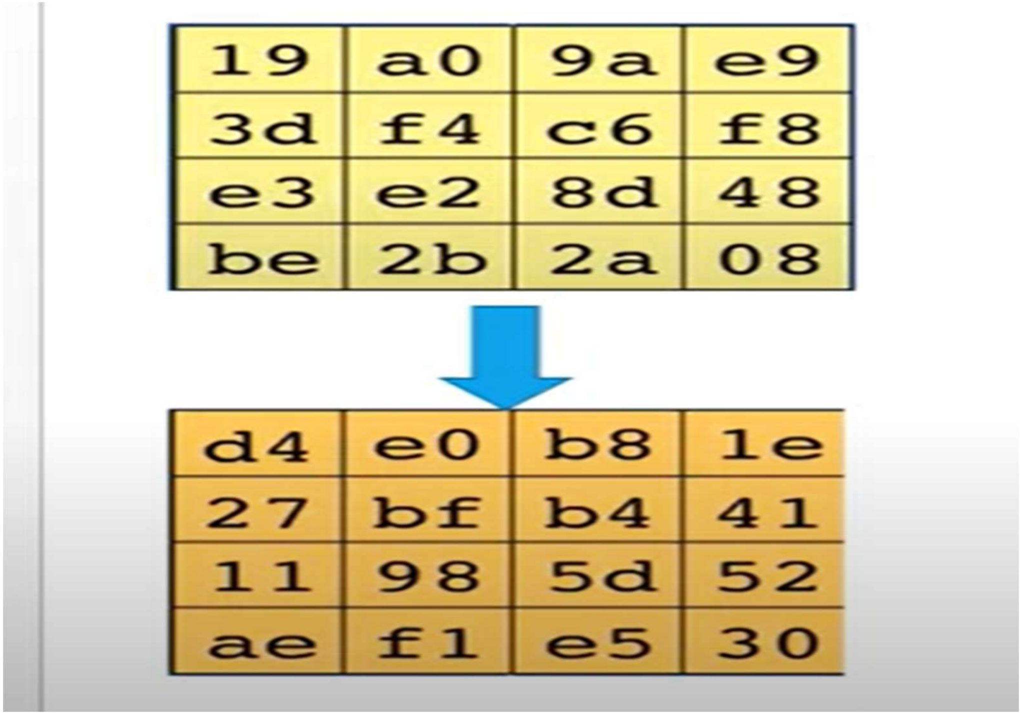
Key

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

3. Main Rounds (repeated 9, 11, or 13 times depending on key size):

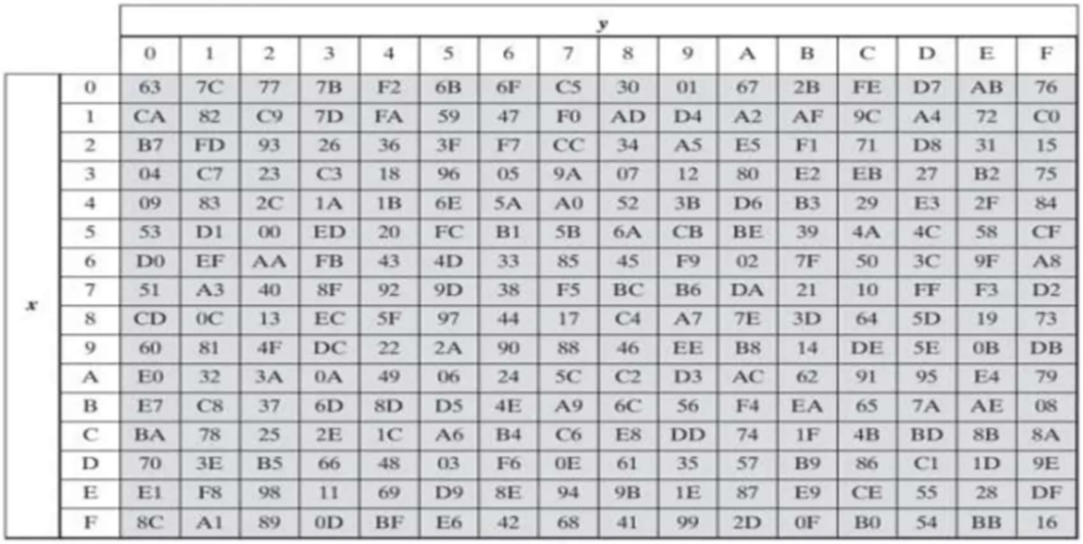
- **Sub Bytes:** Each byte in the state array is replaced with its corresponding byte from the S-box (a fixed 16x16 table). This provides non-linearity in the cipher.



