Unit -2

Advanced Data Encryption Standard (AES)

- The principal drawback of 3DES is that the algorithm is relatively slow in software.
- The original DEA was designed for mid-1970s hardware implementation and does not produce efficient software code.
- 3DES, which has three times as many rounds as DEA, is correspondingly slower.
- A secondary drawback is that both DEA and 3DES use a 64-bit block size.
- For reasons of both efficiency and security, a larger block size is desirable.
- As a replacement, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have a security strength equal to or better than 3DES and significantly improved efficiency.
- In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits.
- Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.
- The two researchers who developed AES are both cryptographers from Belgium:

  Dr. JoanDaemen and Dr.Vincent Rijmen.

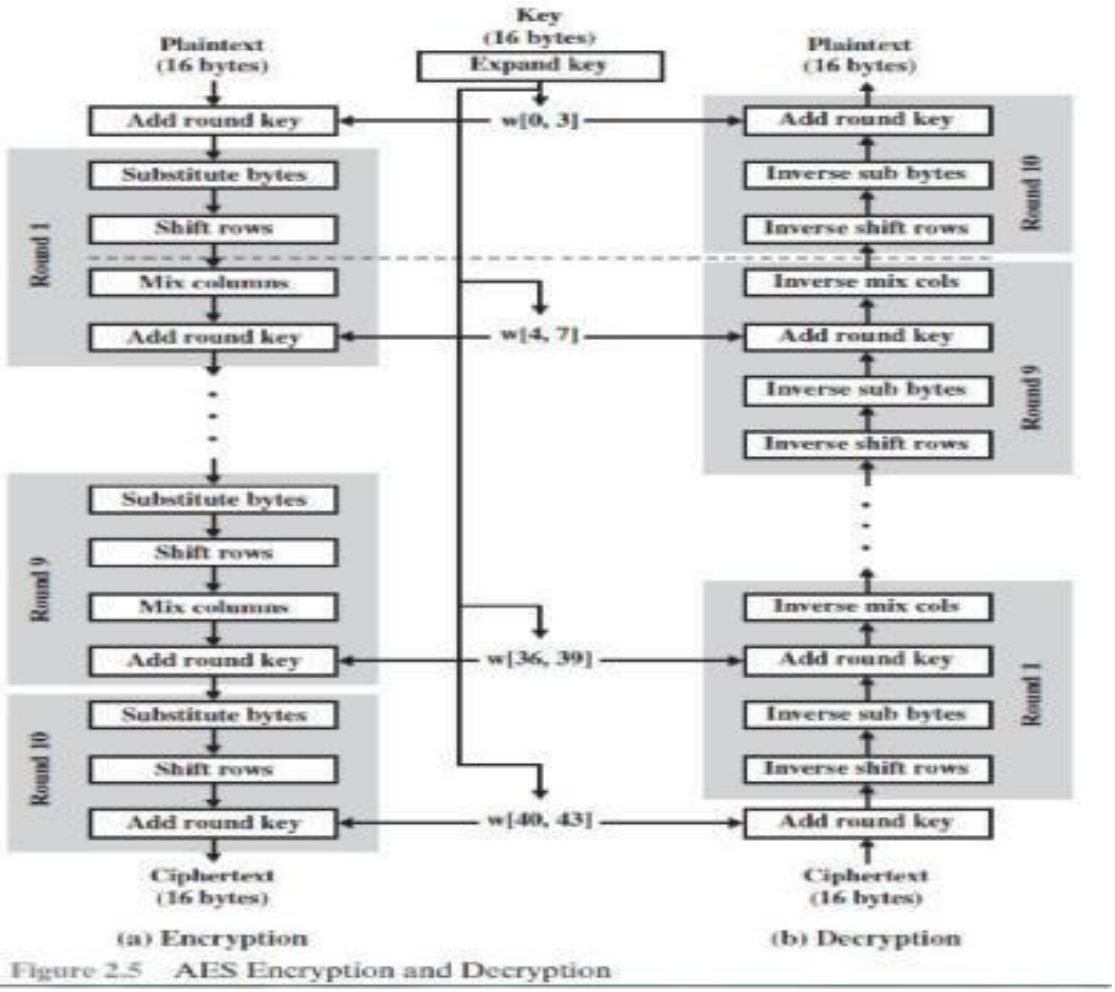


Figure 2.5 AES Encryption and Decryption

The following comments give some insight into AES.

