Chapter 5

Advanced Encryption Standard (AES)

Dr. Shin-Ming Cheng

NTUST
CONNECTIVITY LAB

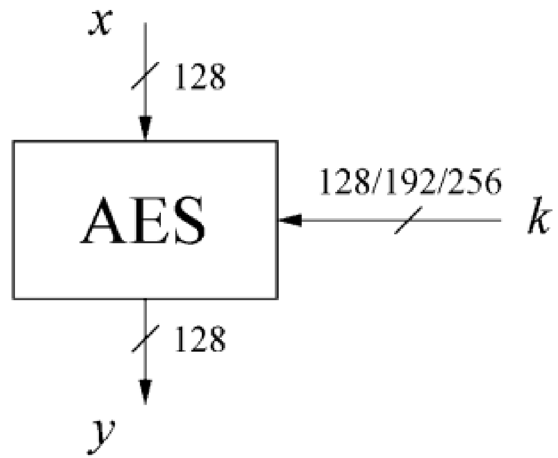
Origins

- Clear a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- Triple-DES
  - but slow, has small blocks
- US NIST issued call for ciphers in 1997
  - 15 candidates accepted in Jun 98
  - 5 were shortlisted in Aug-99
  - Rijndael was selected as the AES in Oct-2000
  - issued as FIPS PUB 197 standard in Nov-2001

The AES Cipher - Rijndael

- Designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- an **iterative** rather than **feistel** cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to be:
  - resistant against known attacks
  - speed and code compactness on many CPUs
  - design simplicity