19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

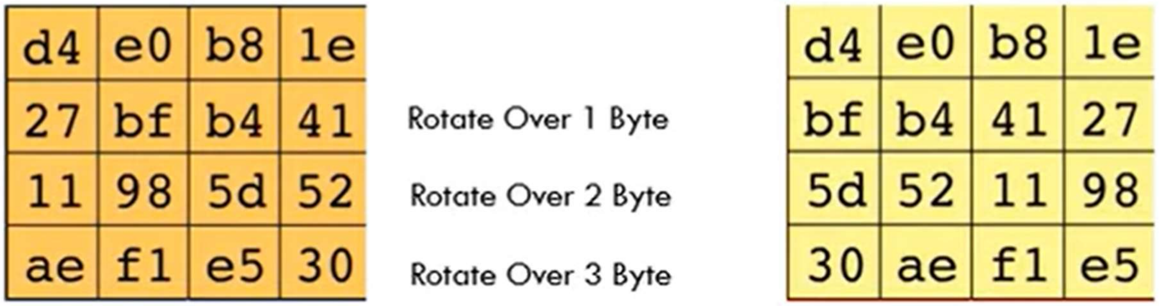
Table 5.2 AES S-Boxes



		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

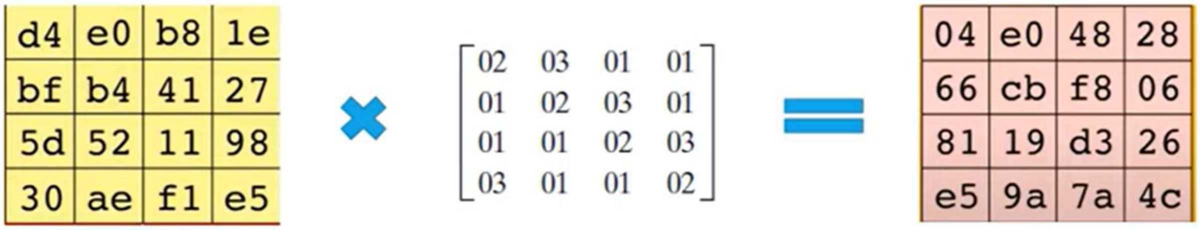
(a) S-box

- Shift Rows: The rows of the state array are shifted cyclically to the left. The amount of shift depends on the row index (e.g., the first row is left unchanged, the second row is shifted one position to the left, etc.).



d4	e0	b8	1e		d4	e0	b8	1e
27	bf	b4	41	Rotate Over 1 Byte	bf	b4	41	27
11	98	5d	52	Rotate Over 2 Byte	5d	52	11	98
ae	f1	e5	30	Rotate Over 3 Byte	30	ae	f1	e5

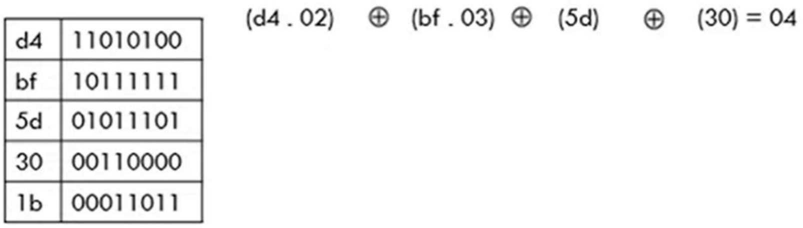
- Mix Columns: Each column of the state array is mixed using matrix multiplication in the Galois Field (2^8). This step combines the four bytes in each column.



