Introduction to Cryptography and Information Security
UEE4611, Spring Semester

Ching-Yi Lai
Institute of Communications Engineering
National Chiao Tung University

Chapter 6: Advanced Encryption Standard

- AES Structure
- AES Transformation Functions
- AES Key Expansion
- AES Implementation

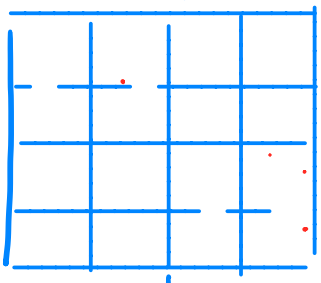
Advanced Encryption Standard. (AES).

Input: 16 bytes (128 bits).

key: M bytes.

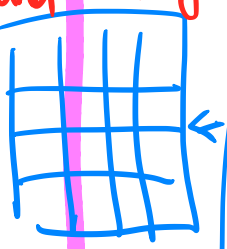
Input State (16 bytes).

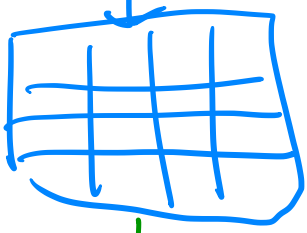
0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15



Round 0 key.

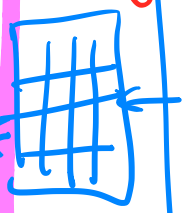
Initial transformation





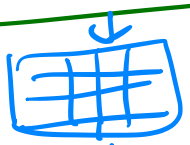
Round 1 key

Round 1 4 transformations

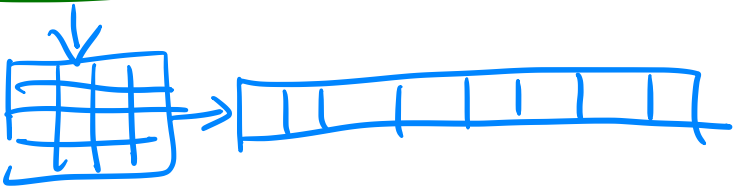


Key Expansion

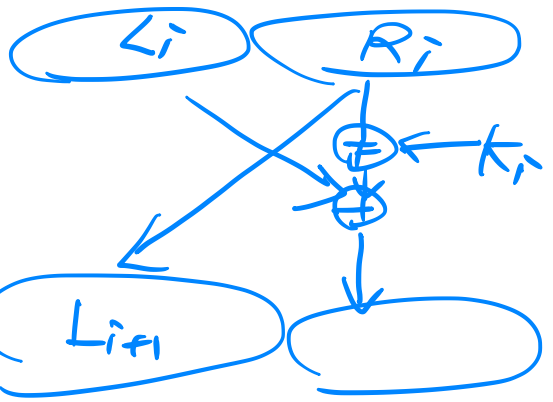
Round 9 4 tranformations



Round 10. 3 transformations



AES Structure



1. not a Feistel structure

2. The key (16 bytes) is expanded to 176 bytes. (176 = 16×11).
   11 rounds.

3. Four stages (in a round).
   - substitute bytes (S-box). 1-1 & onto.
     Inverse S-box (IS-box).
   - Shift Rows.
   - Mix columns
   - Add Round key.

4. 9 Rounds of 4 stages.
   & the last round of 3 stages.

5. Only the Add Round key stage makes use of the key.

6. The combination of the stages provide confusion, diffusion, and nonlinearity.

7. The decryption algorithm is not identical to the encryption.

1. Substitute Byte Transformation.

AES defines a 16×16 matrix of bytes values, called an S-box.

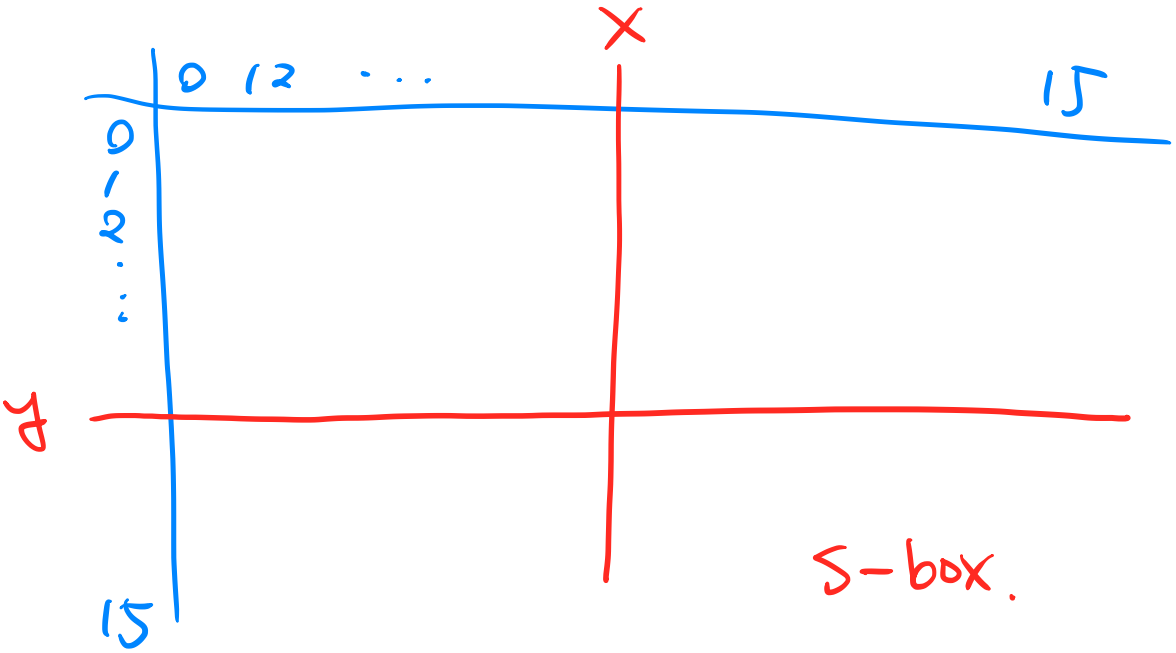
Each byte in state $[s_{ij}]_{i,j=1}^{4}$, say $s_{ij} \in \{0,1\}^8$

4×4.

and $s_{ij} = y : x$

$y, x \in \{0,1\}^4$,

is mapped to S-box$(y : x)$.



Ex. $\{9,5\} \xrightarrow{\text{S-box}} \{2A\}$

$\{2A\} \xrightarrow{\text{IS-box}} \{9,5\}$.