AES: Overview

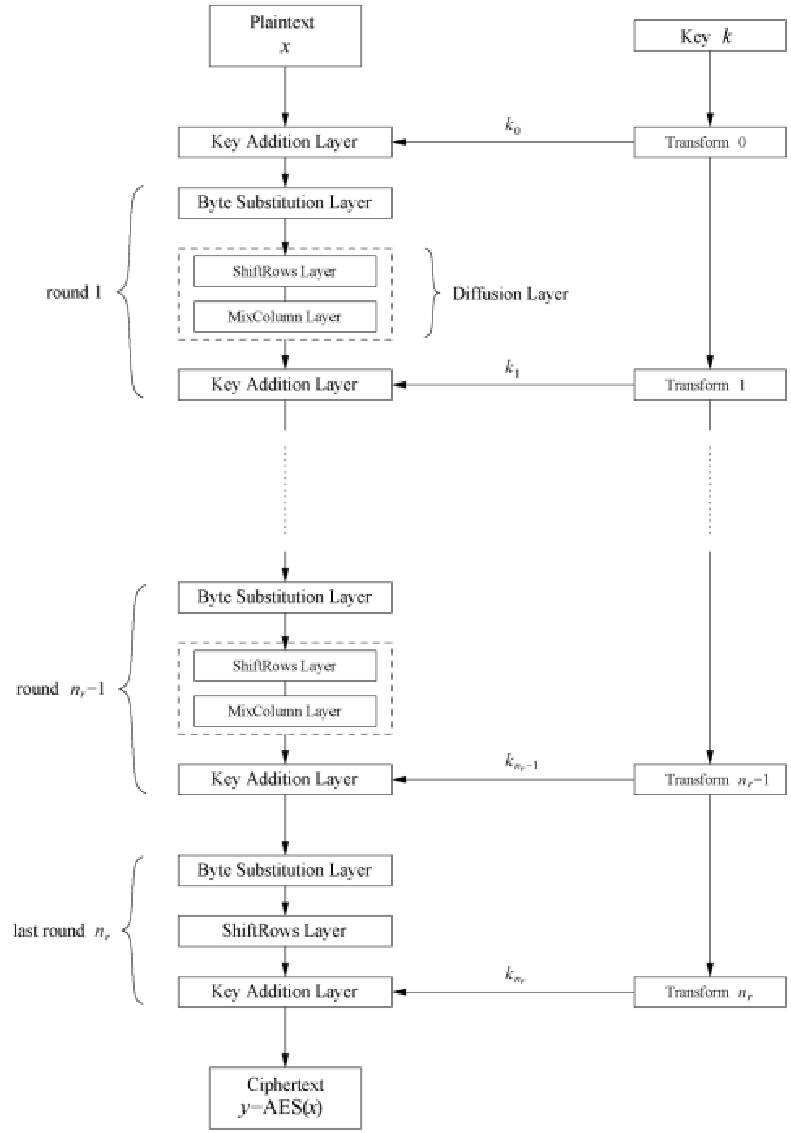


The number of rounds depends on the chosen key length:

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"



Content of this Chapter

- Overview of the AES algorithm
- **Internal structure of AES**
  - Byte Substitution layer
  - Diffusion layer
  - Key Addition layer
  - Key schedule
- Decryption
- Security

Internal Structure of AES

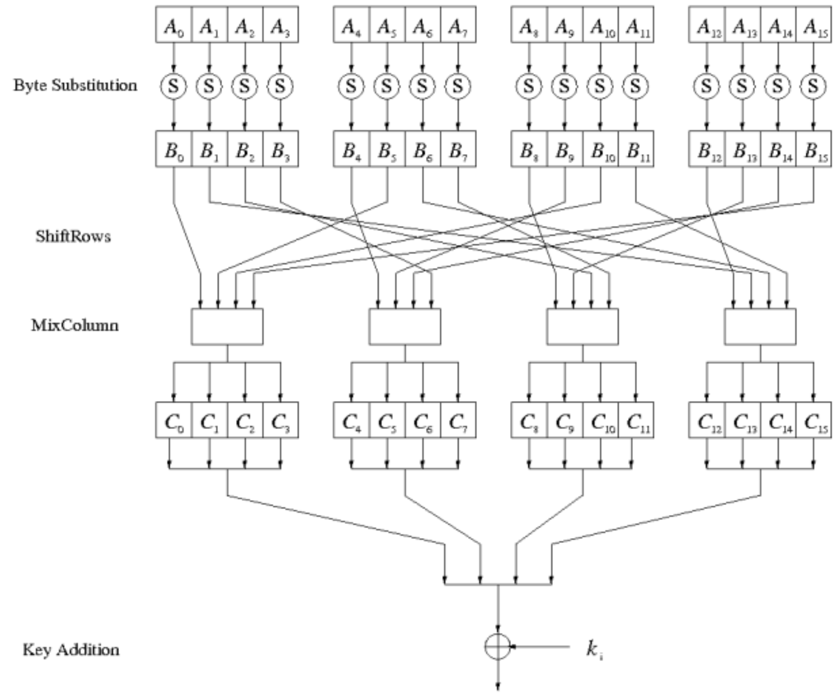
- AES is a byte-oriented cipher
- The state A (i.e., the 128-bit/16-byte data path) can be arranged in a 4×4 matrix:

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

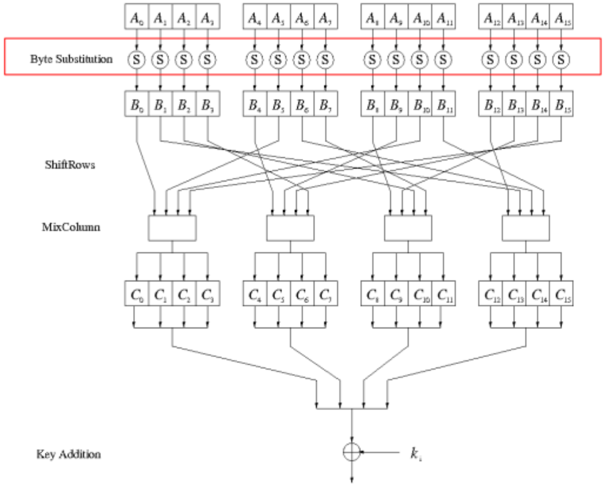
› Round function for rounds $1, 2, \ldots, nr_1$