d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

$$\times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} =$$

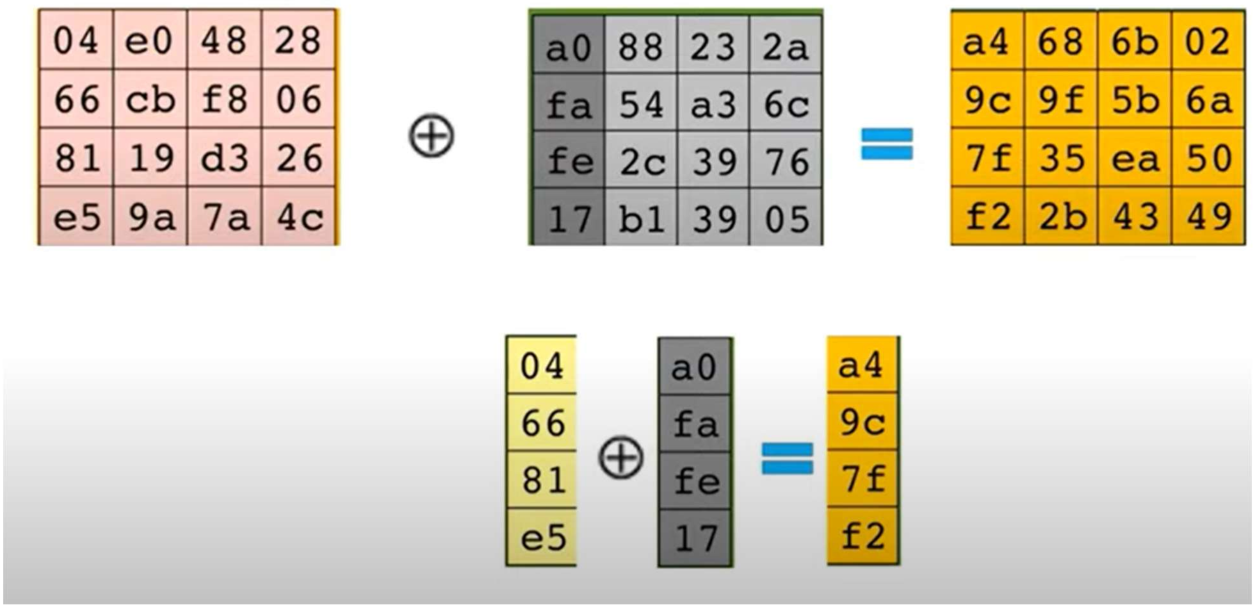
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c



d4	11010100
bf	10111111
5d	01011101
30	00110000
1b	00011011

(d4 . 02) ⊕ (bf . 03) ⊕ (5d) ⊕ (30) = 04

- **Add Round Key:** The state array is XORed with the round key generated during the key expansion step.

