Page No.
Date :

INTRODUCTION

The Advance Encryption Standard (AES) is a widely used symmetric encryption algorithm that secures electronic data. It was selected by the US National Institute of Standards and Technology (NIST) as a replacement for the olde Data Encryption standard in 2001.

AES is a block cipher that encrypts data in fixed size blocks of 128 bits, and it operates on a secret key that can be 128, 192 or 256 bits in length. It uses a series of rounds to transform plaintext into ciphetext, with the number of rounds depending on the key length.

AES is a symmetric encryption algorithm, which means that the same key is used for both encryption and decryption. This makes it faster and more difficult for asymmetric encryption, where two keys are used.

AES encrypts data in blocks of 128 bits at a time, and each block goes through a series of transformations known as rounds. The number of rounds depends on the key length, with more rounds required for longer key lengths.

AES supports three key sizes: 128 bits, 192 bits and 256 bits. The longer the key, the stronger the encryption. AES-256 is currently considered to be the most secure.

AES has been adopted as a standard by governments, banks, and other organizations around the world, and it is used to protect sensitive information in a wide range of applications.

One of the strengths of AES is that it has been extensively studied and analyzed by cryptography experts and no serious weaknesses have been found. This

gives organizations confidence that their data is secure when encrypted with AES.

AES was created to replace the older Data Encryption Standards (DES) which had become vulnerable to brute force attacks due to its small key size.

AES was designed through an open competition proven, with many different encryption algorithms submitted for consideration. After extensive evaluation by experts, AES was seleded as the winner due to its strong security, efficiency and flexibility.

AES was more secure than many older algorithms because it uses longer key lengths and more rounds of transformation. It has also been extensively studied and analyzed by cryptography expets, who have not found any serious weaknesses.

AES was invented by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted an algorithm called Rijndael to the AES competition. Their algorithm was ultimately selected as the winner known as AES.

Before the Data Encryption standard (DES) was the most widely used encryption algorithm. However, DES had become vulnerable to brute-force attacks due to its small key size, and it was no longer considered secure for many application. Other encryption algorithms, such as Triple DES and Blowfish, were also used but had their own limitations and weaknesses.

Comparisons:

1) Twofish : Twofish is a symmetric block cipher that also uses variable block sizes of 128, 192 or 256 bits and key size of upto 256 bits. Twofish has a more complex key schedule and uses large number of rounds than AES. AES preferred for its efficient implementation and widespread support, while Twofish may be preferred for its flexibility and potentially higher security.

2) Threefish : Threefish is a tweakable block cipher that designed to be used with Skein, a cryptographic hash function. It has a block ~~be~~ size of 256, 512 or 1024 bits and key length that can be upto 1024 bits. Threefish is known for encryption, authentication and key derivation.

3) Serpent : Serpent is another symmetric block cipher that uses variable block cipher sizes of 128, 192 and 256 bits and key size upto 256 bits. It is been analyzed and found to be secure against various attacks.

4) ChaCha20 : ChaCha20 is a stream cipher that uses 256-bit key a 64-bit ~~nonce~~ nonce. It is designed to be fast and secure authentication algorithm.

Versions of AES :

There are three versions of AES

1) AES-128 : This version of AES uses a 128-bit key to encrypt and decrypt data. It is the most commonly used version of AES.

2) AES-192 : This version of AES uses a 192-bit key to encrypt and decrypt data. It provides higher level security than AES-128, but is less commonly used.

3) AES-256 : This version of AES uses a 256-bit key to encrypt and decrypt data. It provides the highest level of security among the three versions of AES and is used for highly sensitive data.

The key size determines the strength of the encryption, with a larger key size providing stronger protection.

Applications of AES

1) WhatsApp : WhatsApp uses end-to-end encryption that relies on the AES to protect messages, voice calls and video calls between the users.

2) Dropbox : Secure cloud storage. Dropbox uses AES-256 to encrypt data at rest and in transit, including files, folders, and disk images stored in its server.

3) Google Drive, Microsoft OneDrive, iCloud : uses AES 128, AES 256 to protect files, folders, images, backups stored on its servers.

4) League of Legends : League of Legends is a popular multiplayer online battle arena game that uses AES to protect data packets transmitted between game servers.

