The Advanced Encryption Standard

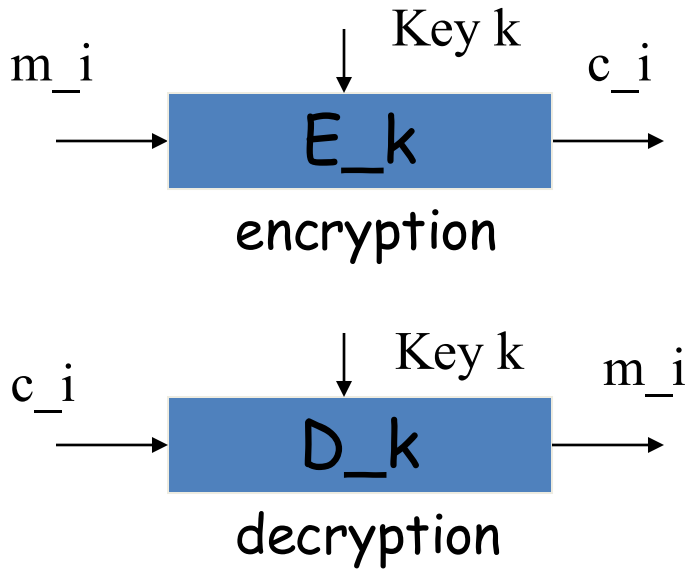
Cunsheng Ding
HKUST, Hong Kong, CHINA

The Preparations Done Before and the Objective of This Lecture

- One-key block ciphers were defined in Lecture 4.
- Linear and nonlinear functions were studied in Lecture 5.
- An iterative design paradigm and an example cipher were introduced in Lecture 6.
- The DES, 3DES and AES were **briefly** introduced in Lecture 7.
- The objective of this lecture is to introduce AES to certain technical details.

One-Key Block Ciphers

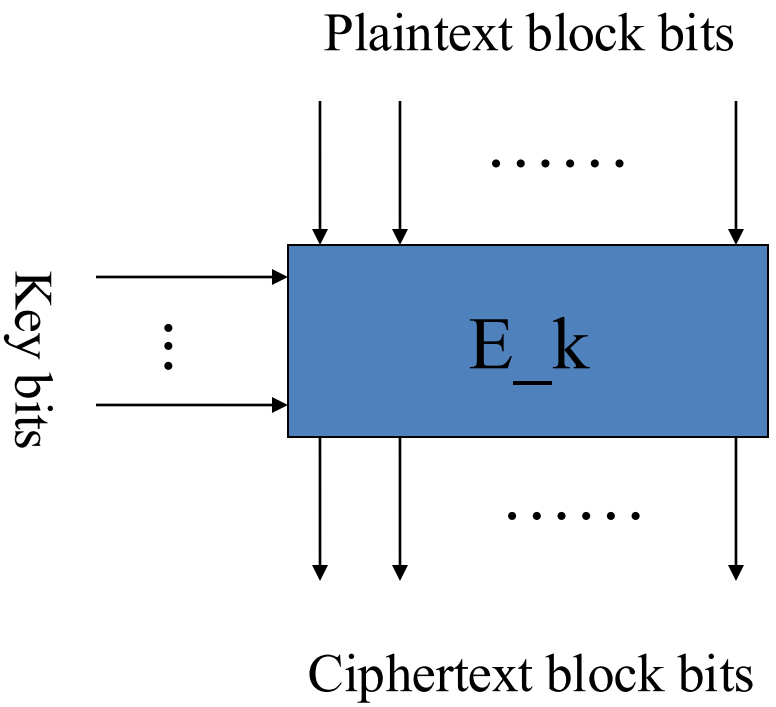
Pictorial discription



- Definition:
  - (M, C, K, E_k, D_k)
  - the ciphertext c=E_k(m) depends only on m and k.
- How to design a secure and practical block cipher?
  - Secure w.r.t. ciphertext-only attacks
  - Secure w.r.t. known-plaintext attacks
  - It should be practical (rather than the one-time-pad cipher)