One noteworthy feature of this structure is that it is not a Feistel structure, but processes the entire data block in parallel during each roundusing substitutions and permutation.

The key that is provided as input is expanded into an array of forty- four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round.

Four different stages are used, one of permutation and three of substitution:

substitution of the block.

- **Shift rows:**A simple permutation that is performed row by row.
- **Mix columns:**A substitution that alters each byte in a column as afunction of all of the bytes in the column.

Add round key:A simple bitwise XOR of the current block with a portion ofthe expanded key.

The structure is quite simple. For both encryption and decryption, the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.

Only the **Add Round Key** stage makes use of the key. For this reason, the cipherbegins and ends with an Add Round Key stage.

The Add Round Key stage by itself would not be tough. The other three stages together scramble the bits, but by themselves, they would provide no security because they do not use the key.

Each stage is easily reversible. For the Substitute Byte, Shift Row, and Mix Columns stages, an inverse function is used in the decryption algorithm.

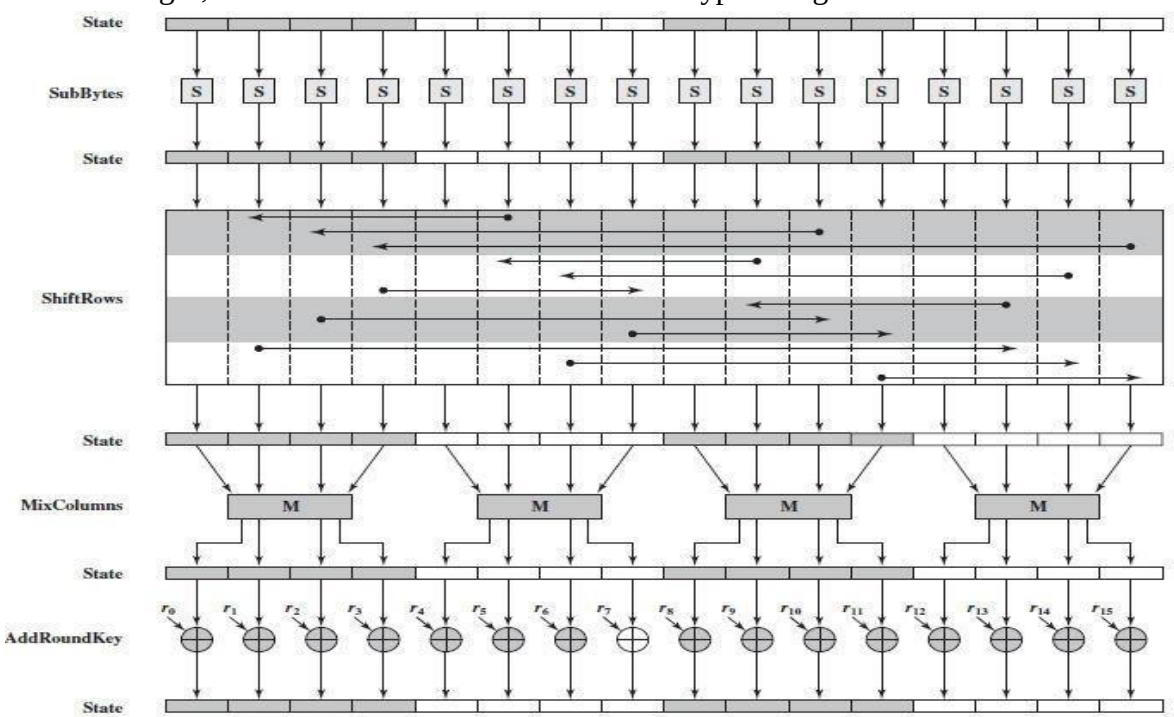


Figure 2.6 AES Encryption Round

Other Symmetric Block Ciphers:

International Data Encryption Algorithm (IDEA)

23 128-bit key

24 Used in PGP

Blowfish

23 Easy to implement

24 High execution speed

25 Run in less than 5K of memory

RC5

5888 Suitable for hardware and software
5889 Fast, simple
5890 Adaptable to processors of different word lengths
5891 Variable number of rounds
5892 Variable-length key
5893 Low memory requirement
5894 High security
5895 Data-dependent rotations

5889 Cast-128

5888 Key size from 40 to 128 bits

5889 The round function differs from round to round

2.1 Cipher block modes of operation:

1. block ciphers encrypt fixed size blocks
   eg. DES encrypts 64-bit blocks, with 56-bit key
2. To apply DES in variety of applications, five **"**modes of application**"** havebeen defined.
   a. Electronic Code book(ECB)
   b. Cipher Block chaining(CBC)
   c. Cipher Feedback(CFB)
   d. Output Feedback(OFB)
   e. Counter(CTR)
3. These modes are intended for use with any symmetric block cipher including DESand AES.

Electronic Code Book:

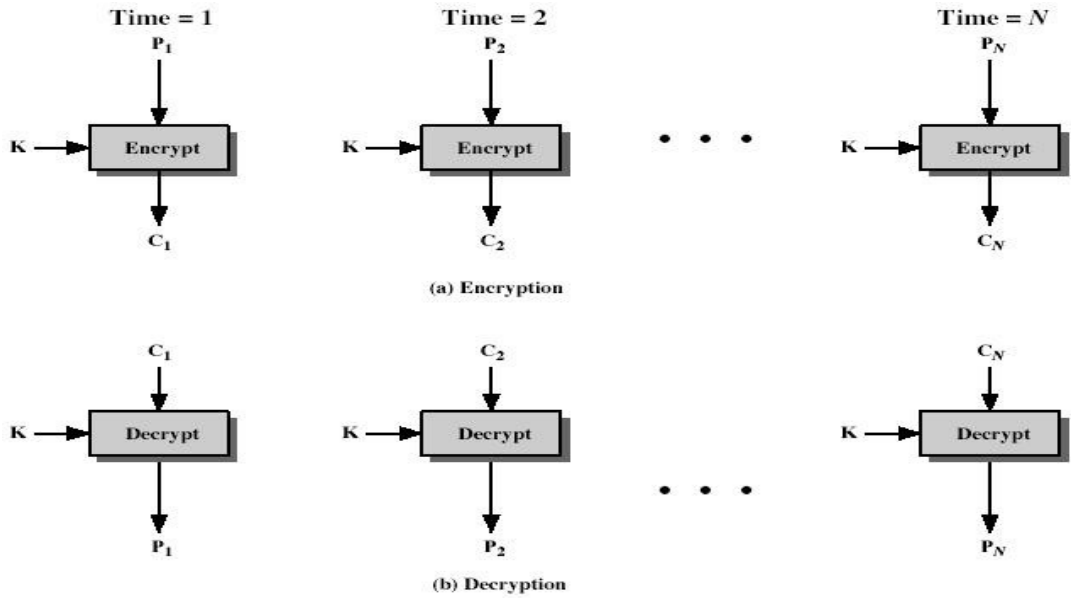
Message is broken into independent blocks which are encrypted.
Each block is a value which is substituted, like a codebook, hence name.5890Each block is encoded independently of the other blocks.

- Ci = DESK1 (Pi)

uses: secure transmission of single values.