5) Call of Duty, Counter Strike : Popular battle and shooter games uses AES to protect game data and prevent cheating.

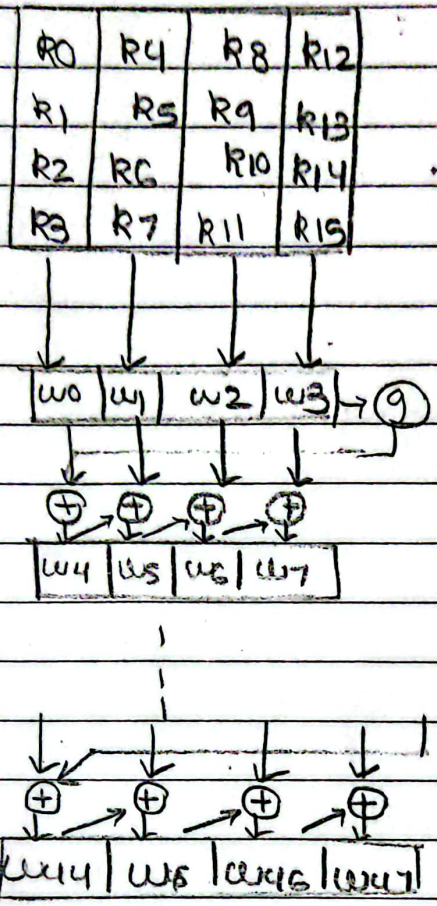
6) Amazon, eBay, Shopify : E-commerce platforms uses AES along with SSL/TLS encryption to protect customer data and personal details during online transactions.

KEY GENERATION ALGORITHM

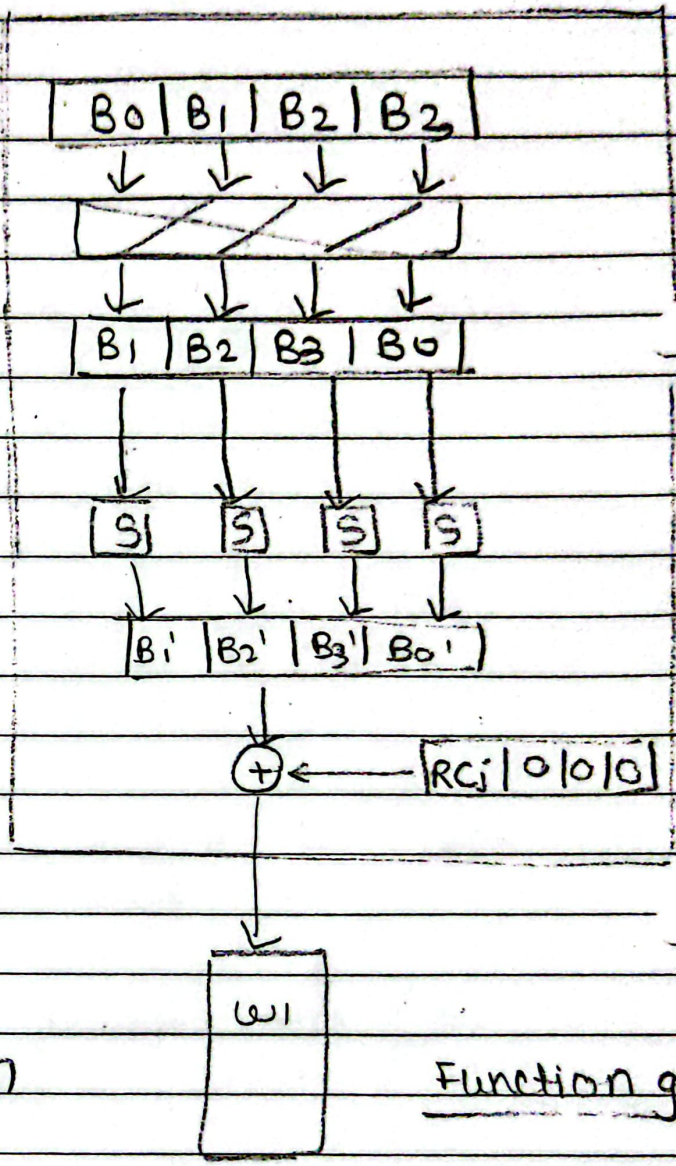
- Key scheduling is an important step in the AES (Advance Encryption standard) algorithm. and involves expanding the initial key into a set of round keys used in the encryption and decryption process.
- The AES key schedule generates a total of 11 subkeys of 128 bit each. This is sufficient to provide a four word round key for the initial Add Round key stage and each of the 10 rounds of the cipher.
- Also the AES algorithm supports three different key sizes: 128, 192 and 256 bits