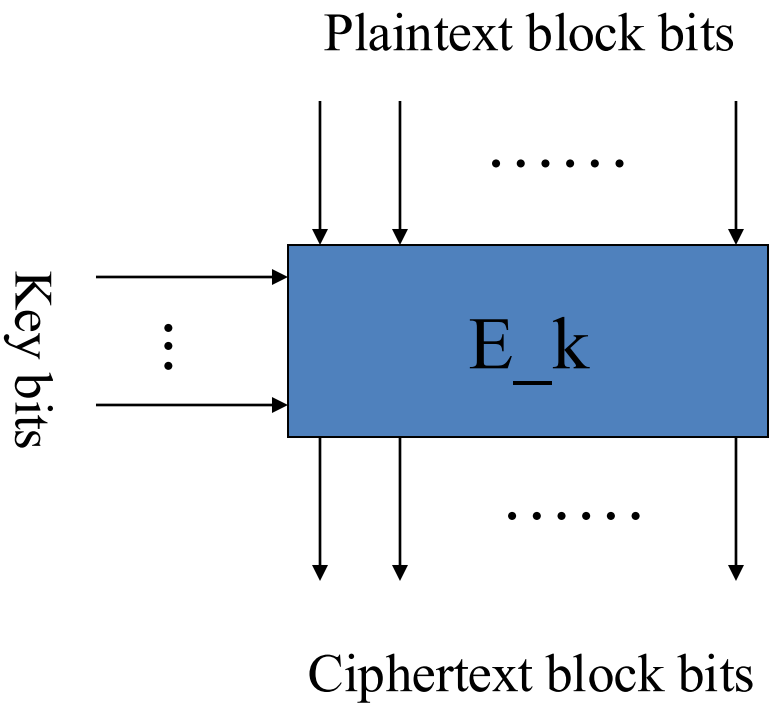
Shannon's Idea of Diffusion

- Good diffusion
  - Every plaintext block bit is involved in many ciphertext block bits.
  - Every key bit is involved in many ciphertext block bits.
  - Linear and nonlinear functions are used for diffusion purpose.



Shannon's Idea of Confusion

- Good confusion
  - Every ciphertext block bit is a function of plaintext block bits and key bits.
  - These functions should be very complex in format.
  - Nonlinear functions are necessary for confusion.



The Design Paradigm of Block Ciphers

- Linear functions are **mainly** used for diffusion.
- Nonlinear functions are **mainly** used for confusion.
- A simple round function is iterated for a certain number of times.
- Most one-key block ciphers are designed by following these design strategies.

The Advanced Encryption Standard (AES)

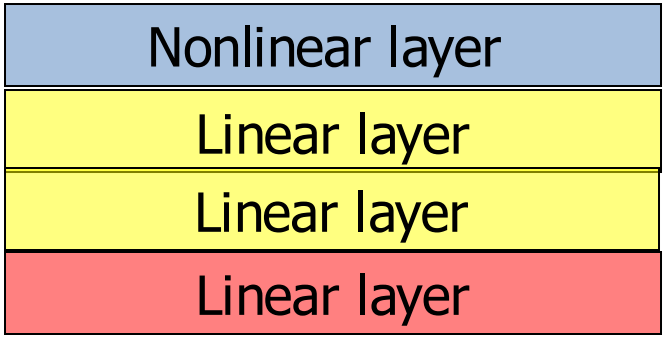
- In the 90's, a replacement for DES was needed because the DES is subject to exhaustive key search attacks.
- The NIST of the USA issued a call for ciphers in 1997.
- After three rounds of selection, "Rijndael" was selected as the AES in Oct-2000.
- It was issued as a Federal Information Processing Standard in Nov-2001.

AES Design Requirements

- A one-key block cipher.
- 128-bit plaintext block.
- 128/192/256-bit keys.
- Stronger & faster than Triple-DES.
- Active life of 20-30 years.
- Efficient in both software and hardware implementations.
- Simple in design.
- Suitable for smart cards (memory requirement).