Advantages and Limitations of ECB:

Repetitions in message may show in cipher text
if aligned with message block
particularly with data such graphics
or with messages that change very little, which become a code-book analysis problem
Weakness due to encrypted message blocks being Independent.5893 main use is sending a few blocks of data

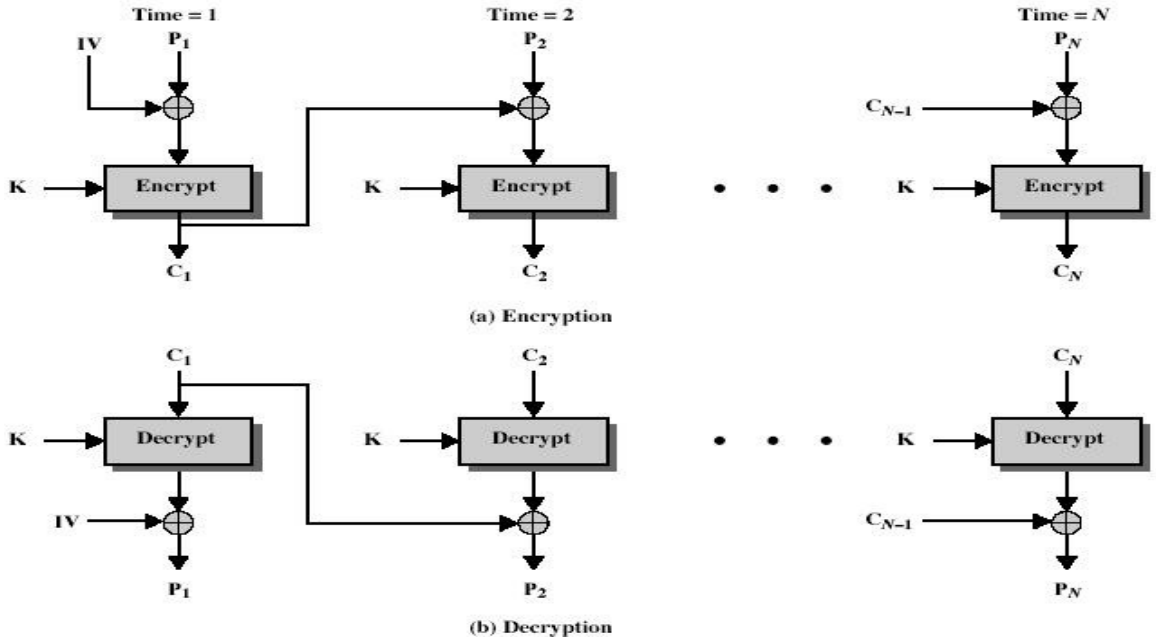


Cipher Block Chaining (CBC):

- Message is broken into blocks.
- but these are linked together in the encryption operation.
- Each previous cipher blocks is chained with current plaintext block, hence name.
- Use Initial Vector (IV) to start process.
- Ci = DESK1(Pi XOR Ci-1)5 C-1 = IV
- Uses: bulk data encryption, authentication.

Advantages and Limitations of CBC:

- each ciphertext block depends on **all** message blocks
- thus a change in the message affects all ciphertext blocks after the change as well asthe original block
- need **Initial Value** (IV) known to sender & receiver
  - however if IV is sent in the clear, an attacker can change bits of the firstblock, and change IV to compensate
  - hence either IV must be a fixed value or it must be sent encrypted in ECBmode before rest of message
- at end of message, handle possible last short block
  - by padding either with known non-data value (eg nulls)
  - or pad last block with count of pad size
- eg. [b1 b2 b3 0 0 0 0 5] □ 3 data bytes, then 5 bytes pad+count