- The key generation works as follows:
  1. The key is copied into the first four words of the expanded key.

  2. Each added word w[i] depends on the immediately preceding word, w[i-1] and the word four positions back, w[i-4]



AES KEY Expansion



Function g

3. For a word whose position in w array is a multiple of 4, a more complex function is used. The function g consist of the following sub functions :

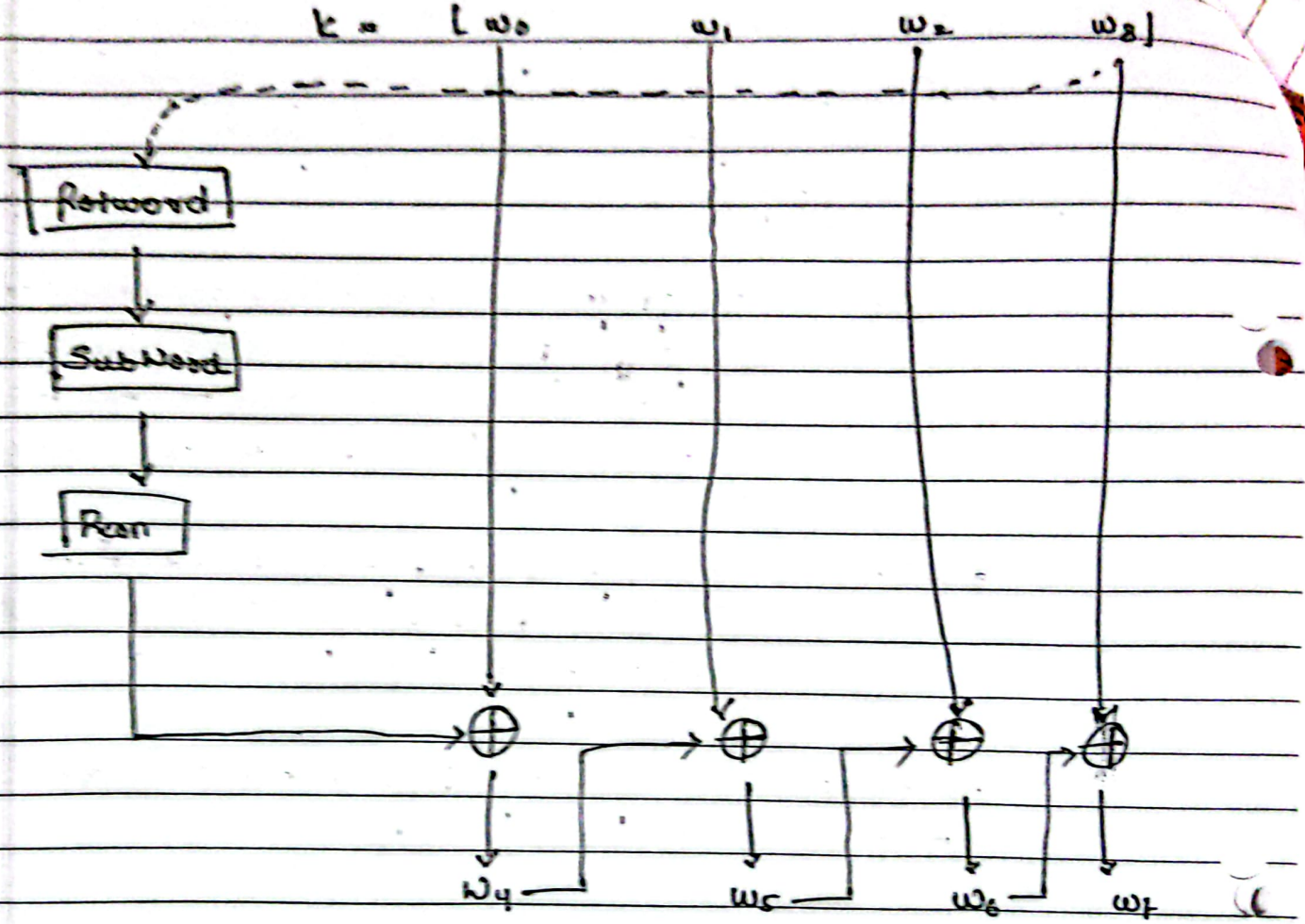
- Rotword : performs a one-byte circular left shift on a word. This means that an input word $[B_0, B_1, B_2, B_3]$ is transposed into $[B_1, B_2, B_3, B_0]$.