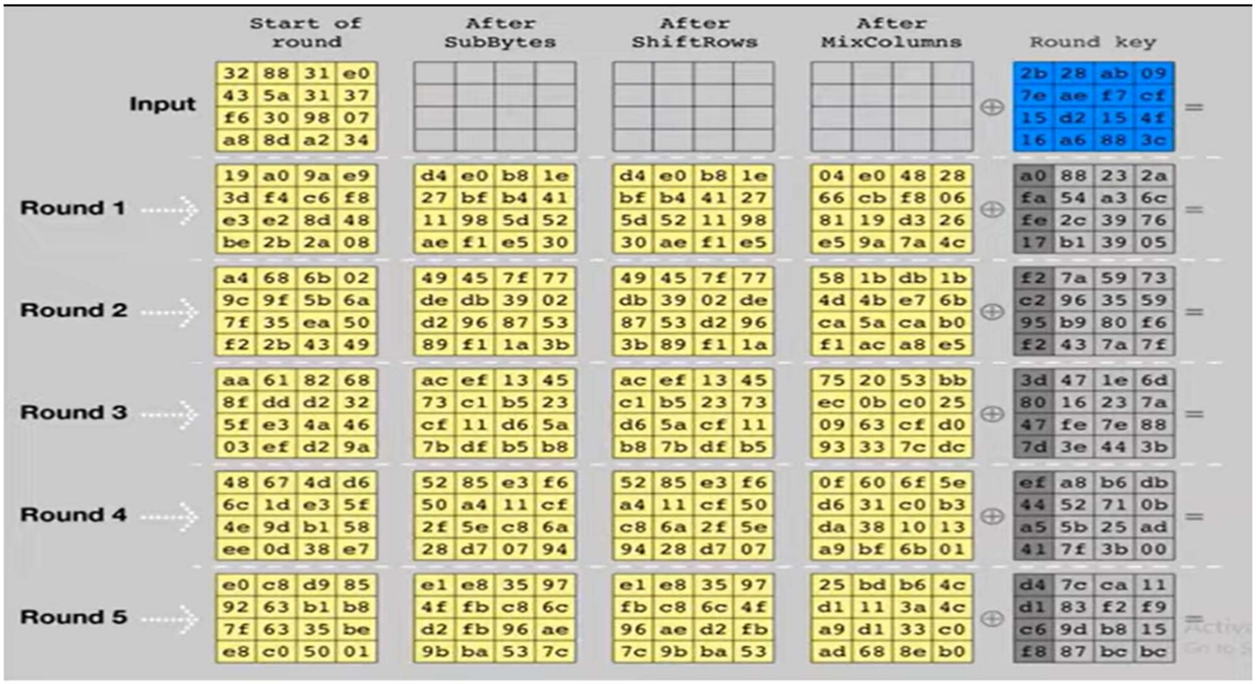


$$\begin{matrix} 04 & e0 & 48 & 28 \\ 66 & cb & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{matrix} \oplus \begin{matrix} a0 & 88 & 23 & 2a \\ fa & 54 & a3 & 6c \\ fe & 2c & 39 & 76 \\ 17 & b1 & 39 & 05 \end{matrix} = \begin{matrix} a4 & 68 & 6b & 02 \\ 9c & 9f & 5b & 6a \\ 7f & 35 & ea & 50 \\ f2 & 2b & 43 & 49 \end{matrix}$$