– In the last round, the MixColumn transformation is omitted

Byte Substitution Layer

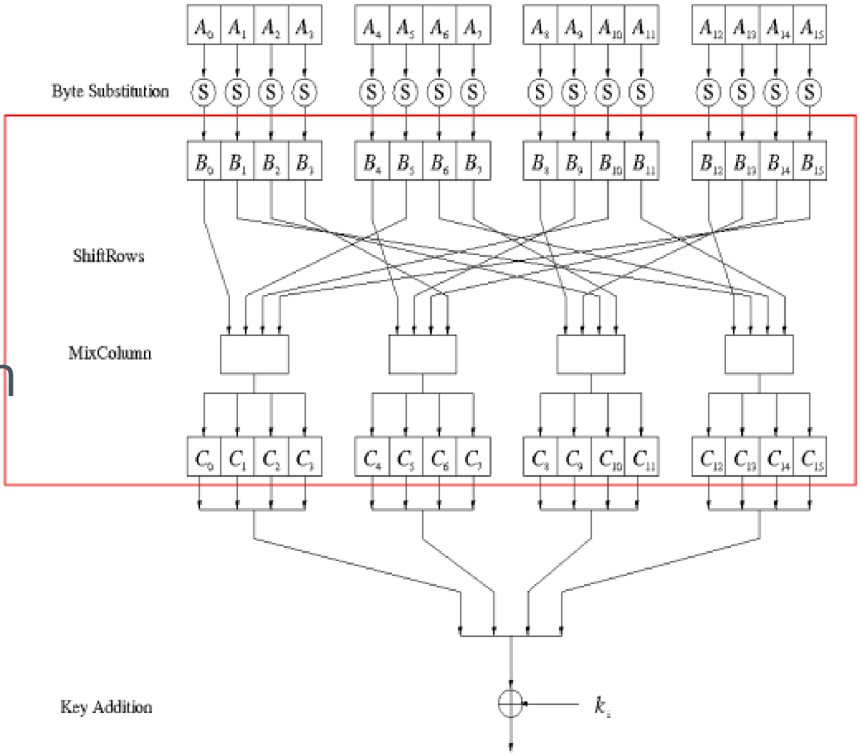
- The Byte Substitution layer consists of 16 S-Boxes with the following properties:
- The S-Boxes are
  - identical
  - the only **nonlinear** operation of AES,
  - $ByteSub(A_i) + ByteSub(A_j) \neq ByteSub(A_i + A_j)$, for $i, j = 0, \ldots, 15$



- Bijective
  - there exists a one-to-one mapping of input and output bytes
- S-Box can be uniquely reversed
  - In software implementations, the S-Box is usually realized as a lookup table

Diffusion Layer

- Provides diffusion over all input state bits
  - ShiftRows Sublayer: Permutation of the data on a byte level
  - MixColumn Sublayer: Matrix operation which combines ("mixes") blocks of four bytes
- Performs a linear operation on state matrices A, B
  - $DIFF(A) + DIFF(B) = DIFF(A + B)$

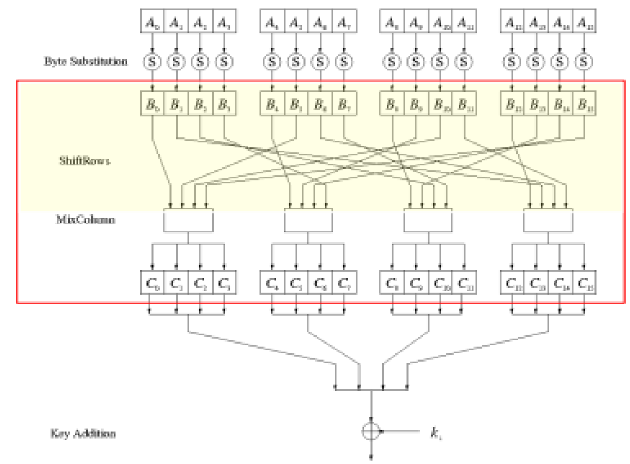


ShiftRows Sublayer

› Rows of the state matrix are shifted cyclically:

Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}



Output matrix

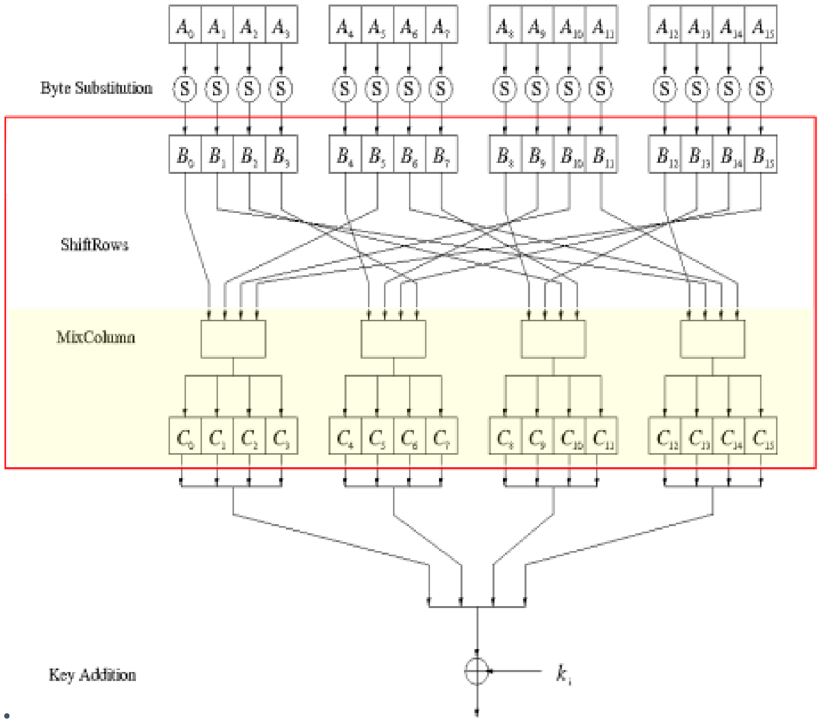
B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift

MixColumn Sublayer

- Linear transformation which mixes each column of the state matrix
- Each 4-byte column is considered as a vector and multiplied by a fixed 4×4 matrix, e.g.,

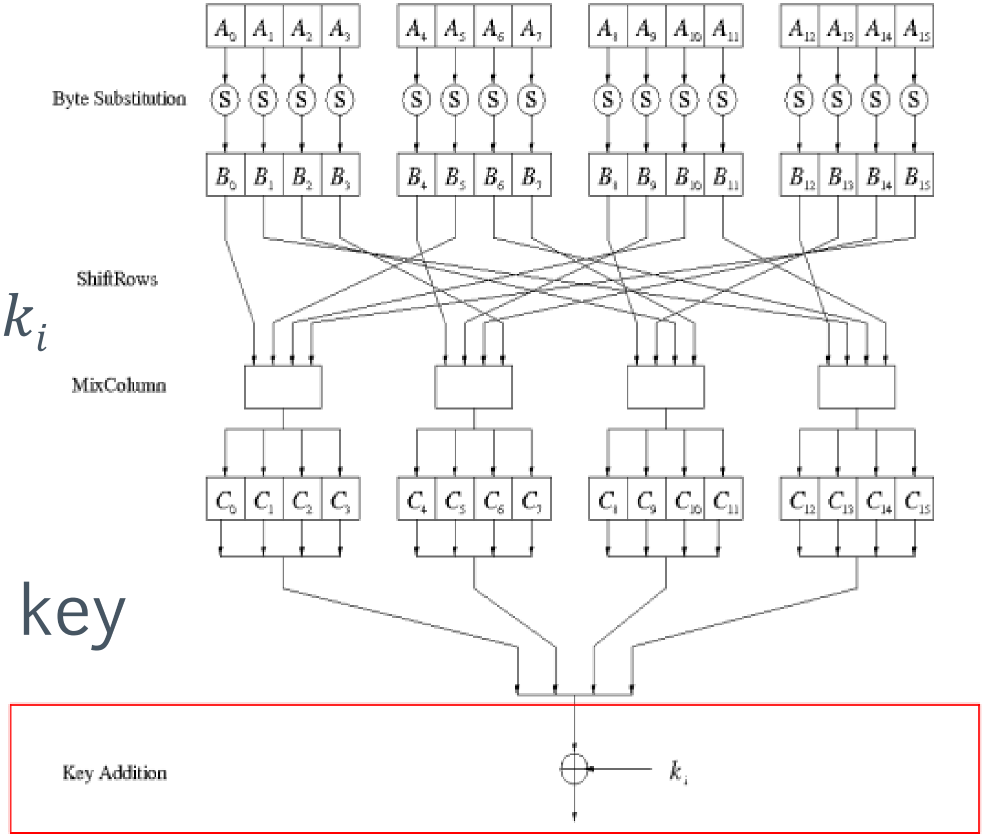
$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