- Subword : performs a byte substitution on each byte of its input word using the s-box.

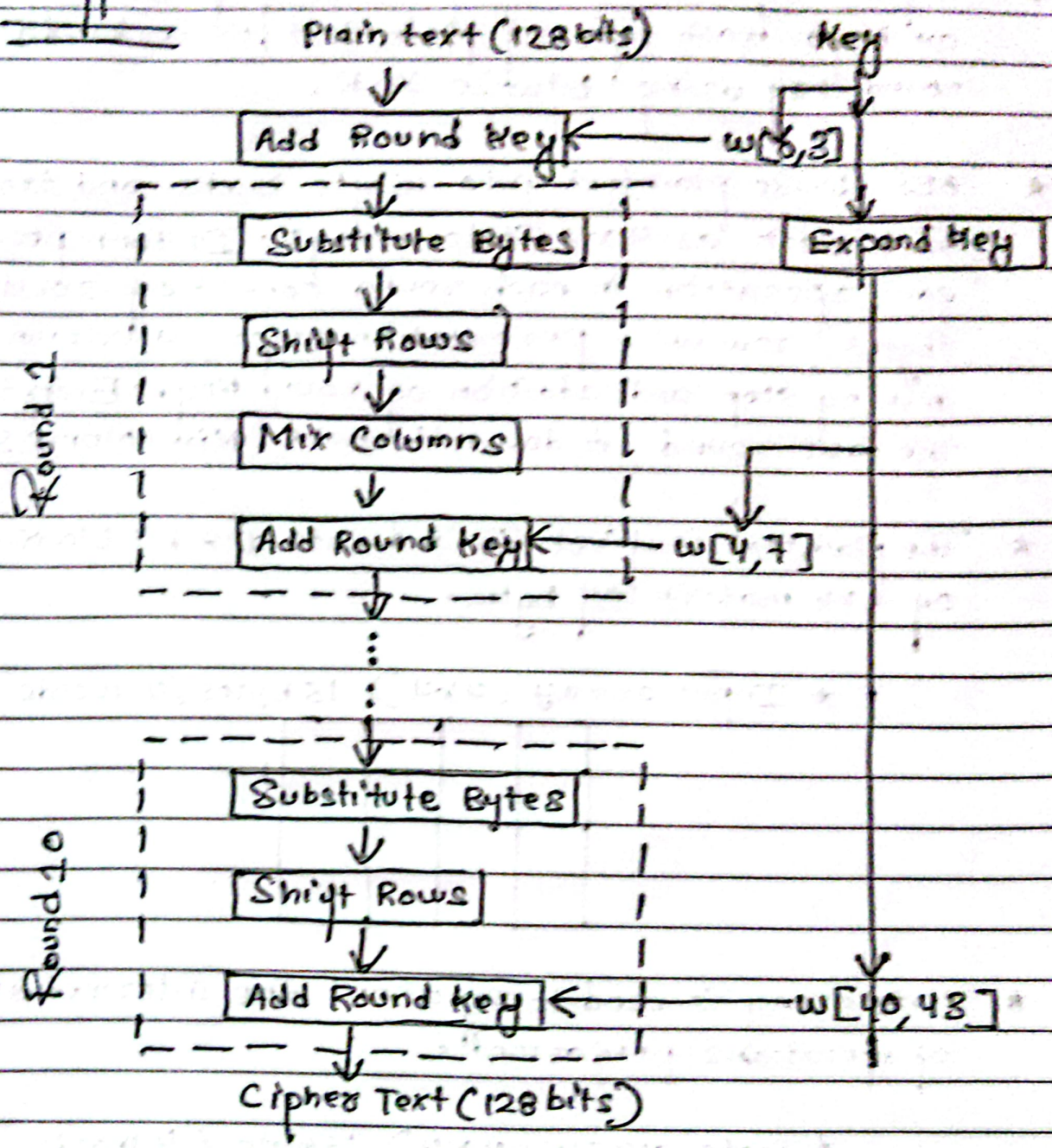
- The result of steps 1 and 2 is XORed with a round constant, Rcon[j].