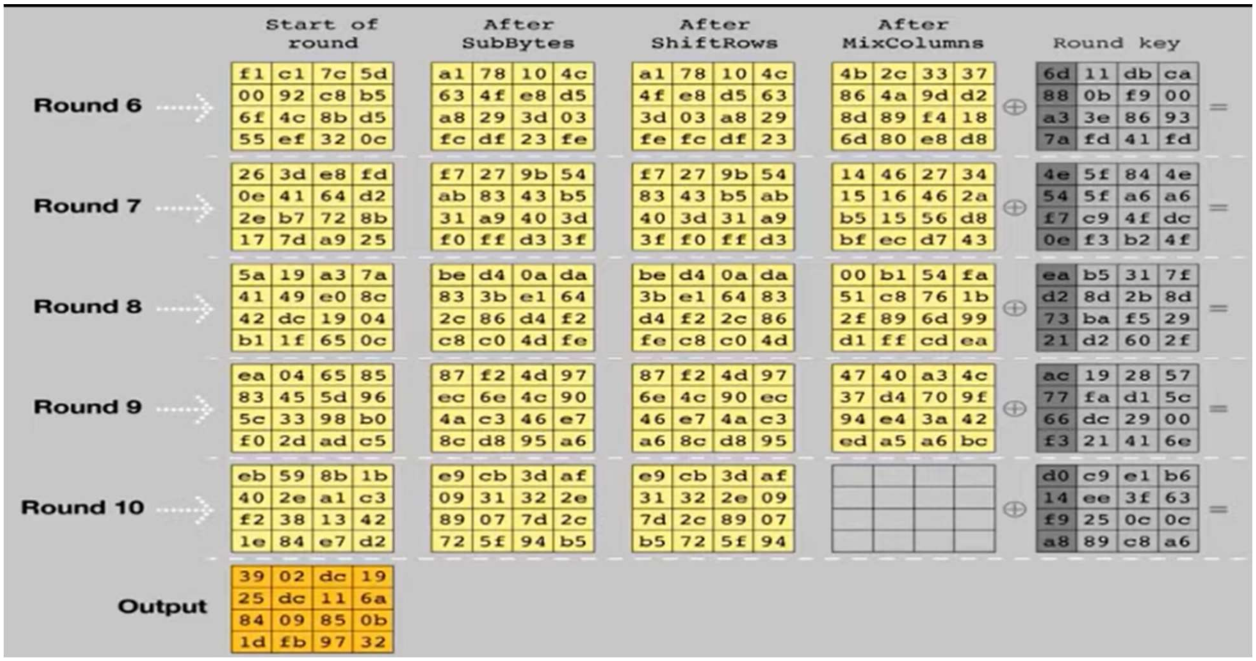
$$\begin{matrix} 04 \\ 66 \\ 81 \\ e5 \end{matrix} \oplus \begin{matrix} a0 \\ fa \\ fe \\ 17 \end{matrix} = \begin{matrix} a4 \\ 9c \\ 7f \\ f2 \end{matrix}$$

4. Final Round (similar to main rounds but without Mix Columns):

- Sub Bytes
- Shift Rows
- Add Round Key



	Start of round	After SubBytes	After ShiftRows	After MixColumns		Round key	
Input	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				⊕	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	=
Round 1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	⊕	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	=
Round 2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	⊕	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	=
Round 3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	⊕	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	=
Round 4	48 67 4d d6 6c 1d e3 5f 4e 9d b1 58 ee 0d 38 e7	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 bf 6b 01	⊕	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	=
Round 5	e0 c8 d9 85 92 63 b1 b8 7f 63 35 be e8 c0 50 01	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8e b0	⊕	d4 7c ca 11 d1 83 f2 f9 c6 9d b8 15 f8 87 bc bc	=



	Start of round	After SubBytes	After ShiftRows	After MixColumns	Round key
Round 6	f1 c1 7c 5d 00 92 c8 b5 6f 4c 8b d5 55 ef 32 0c	a1 78 10 4c 63 4f e8 d5 a8 29 3d 03 fc df 23 fe	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18 6d 80 e8 d8	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd
Round 7	26 3d e8 fd 0e 41 64 d2 2e b7 72 8b 17 7d a9 25	f7 27 9b 54 ab 83 43 b5 31 a9 40 3d f0 ff d3 3f	f7 27 9b 54 83 43 b5 ab 40 3d 31 a9 3f f0 ff d3	14 46 27 34 15 16 46 2a b5 15 56 d8 bf ec d7 43	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f
Round 8	5a 19 a3 7a 41 49 e0 8c 42 dc 19 04 b1 1f 65 0c	be d4 0a da 83 3b e1 64 2c 86 d4 f2 c8 c0 4d fe	be d4 0a da 3b e1 64 83 d4 f2 2c 86 fe c8 c0 4d	00 b1 54 fa 51 c8 76 1b 2f 89 6d 99 d1 ff cd ea	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f
Round 9	ea 04 65 85 83 45 5d 96 5c 33 98 b0 f0 2d ad c5	87 f2 4d 97 ec 6e 4c 90 4a c3 46 e7 8c d8 95 a6	87 f2 4d 97 6e 4c 90 ec 46 e7 4a c3 a6 8c d8 95	47 40 a3 4c 37 d4 70 9f 94 e4 3a 42 ed a5 a6 bc	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e
Round 10	eb 59 8b 1b 40 2e a1 c3 f2 38 13 42 1e 84 e7 d2	e9 cb 3d af 09 31 32 2e 89 07 7d 2c 72 5f 94 b5	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 b5 72 5f 94		d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6
Output	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32				