where 01, 02 and 03 are given in hexadecimal notation



Key Addition Layer

- Inputs:
  - 16-byte state matrix C
  - 16-byte subkey k_i
- Output: $C \oplus k_i$
- The subkeys are generated in the key schedule



Key Schedule

› Subkeys are derived recursively from the original 128/192/256-bit input key

› Each round has 1 subkey, plus 1 subkey at the beginning of AES

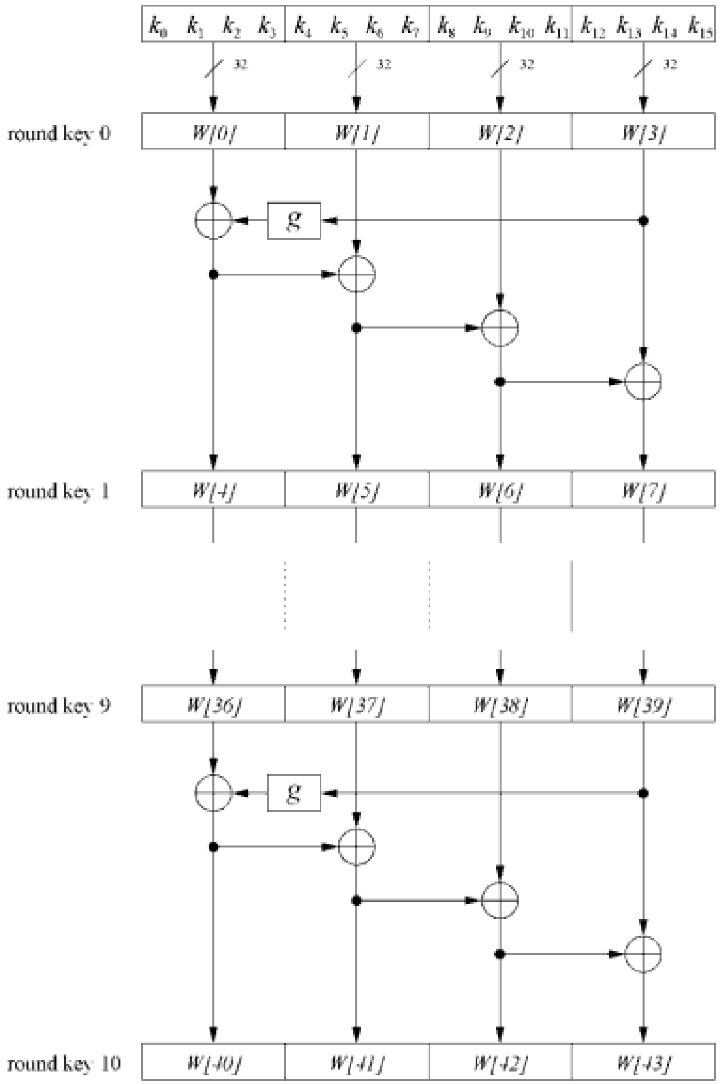
Key length (bits)	Number of subkeys
128	11
192	13
256	15

