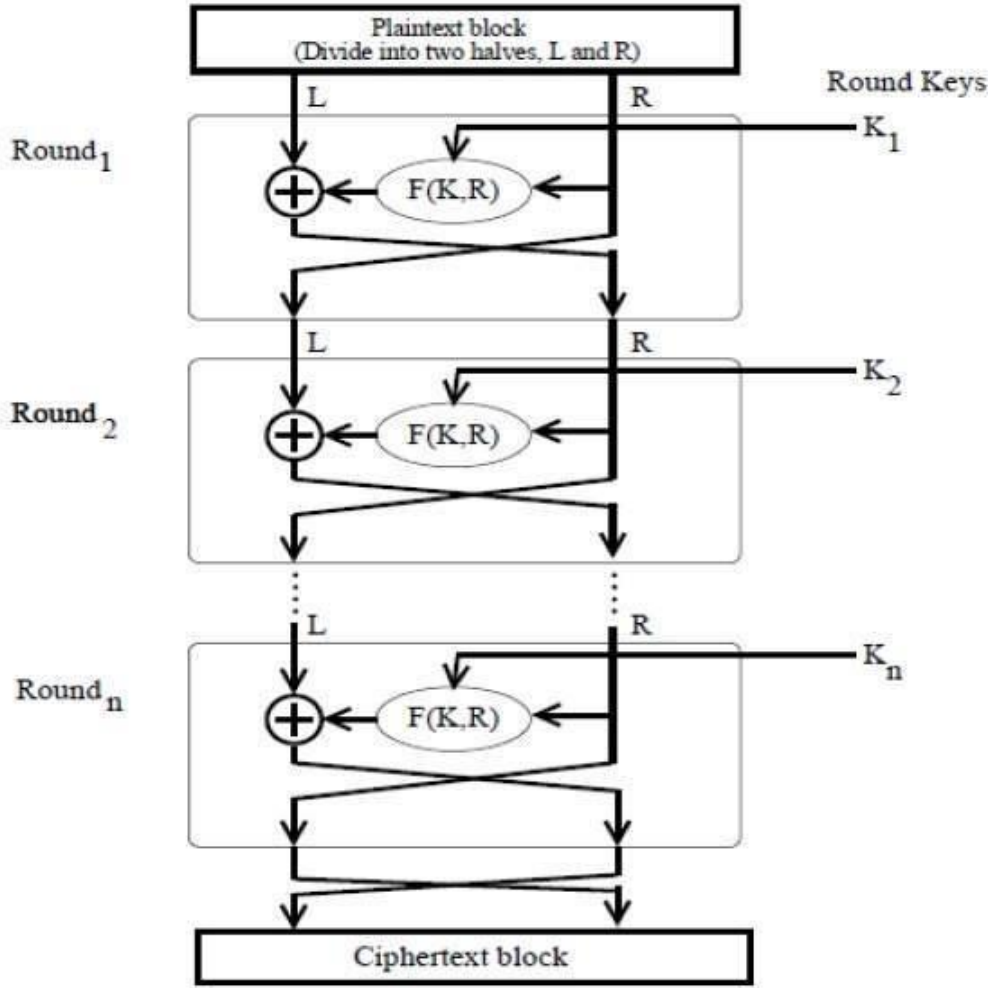
AES Cipher Block

Compiled by - Nazmus Sakib Akash

Some Background Into Feistel Block Cipher Model



Example:
DES Cipher

Feistel Block Model Continued (Encryption)

- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function ‘f’ that takes two input − the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- Above substitution and permutation steps form a ‘round’. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function ‘f’. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

Feistel Block Model Continued (Decryption)

Decryption Process

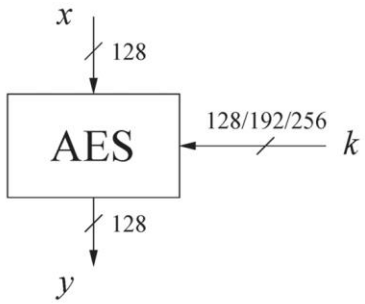
The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of ‘L’ and ‘R’ in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

AES Cipher Block

- NOT a Feistel Block Model.
- AES encrypts all 128 bits of the datapath in 1 round.



