Announcements

- Jamboards looked pretty good
- Problem Sets are *collaborative*
  - Should make contact Thursday or Friday to schedule meetings
  - After completing a problem, think about what it tells you *before* writing up the solution to turn in
  - Opportunity to take advantage of your peers' insights
- Check solutions to Problem Sets
- Exam 1 in two weeks
  More details next week
  Start looking for "Crypto in the news" to submit as part of exam

General structure of AES

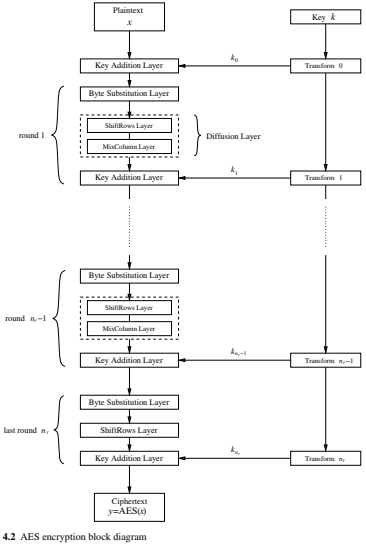


Fig. 4.2 AES encryption block diagram

Details of AES round structure

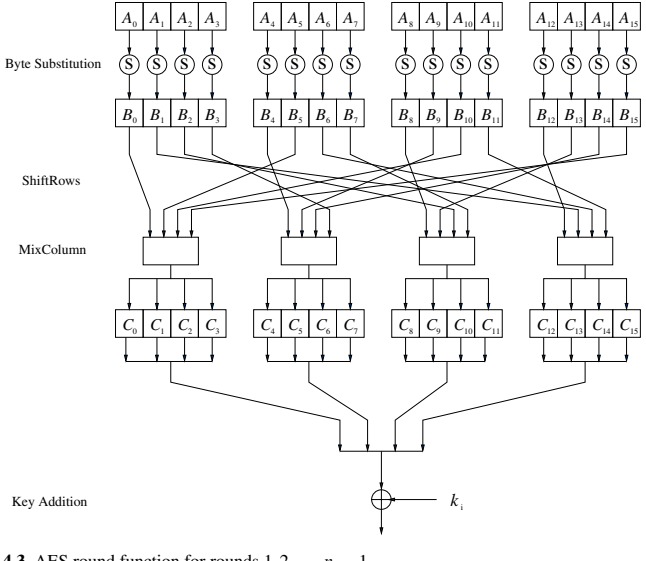
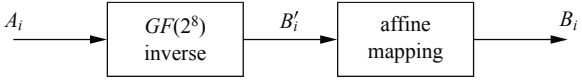


Fig. 4.3 AES round function for rounds $1, 2, \ldots, n_r - 1$

The Byte Substitution Layer / AES S-box



where the affine mapping is

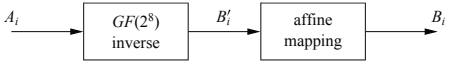
$$MB'_i + v \mod 2$$

with matrix M and vector v

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \mod 2$$

B_i M B'_i v

The Byte Substitution Layer / AES S-box



where the affine mapping is $MB'_i + v \mod 2$ with

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \mod 2$$

B_i M B'_i v

If input is $A_i = 2C$, what is the output B_i? You can use Table 4.2

The ShiftRows Layer

Place output from byte substitution in a 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}

Perform the ShiftRows

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

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

The MixColumns Layer

$$\begin{bmatrix} C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \\ C_3 & C_7 & C_{11} & C_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_5 & B_9 & B_{13} & B_1 \\ B_{10} & B_{14} & B_2 & B_6 \\ B_{15} & B_3 & B_7 & B_{11} \end{bmatrix}$$

Notice that all operations in the matrix multiplication are taking place in $GF(2^8)$

If the output from the Byte Substitution Layer is

B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}
2A	C2	1F	43	8A	03	17	02	41	32	18	CB	A4	20	9B	37

What is the output byte C_0 from the MixColumns layer?