Detailed Steps in Each Round:

- Sub Bytes:

- Uses a non-linear substitution table (S-box) to perform a byte-by-byte substitution of the block.

- Shift Rows:

- A transposition step where the rows of the state are shifted cyclically.

- Mix Columns:

- A mixing operation that operates on the columns of the state, combining the four bytes in each column.

- Add Round Key:

- Each byte of the state is combined with the round key using bitwise XOR.

AES DECRYPTION

Describing AES decryption in a written format, such as in a paper or theoretical context, involves explaining the process and mathematics behind the algorithm. Here is a detailed step-by-step explanation of AES decryption:

AES Decryption Overview

AES (Advanced Encryption Standard) is a symmetric key encryption algorithm, and its decryption process involves reversing the steps of encryption. AES operates on a fixed block size of 128 bits (16 bytes) and supports key sizes of 128, 192, and 256 bits. For simplicity, we will focus on AES-128.

Steps in AES Decryption

1. initial Setup:

- The ciphertext is divided into 128-bit blocks.

- The key schedule is computed to generate round keys from the original key.

2. initial Round:

- Add Round Key: The ciphertext block undergoes an XOR operation with the last round key (derived from the key schedule).

3. Main Rounds:

AES-128 involves 10 rounds, AES-192 involves 12 rounds, and AES-256 involves 14 rounds. Each round except the last consists of the following transformations:

- **Inv Shift Rows:** This is the inverse of the Shift Rows step in encryption. The rows of the state (intermediate ciphertext) are shifted right by different offsets:

  - The first row is not shifted.

  - The second row is shifted right by 1 byte.

  - The third row is shifted right by 2 bytes.

  - The fourth row is shifted right by 3 bytes.

- **Inv Sub Bytes:** This is the inverse of the Sub Bytes step in encryption. Each byte of the state is replaced with its value in the inverse S-box (a predefined substitution table).

- **Add Round Key:** The state undergoes an XOR operation with the round key corresponding to the current round.

- **Inv Mix Columns:** This is the inverse of the Mix Columns step in encryption. Each column of the state is multiplied by the inverse of a fixed polynomial in GF(2^8). This step is omitted in the last round.

4. Final Round:

The final round involves only three transformations:

- Inv Shift Rows
- Inv Sub Bytes
- Add Round Key

Key Schedule

The key schedule generates a series of round keys from the original key. These round keys are used in the Add Round Key step. The key expansion algorithm involves:

- Rotating and substituting the key bytes.
- XORing the transformed bytes with a round constant (Rcon) and parts of the original key.

The Advanced Encryption Standard (AES) offers several advantages over other encryption algorithms:

1. Strong Security: AES has been extensively analyzed and is considered secure against all known attacks when used properly. Its design includes multiple rounds of encryption, which increases its resistance to cryptographic attacks.

2. Efficiency: AES is computationally efficient and can be implemented in both hardware and software without requiring a significant amount of resources. This efficiency makes it suitable for use in a wide range of applications, from embedded systems to high-performance servers.

3. Standardization: AES is a standard encryption algorithm adopted by governments, businesses, and industries worldwide. Its standardization ensures interoperability and compatibility between different systems and applications.

4. Flexibility: AES supports key sizes of 128, 192, and 256 bits, allowing users to choose the level of security that best suits their needs. This flexibility makes AES suitable for a variety of use cases.

5. Ease of Implementation: AES's algorithm is straightforward and well-defined, making it relatively easy to implement in different programming languages and environments.