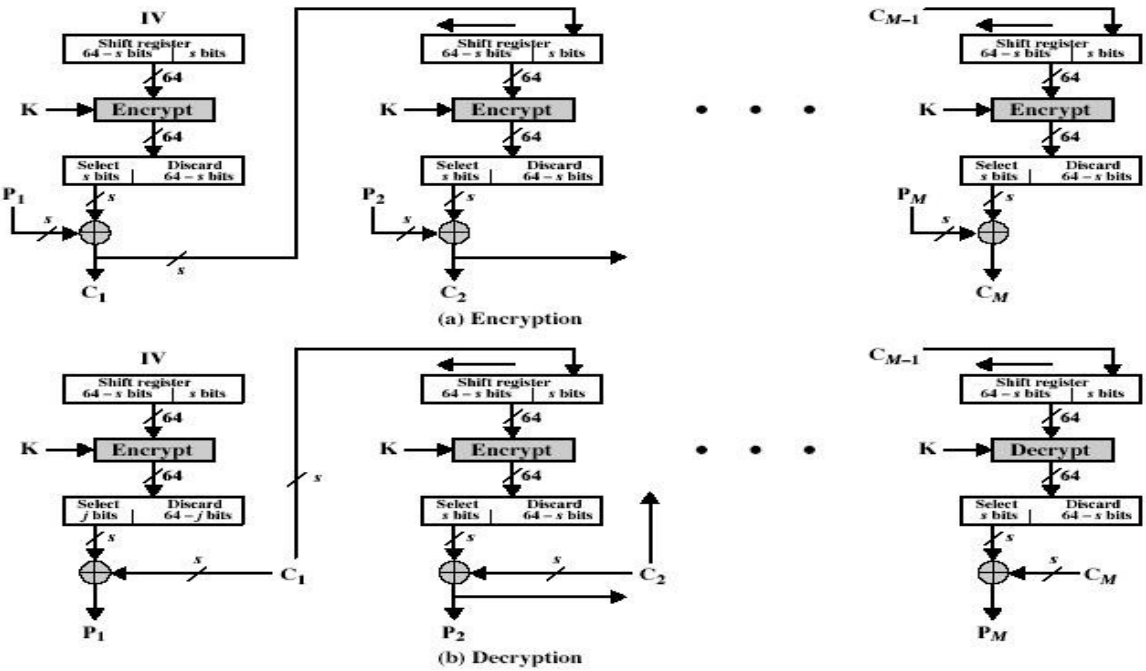


Cipher Feedback (CFB):

- Message is treated as a stream of bits.
- Added to the output of the block cipher .
- Result is feed back for next stage (hence name).
- Standard allows any number of bit (1,8 or 64 or whatever) to be feed back
- denoted CFB-1, CFB-8, CFB-64 etc
- Is most efficient to use all 64 bits (CFB-64).
    - $C_i = P_i$ XOR $DES_{K1}(C_{i-1})$ C_{-1} = IV
- Uses: stream data encryption, authentication.

Advantages and Limitations of CFB:

- Appropriate when data arrives in bits/bytes .
- Most common stream mode.
- Note that the block cipher is used in encryption mode at both ends.
- Errors propagate for several blocks after the error.



Output FeedBack (OFB):

The alternative to CFB is OFB. Here the generation of the "random" bits is independentof the message being encrypted. The advantage is that firstly, they can be computedin advance, good for bursty traffic, and secondly, any bit error only affects a single bit. Thus this is good for noisy links (eg satellite TV transmissions etc).

Message is treated as a stream of bits

Output of cipher is added to message

Output is then feedback (hence name)