Rijndael: Design Techniques

- It uses Shannon's idea of diffusion and confusion
- It was designed by following the design paradigm introduced in Lecture 6
- The round function has the form



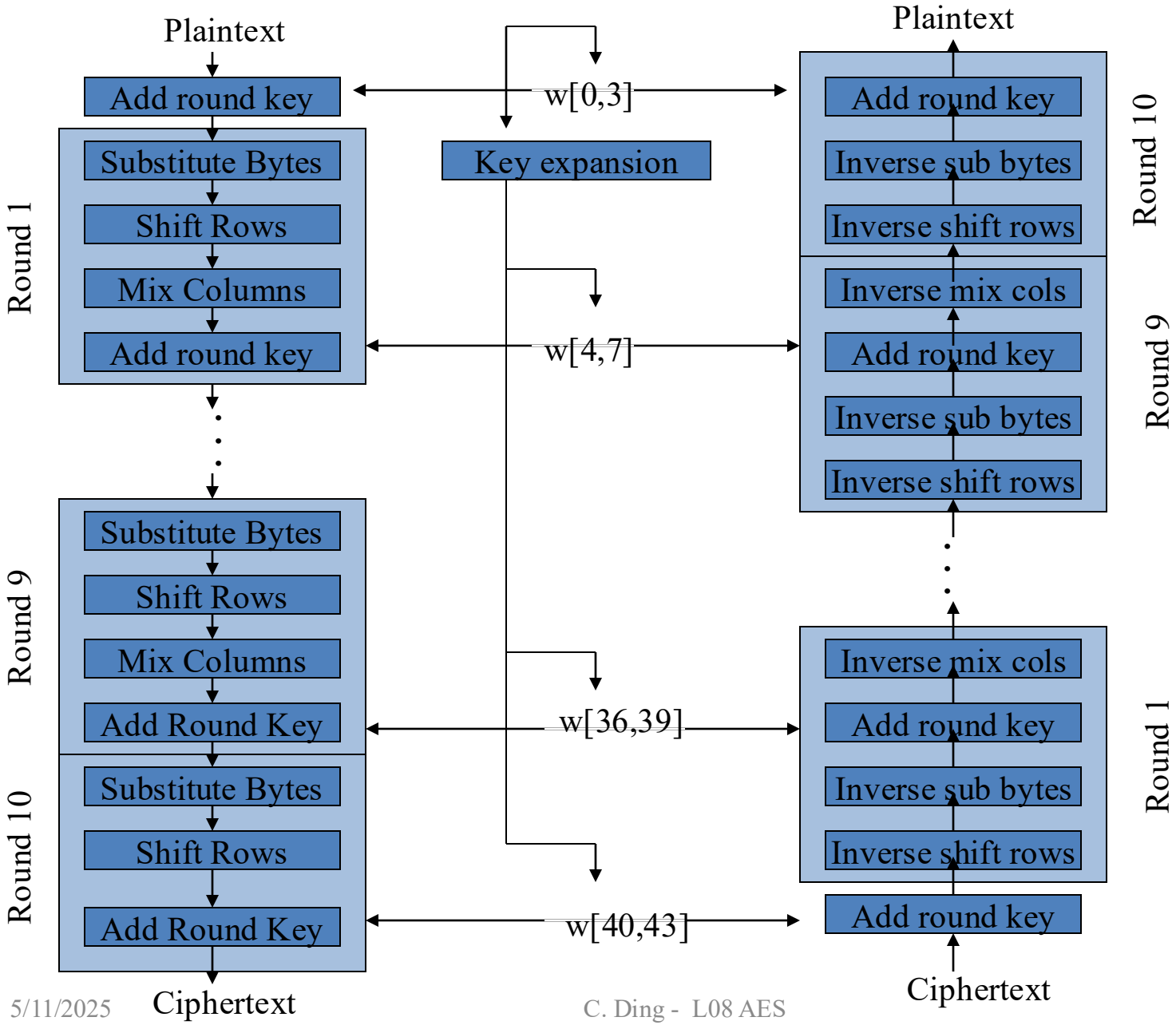
Rijndael: Key and Block Size

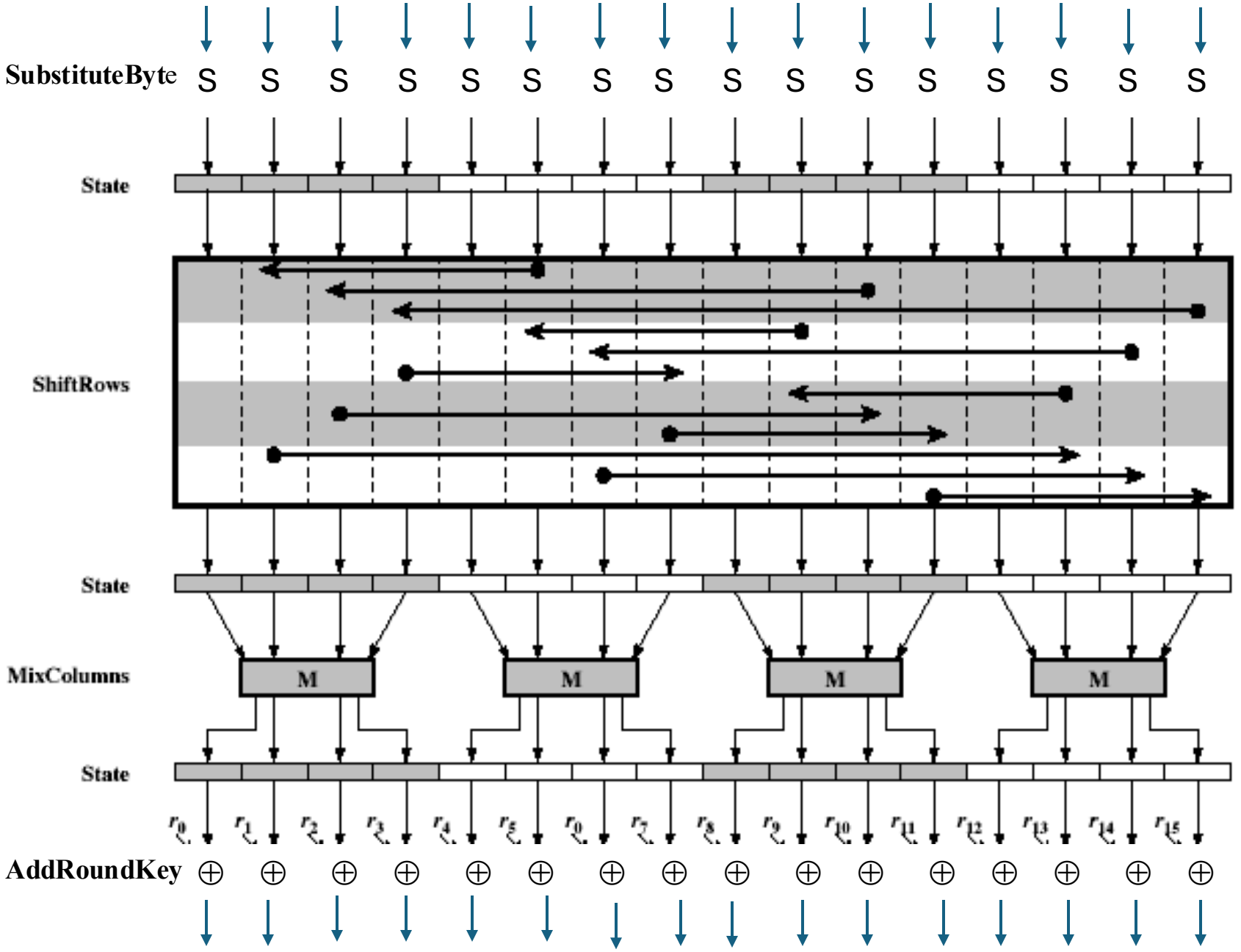
Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128

The Internal Structure of AES

- We will now consider the default case, i.e., the secret key has 128 bits.
- In this case, there are an initial round and 10 rounds of iteration.
- We will not introduce every small building block, as it is too technical to do so. But references for them will be provided.