› Key whitening: Subkey is used both at the input and output of AES

$\Rightarrow \#\, subkeys = \#\, rounds + 1$

› There are different key schedules for the different key sizes

Key Schedule



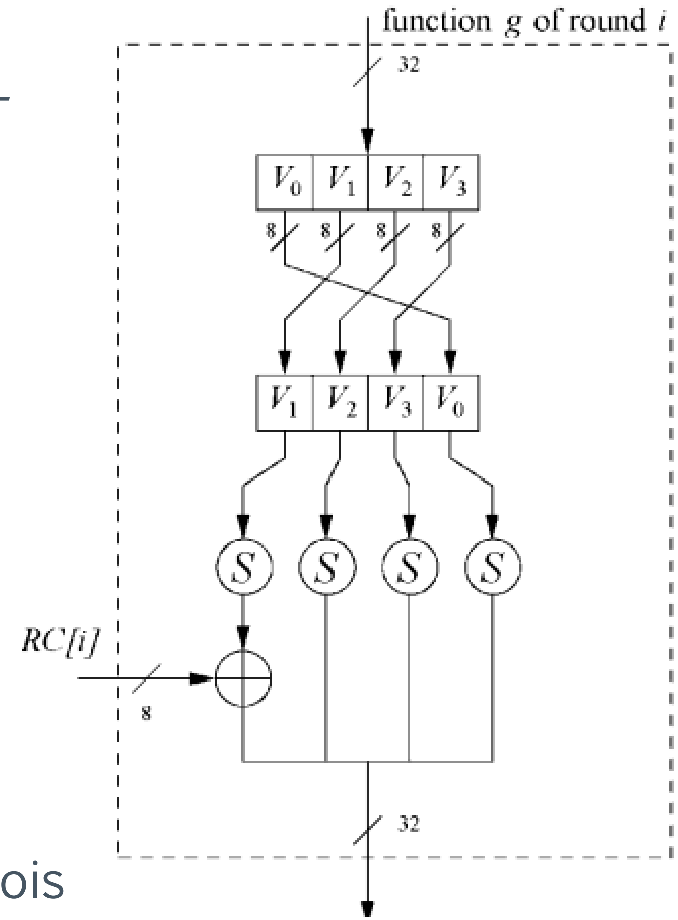
- Word-oriented:
  - $1\, word = 32\, bits$
- 11 subkeys are stored in
  - $W[0], \ldots, W[3], W[4], \ldots, W[7], \ldots, W[40], \ldots, W[43]$
- First subkey $W[0] \ldots W[3]$ is the original AES key

Key Schedule

- Function g rotates its four input bytes and performs a bytewise S-Box substitution
  - Nonlinearity
- The round coefficient RC is only added to the leftmost byte and varies from round to round:

$$RC[1] = x^0 = (00000001)_2$$
$$RC[2] = x^1 = (00000010)_2$$
$$RC[3] = x^2 = (00000100)_2$$
$$\ldots$$
$$RC[10] = x^9 = (00110110)_2$$