The number of rounds depends on the chosen key length:

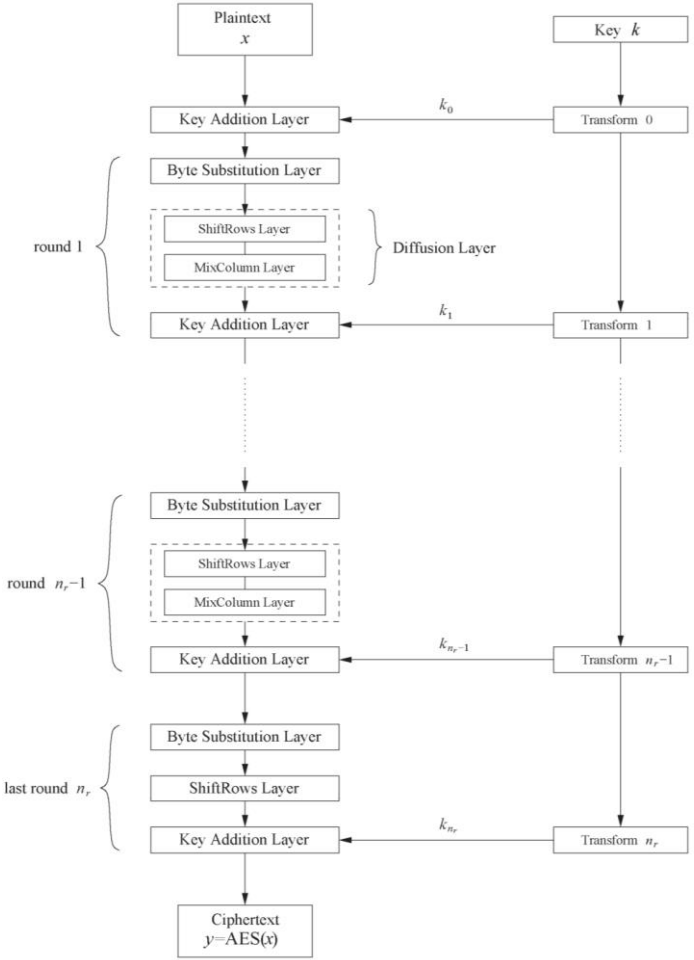
Key length (bits)	Number of rounds
128	10
192	12
256	14

AES: Overview

- Iterated cipher with 10/12/14 rounds.
- Each round consists of “Layers”
  - Byte Substitution -> provides confusion
  - ShiftRow, MixCol -> provides diffusion
  - Key Addition layer
  - Key Scheduling

Confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible.

Diffusion refers to the property that the redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. Diffusion means that the output bits should depend on the input bits in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudo-random manner.



AES: Algorithm

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial round key addition:
   - AddRoundKey—each byte of the state is combined with a byte of the round key using bitwise xor.

3. 10, 12 or 14 rounds:
   - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   - MixColumns—a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
   - AddRoundKey

4. Final round (making 10, 12 or 14 rounds in total):
   - SubBytes
   - ShiftRows
   - AddRoundKey

Internal Structure of AES

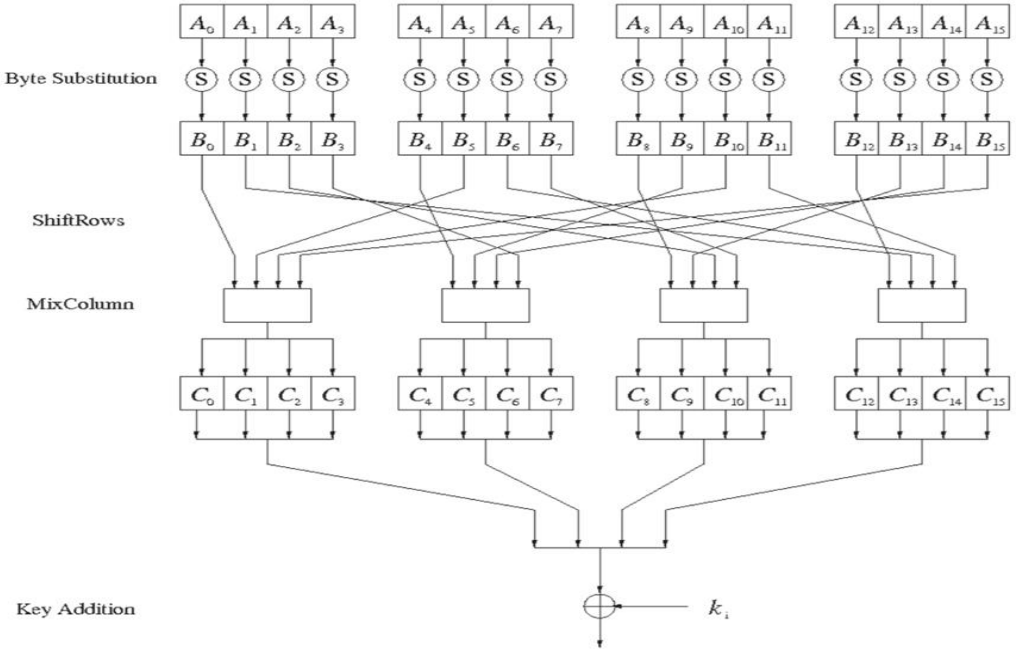
- AES is a byte-oriented cipher
- The state *A* (i.e., the 128-bit data path) can be arranged in a 4x4 matrix:

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

with $A_0, \ldots, A_{15}$ denoting the 16-byte input of AES

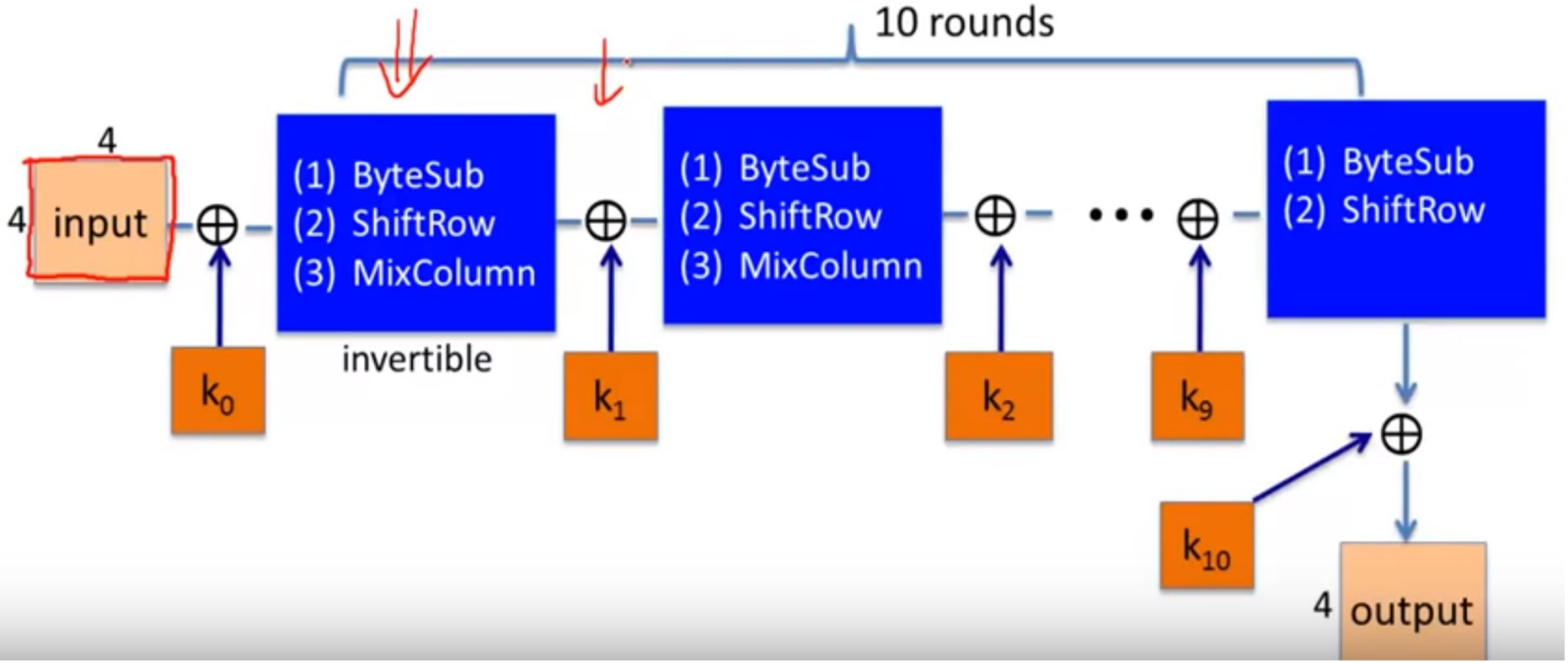
Internal Structure of AES

- Round function for rounds 1,2,…,n_{r-1}:



- Note: In the last round, the MixColumn tansformation is omitted

AES-128 schematic



What happens inside the layers?

https://youtu.be/NHuibtoL_qk?t=1945

Security

- **Brute-force attack:** Due to the key length of 128, 192 or 256 bits, a brute-force attack is not possible
- **Analytical attacks:** There is no analytical attack known that is better than brute-force
- **Side-channel attacks:**
  - Several side-channel attacks have been published
  - Note that side-channel attacks do not attack the underlying algorithm but the implementation of it

Lessons Learned

- AES is a modern block cipher which supports three key lengths of 128, 192 and 256 bit. It provides excellent long-term security against brute-force attacks.
- AES has been studied intensively since the late 1990s and no attacks have been found that are better than brute-force.
- AES is not based on Feistel networks. Its basic operations use Galois field arithmetic and provide strong diffusion and confusion.
- AES is part of numerous open standards such as IPsec or TLS, in addition to being the mandatory encryption algorithm for US government applications. It seems likely that the cipher will be the dominant encryption algorithm for many years to come.
- AES is efficient in software and hardware.