6. Wide Adoption: AES is one of the most widely used encryption algorithms in the world. Its widespread adoption and acceptance make it a trusted choice for securing sensitive information.

Advanced Encryption Standard (AES) is a highly secure and efficient encryption algorithm, it does have some limitations and potential disadvantages:

1. Resource Intensive: AES can be computationally intensive, especially when using longer key lengths (e.g., 192 or 256 bits). This can impact performance on devices with limited processing power.

2. Key Management: AES requires careful key management practices to ensure the security of encrypted data. The complexity of managing keys increases with the number of keys and the size of the encrypted data.

3. Side-Channel Attacks: AES implementations may be vulnerable to side-channel attacks, where an attacker observes the physical characteristics of the encryption process (such as power consumption or electromagnetic radiation) to infer information about the encryption key.

4. Potential Quantum Computing Vulnerability: While AES is currently considered secure against quantum attacks, future advancements in quantum computing could potentially threaten its security, especially for shorter key lengths.

5. Block Size Limitation: AES operates on fixed block sizes of 128 bits. While this is sufficient for many applications, it can be a limitation in scenarios where variable-length data needs to be encrypted.

6. Complexity for Beginners: While the AES algorithm itself is well-defined, understanding and implementing it from scratch can be challenging for beginners in cryptography.

The Advanced Encryption Standard (AES) algorithm finds applications in various areas where secure encryption and decryption of data are crucial. Some prominent application areas of AES include:

1. Secure Communication: AES is widely used in securing communication channels, such as:

- **Internet Communication:** HTTPS (HTTP Secure) uses AES to encrypt data transmitted over the internet, ensuring confidentiality and integrity.

- **Email Encryption:** AES is used in email encryption protocols like S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) to protect email contents from unauthorized access.

2. Data Storage: AES is utilized to encrypt data stored on various devices to prevent unauthorized access, including:

- **File Encryption:** Operating systems like Windows (BitLocker) and macOS (FileVault) use AES to encrypt files and directories.

- **Cloud Storage:** Cloud service providers use AES to encrypt data stored in the cloud, ensuring data privacy and security.

3. Wireless Security: AES is a part of the security protocols used to secure wireless networks, such as:

- **Wi-Fi Security: WPA2** (Wi-Fi Protected Access 2) uses AES for encryption, protecting wireless networks from unauthorized access.

4. VPN (Virtual Private Network): AES is used in VPNs to encrypt data transmitted over virtual private networks, ensuring privacy and security.

5. Smartphones and Mobile Devices: AES is used in securing data on smartphones and mobile devices, including data encryption for apps and files.

Conclusion:

The Advanced Encryption Standard (AES) is a highly effective and widely adopted encryption algorithm that provides strong security and efficiency for securing digital data. AES has several advantages, including its strong security against known attacks, efficiency in terms of computational resources, standardization for interoperability, flexibility in key sizes, and ease of implementation.

While AES has some limitations, such as potential vulnerability to future quantum computing attacks and the need for careful key management, these drawbacks are outweighed by its numerous benefits. AES's widespread adoption and acceptance as a global encryption standard makes it a trusted choice for securing sensitive information in various applications.

Overall, AES has proven to be a reliable and versatile encryption algorithm, playing a crucial role in ensuring the confidentiality and integrity of data in today's digital world.

Here's an example of how you might cite references for AES:

1. National Institute of Standards and Technology (NIST). "Announcing the ADVANCED ENCRYPTION STANDARD (AES)." Federal Information Processing Standards Publication 197, November 2001.

2. Daemen, Joan, and Vincent Rijmen. "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer, 2002.

3. Schneier, Bruce. "Applied Cryptography." John Wiley & Sons, 1996.

4. Ferguson, Niels, and Bruce Schneier. "Cryptography Engineering: Design Principles and Practical Applications." John Wiley & Sons, 2010.