Feedback is independent of message

Can be computed in advance

$C_I = P_I \text{ XOR } O_I$

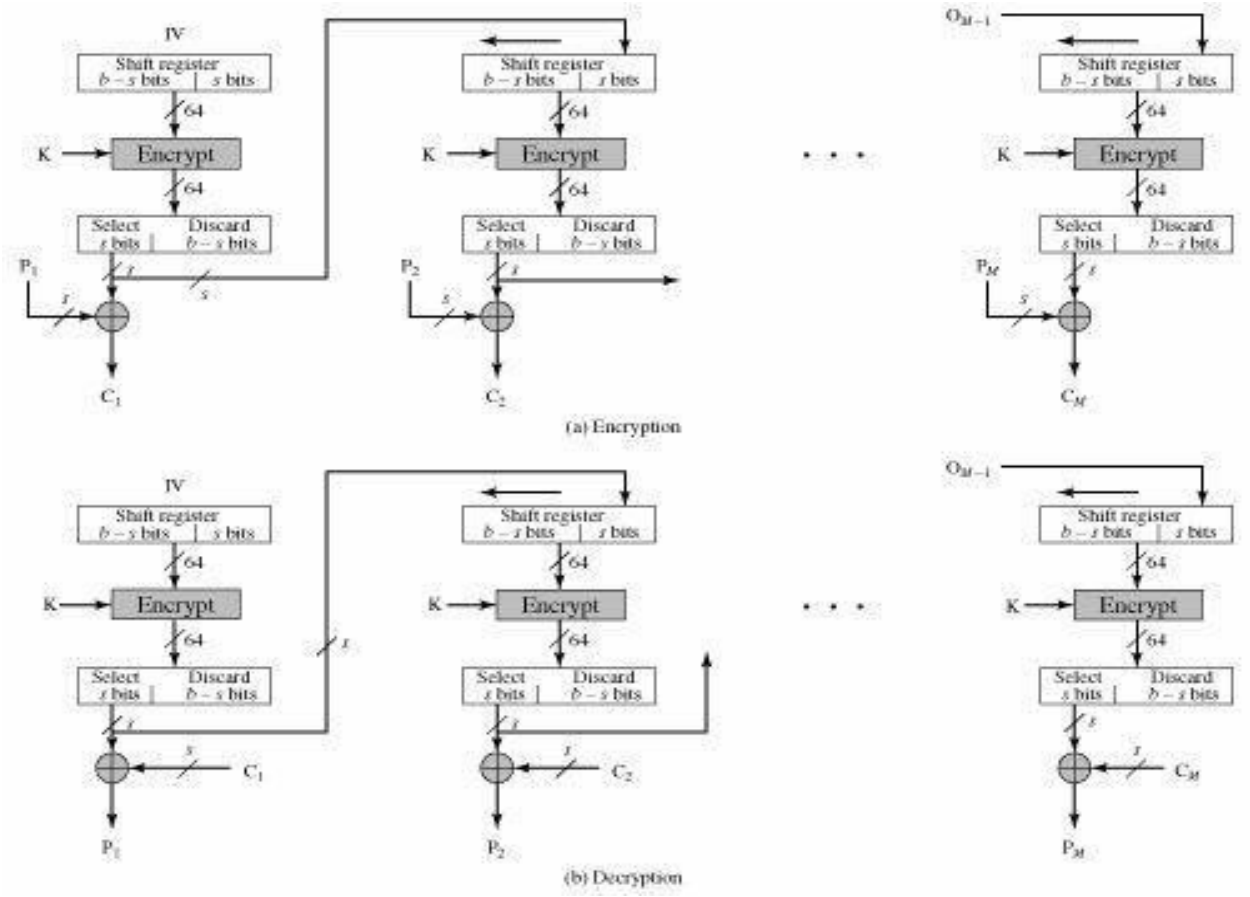
$O_I = DES_{K1}(O_{I-1})$

$O_{-1} = IV$

Uses: stream encryption over noisy channels.

Advantages and Limitations of OFB:

- Used when error feedback a problem or where need to encryptions before message isavailable.
- Superficially similar to CFB.
- But feedback is from the output of cipher and is independent of message.
- sender and receiver must remain in sync, and some recovery method is needed toensure this occurs
- Originally specified with m-bit feedback in the standards.
- Subsequent research has shown that only OFB-64 should ever be used.



Comparison of Different Modes

Operation Mode	*Description*	*Type of Result*	*Data Unit Size*
ECB	Each n-bit block is encrypted independently with the same cipher key.	Block cipher	n
CBC	Same as ECB, but each block is first exclusive-ored with the previous ciphertext.	Block cipher	n
CFB	Each r-bit block is exclusive-ored with an r-bit key, which is part of previous cipher text	Stream cipher	$r \leq n$
OFB	Same as CFB, but the shift register is updated by the previous r-bit key.	Stream cipher	$r \leq n$
CTR	Same as OFB, but a counter is used instead of a shift register.	Stream cipher	n