AES Encryption & Decryption





AES Round Function

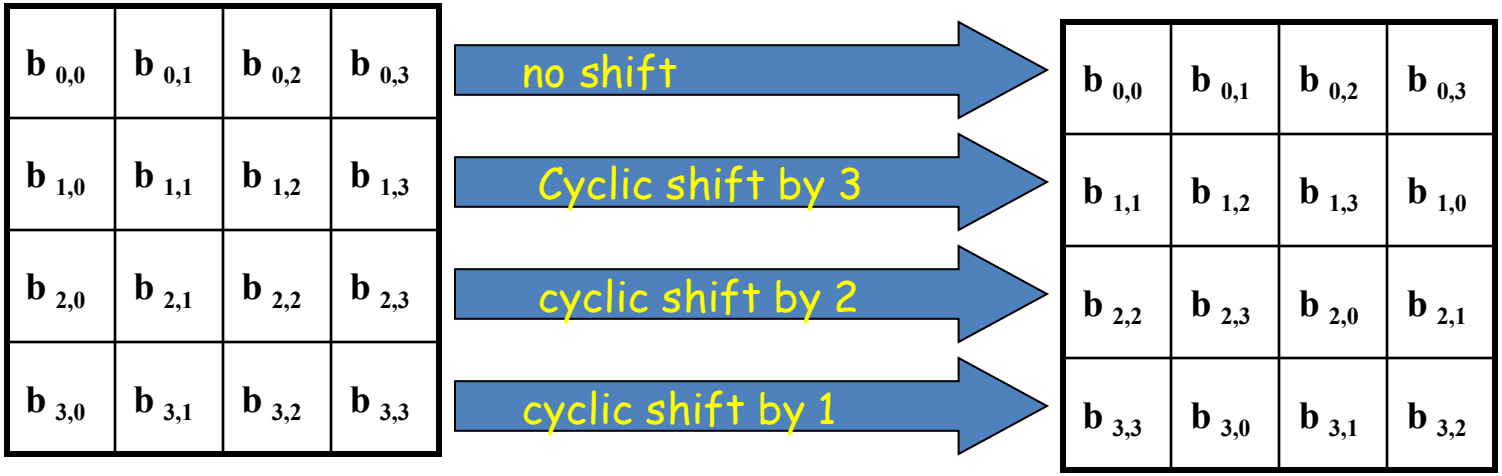
Round Function: SubstituteByte

- The "SubstituteByte" function (denote by S in the picture in the previous slide) acts on individual bytes of the State.
- It maps a byte to a byte.
- It is a one-to-one nonlinear function.
- It is mainly used for providing confusion.
- For details see

https://www.cse.ust.hk/faculty/cding/COMP3631/SLIDES/GF256.pdf

- You are not required to read technical details of the permutation "SubstituteByte".

Round Function : ShiftRows



- "ShiftRows" operates on the bytes of the State.
- It maps 16 bytes to 16 bytes.
- It is a one-to-one linear function.
- The purpose is to provide inter **column diffusion**.

Round Function : MixColumns

- It maps 4 bytes to 4 bytes.
- It is a one-to-one linear function.
- It is designed with "coding theory".
- It is mainly used for providing diffusion.
- For details, see

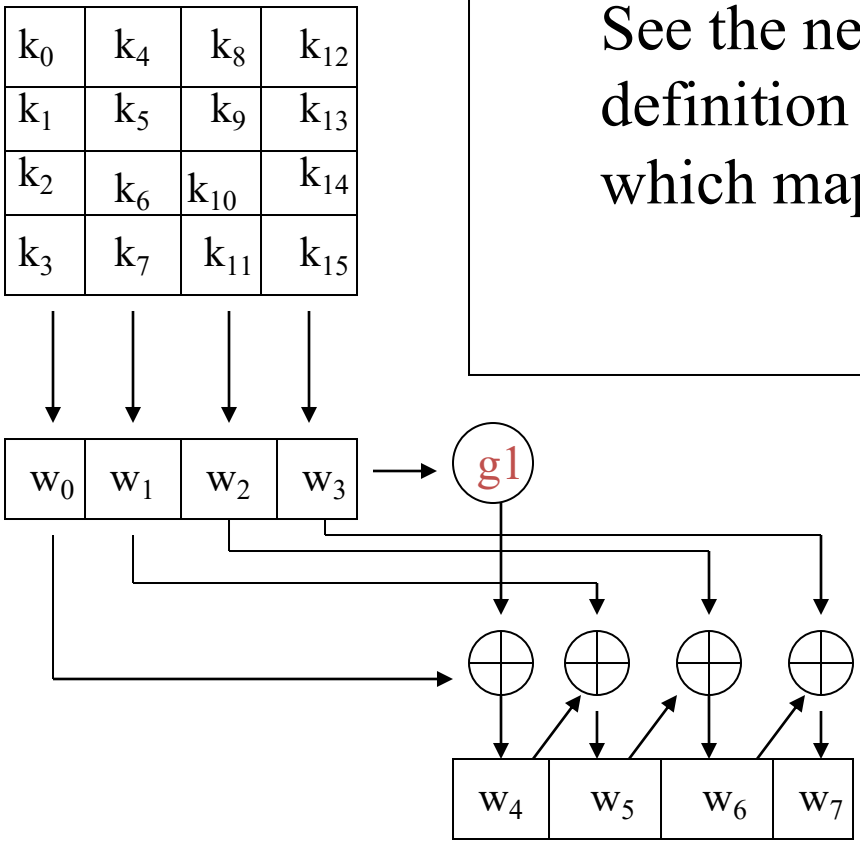
https://www.cse.ust.hk/faculty/cding/COMP3631/SLIDES/GF256.pdf