4. The key transformation is repeated until the required number of round is generated.

AES Key Schedule.



Encryption :



★ The number of rounds are 10 when the encryption key is of 128 bit. It changes with the change in size of key.

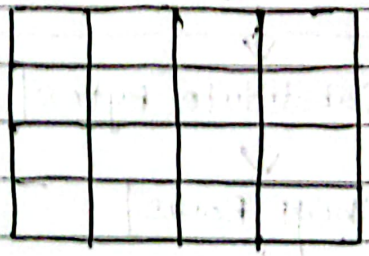
→ 10 rounds for 128 bit key
→ 12 rounds for 192 bit key
→ 14 rounds for 256 bit key.

* Before any round-based processing for encryption can begin each byte of plain text is combined with round key using bitwise XOR.

* AES divide plaintext into 16byte blocks and treats each block as 4x4 state arrays. It then performs four operation in each round consist of substitute bytes, row wise permutation steps, a column wise mixing step and addition of round key. Except for the last round, it doesn't have Mix columns step.

* The plaintext is first divided into 128 bit block consisting of 4x4 matrix of bytes.

* Input array (4x4) 16 bytes / 4 words

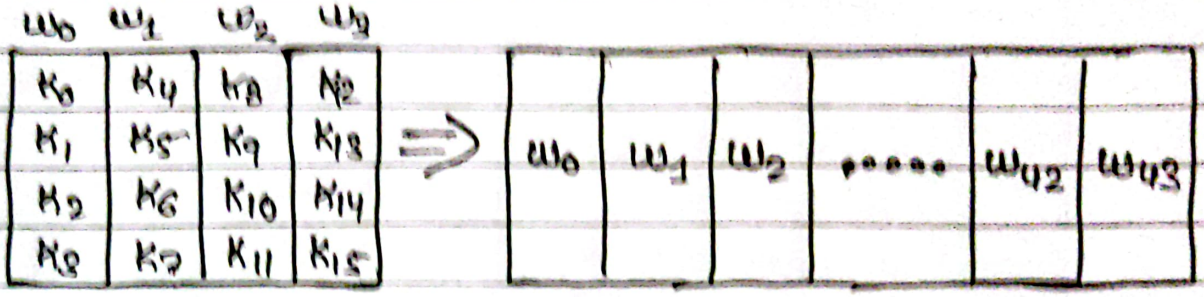


* State array is used to represent the intermediate result of operations performed.

* State array (4x4) 16byte / 4 words.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

★ The expand key operation expands the 4 word key into 44 words



Each 4 words from the expanded key is passed to Add Round Key where the data coming to Add Round Key and 4 words round key are XORed.

CASS ASSIGNMENT.

→ Four stages involved in encryption process of AES (Advanced Encryption Standard)

1. Substitute Bytes

In this stage, each byte of the 128 bit input block is replaced with a corresponding byte from a fixed 256-byte S-box. The S-box is generated using a specific mathematical formula & is designed to provide confusion in the encryption process. The substitution box is done using a fixed table called Rijndael S-box, which map each byte to a unique value.

2. Shift Rows.

In this stage the bytes in each row of the 128 bit i/p block are shifted to the left by different offsets. The first row is left unchanged second row is left shifted by 1, third row is left shifted by 2, & 4th row is left shifted by 3. This operation provides diffusion in the encryption process, as it spreads the data across multiple rows.