  - x^i represents an element in a Galois field

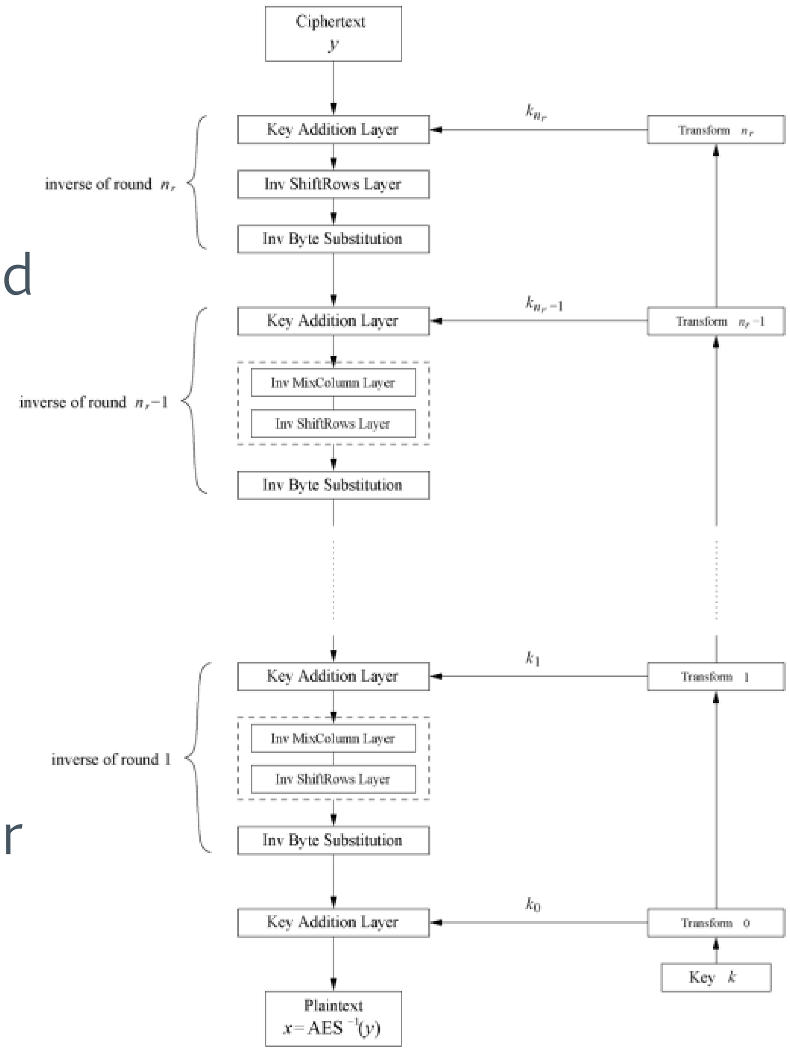


Content of this Chapter

- Overview of the AES algorithm
- Internal structure of AES
  - Byte Substitution layer
  - Diffusion layer
  - Key Addition layer
  - Key schedule
- **Decryption**
- Security

Decryption

- AES is not based on a Feistel network
  - All layers must be inverted for decryption:
- MixColumn layer
  - Inv MixColumn layer
- ShiftRows layer
  - Inv ShiftRows layer
- Byte Substitution layer
  - Inv Byte Substitution layer
- Key Addition layer is its own inverse



Decryption

- Inv MixColumn layer:
  - To reverse the MixColumn operation, each column of the state matrix C must be multiplied with the inverse of the 4×4 matrix, e.g.,

$$\begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

  - where 09, 0B, 0D and 0E are given in hexadecimal notation

- Again, all arithmetic is done in the Galois field $GF(2^8)$

Decryption

› Inv ShiftRows layer:
  - All rows of the state matrix B are shifted to the opposite direction:

Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Output matrix

B_0	B_4	B_8	B_{12}	no shift
B_{13}	B_1	B_5	B_9	→ one position right shift
B_{10}	B_{14}	B_2	B_6	→ two positions right shift
B_7	B_{11}	B_{15}	B_3	→ three positions right shift

Decryption

› Inv Byte Substitution layer:
  – Since the S-Box is bijective, it is possible to construct an inverse, such that

  $A_i = S^{-1}(B_i) = S^{-1}(S(Ai))$

  ⇒The inverse S-Box is used for decryption. It is usually realized as a lookup table

› Decryption key schedule:
  – Subkeys are needed in reversed order (compared to encryption)
  – In practice, for encryption and decryption, the same key schedule is used. This requires that all subkeys must be computed before the encryption of the first block can begin

Content of this Chapter

- Overview of the AES algorithm
- Internal structure of AES
  - Byte Substitution layer
  - Diffusion layer
  - Key Addition layer
  - Key schedule
- Decryption
- **Security**

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