- You are not required to read details of this function "MixColumns".

Round Function : AddRoundKey

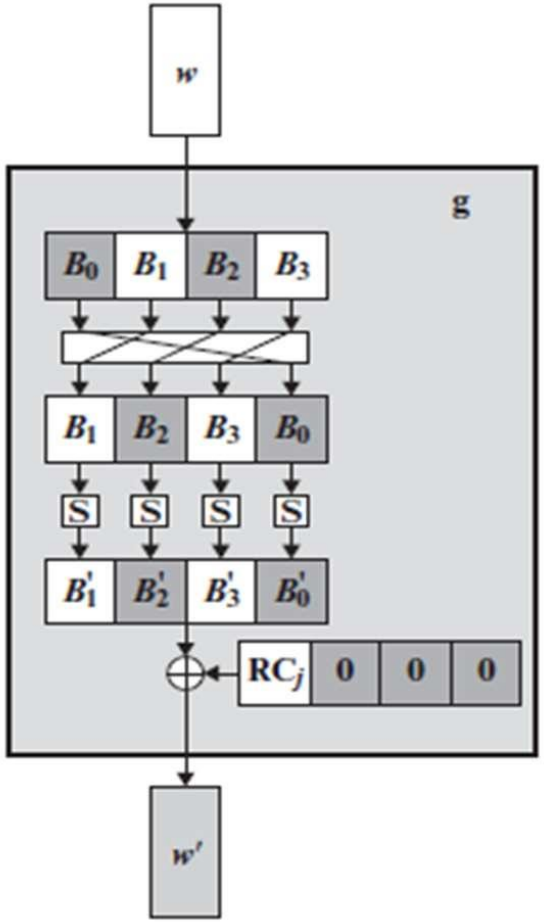
- "AddRoundKey" is the bitwise exclusive-or of the Round Key and the State.
- The purpose is to make the round function key-dependent.
- It is a linear function $x \oplus y$ for any fixed y.

AES Key Expansion



See the next page for the definition of the function g_i, which maps a word to a word

The Function g_j



- For each j in {1,2, …, 10}, the function

  g_j(w)=g(w)⊕(RC_j, 0, 0, 0).
- Each RC_j is a round constant for computing the j-th round key.
- RC_j has one byte
- For definition of RC_j, see:

https://en.wikipedia.org/wiki/AES_key_schedule

The Decryption Function

- It is the inverse function of the encryption function.
- It is not identical to the encryption function.
- We will not talk about the decryption process.

Conclusions

- The round function of AES is simple.
- The round function has a symmetric and parallel structure.
- AES has an efficient implementation in both software and hardware.
- AES is secure against all known cryptanalytic attacks.
- AES is suitable for modern processors.
- It is suitable for smart cards (8-bit processor).
- It is widely used in real-world security systems.

Online Demo of AES

- In the following URL, you find the demo of AES in different modes with/without padding:

- https://8gwifi.org/CipherFunctions.jsp