3. MIX COLUMNS:

In this stage, each column of 128 bit i/p block is transformed using matrix multiplication. The matrix used in this transformation is called Rijndael MixColumns matrix & is fixed. This operation provides further diffusion in the encryption process as it mixes the bits within each column.

4. Add Round Key:

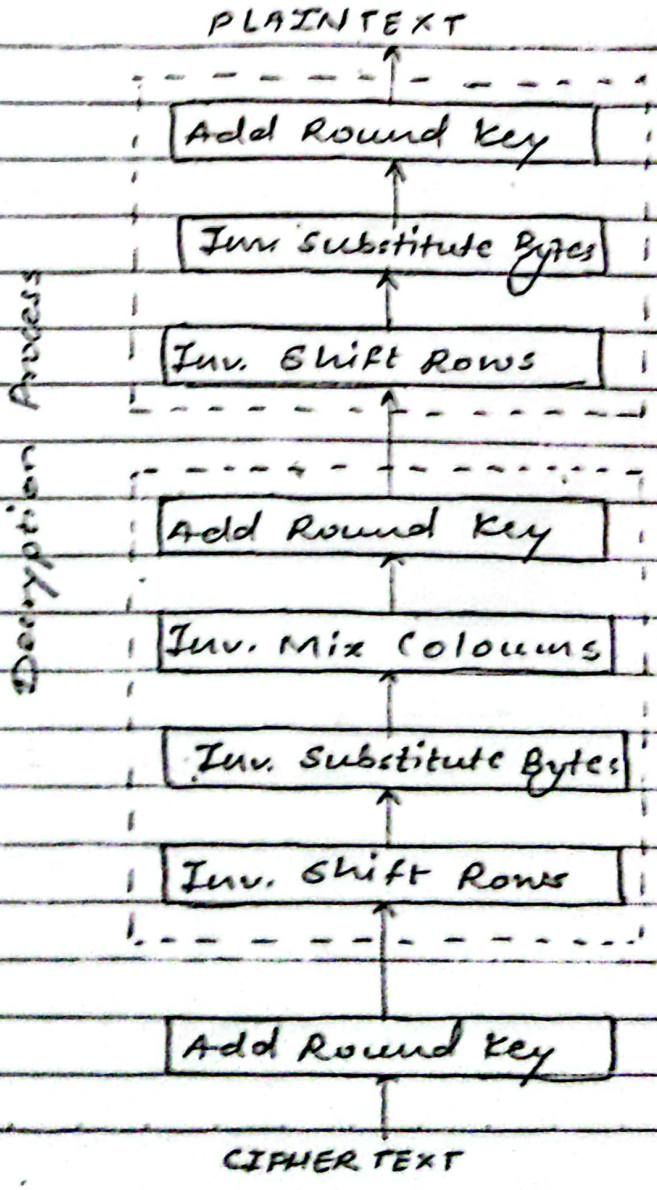
The 128 b input block is combined with round key using bitwise XOR. The round key generated, is from the original encryption key using a process called Key expansion. Each round of operation has its own unique round key, generated from original key using a fixed set of rules.

Overall, these 4 stages are repeated multiple times (depending on key size) to create multiple rounds of encryption. Final round omits the mixcolumn stage to simplify the decryption process. After final round of encryption resulting output is considered to be encrypted data that can be transmitted securely over an insecure channel.

Roll No. 2120 56

Decryption process in AES algorithm

The decryption process in AES algorithm is Essentially the reverse of encryption process. Given an encrypted block of data and secret key, the decryption process involves applying the inverse of each encryption step in reverse order using the same key schedule, but the round keys used in reverse order.



Steps involved in AES decryption :

1. Add Round Key

The current round key is combined with the encrypted matrix using XOR operation

2. Inverse of Mix Columns

Each column of matrix is multiplied by fixed matrix of coefficients to create a new matrix values.

3. Inverse Shift Rows

The rows of the matrix are shifted cyclically to the right by different amount (i.e. as per row number)

4. Inverse substitute Bytes

Each byte in matrix is replaced with a corresponding byte from an inverse S-box.

These steps are repeated for a fixed number of rounds (nine). After the final round which excludes provides resulting matrix represents the decrypted block of data.