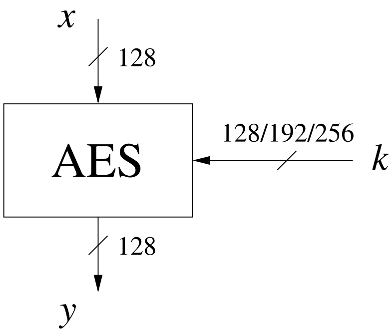
HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

The Advanced Encryption Standard (AES)



Galois field computations are needed for all operations within the AES layers.

Outline

Definition (Field)

A field F is a set of elements with the following properties:

- All elements of F form an additive group with the group operation "$+$" and the neutral element 0.
- All elements of F except 0 form a multiplicative group with the g roup operation "$\times$" and the neutral element 1.
- When the two group operations are mixed, the distributivity law holds, i.e.,

$$a \times (b + c) = (a \times b) + (a \times c), \text{ for all } a, b, c \in F.$$

Example

- The set $\mathbb{R}$ of real numbers is a field with the neutral element 0 for the additive group and the neutral element 1 for the multiplicative group.
- Every real number a has an additive inverse, namely $-a$, and every nonzero element a has a multiplicative inverse $1/a$.

Example

- The set $\mathbb{Z}_p$ with two operations $+$ and $\times$ modulo p that is a prime number is a field. This field has finite element.
- What are the additive and multiplicative inverses of element a in $\mathbb{Z}_p$?

Existence of Finite Fields

The number of elements in the field is called the **order** or **cardinality** of the field.

Theorem

*A field with order n only exists if n is a prime power, i.e., $n = p^m$, for some positive integer m and prime integer p. The number p is called the **characteristic** of the finite field.*

Example

- There is a finite field of 11 elements $GF(11)$.
- There is a finite field of 81 elements $GF(81)$.
- There is a finite field of 256 elements $GF(2^8)$ (called AES field).
- The is no finite field of 12 elements. Why?

Finite fields

$$GF(p^m)$$

$m = 1$: $GF(p)$: Prime Fields $\mathbb{Z}_p$

$m > 1$: $GF(p^m)$: Extension Fields

Extension Fields $GF(p^m)$

The elements of $GF(p^m)$ are polynomials with coefficients in $GF(p)$:

$$a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = A(x) \in GF(2^m)$$

where $a_i \in \mathbb{Z}_p$.

Example

The elements of the field $GF(2^3) = GF(8)$ are the polynomials

$$A(x) = a_2 x^2 + a_1 x + a_0$$

$GF(2^3)$ has $2^3 = 8$ elements:

$$GF(2^3) = \{ \quad 0, \quad 1, \quad x, \quad x+1 \\ x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1 \quad \}$$

Extension Fields $GF(16)$

0	x^2+1
x	x^3+x
x^2	x^2+x+1
x^3	x^3+x^2+x
$x+1$	x^3+x^2+x+1
x^2+x	x^3+x^2+1
x^3+x^2	x^3+1
x^3+x+1	1

Extension Fields $GF(27)$

0	$x+1$	x^2+2x+1
x	x^2+x	$2x^2+2x+2$
x^2	x^2+x+2	$2x^2+x+1$
$x+2$	x^2+2	x^2+1
x^2+2x	2	$2x+2$
$2x^2+x+2$	$2x$	$2x^2+2x$
x^2+x+1	$2x^2$	$2x^2+2x+1$
x^2+2x+2	$2x+1$	$2x^2+1$
$2x^2+2$	$2x^2+x$	1

Questions

What are the operations $(+, -, \times, /)$ on $GF(p^m)$?

- They are simply achieved by performing standard polynomial operations.
- The coefficients are done in the underlying field $GF(p)$.

Addition and Subtraction

Example (in $GF(2^3)$)

$$
\begin{aligned}
A(x) &= x^2 + x + 1 \\
B(x) &= x^2 + 1 \\
A(x) + B(x) &= x
\end{aligned}
$$

Multiplication

Example (in $GF(2^3)$)

$$\begin{aligned} A(x) &= x^2 + x + 1 \\ B(x) &= x^2 + 1 \\ A(x) \times B(x) &= (x^2 + x + 1)(x^2 + 1) \\ &= x^4 + x^3 + x + 1 \notin GF(2^3) \end{aligned}$$

Idea: in the prime field $GF(7) = \{0, 1, \dots, 6\}$

$$3 \cdot 4 = 12 = 5 \mod 7$$

Multiplication in Extension Fields

The product of the multiplication is divided by an irreducible polynomial, and we consider only the remainder after the polynomial division.

Definition (Multiplication in $GF(p^m)$)

Let $A(x), B(x) \in GF(p^m)$ and let

$$P(x) = \sum_{i=0}^{m} p_i x^i, \qquad p_i \in GF(p)$$

is an irreducible polynomial. Multiplication of the two elements $A(x), B(x)$ is performed as

$$C(x) = A(x) \cdot B(x) \mod P(x).$$

Example (Multiplication in $GF(2^3)$)

$$\begin{aligned}
A(x) &= x^2 + x + 1 \\
B(x) &= x^2 + 1 \\
A(x) \times B(x) &= (x^2 + x + 1)(x^2 + 1) \\
&= x^4 + x^3 + x + 1 \notin GF(2^3)
\end{aligned}$$

The irreducible polynomial of this Galois field is given as

$$P(x) = x^3 + x + 1$$

Thus

$$A(x) \cdot B(x) = x^2 + x \mod P(x).$$

Polynomial remainder

Question

How do we reduce $(x^4 + x^3 + x + 1)$ modulo $P(x) = x^3 + x + 1$?

We have

$$\begin{aligned} x^4 &= xP(x) - x^2 - x \\ &= xP(x) + x^2 + x \\ &= x^2 + x \mod P(x) \end{aligned}$$

Thus

$$\begin{aligned} x^4 + x^3 + x + 1 &= (x^2 + x) + P(x) && \mod P(x) \\ &= x^2 + x && \mod P(x) \end{aligned}$$

Finite Fields in SageMath

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

- Finite field $K = GF(2^3)$ with modulo $P(x) = x^3 + x + 1$:

```
K.<x> = GF(2^3, name='x', modulus=x^3 + x +1)
```

- Multiplication in SageMath:

```
A=K(x^2 + x + 1)
B=K(x^2 + 1)
C=A*B
print (C)
```

Irreducible polynomial

- Not all polynomials are irreducible. For example,

$$x^4 + x^3 + x + 1 = (x^2 + x + 1)(x^2 + 1)$$

  is reducible.
- AES uses the irreducible polynomial

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

Inversion in Extension Fields

- the inverse $A^{-1}(x)$ of a nonzero element $A(x) \in GF(2^m)$ is defined as

$$A(x) \cdot A^{-1}(x) = 1 \mod P(x)$$

- The main algorithm for computing multiplicative inverses is the extended Euclidean algorithm.

```
sage: A=K(x^2 + x + 1)
sage: A^-1
x^2
sage: x^2 * A
1
```

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
	1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
	2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
	3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
	4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
	5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
	6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
	7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
X	8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
	9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
	A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
	B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
	C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
	D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
	E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
	F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

For example, the inverse of

$$x^7 + x^6 + x = (11000010)_2 = (C2)_{hex} = (XY)$$

is given by the element in row C, column 2:

$$(2F)_{hex} = (00101111)_2 = x^5 + x^3 + x^2 + x + 1.$$

AES field in SageMath

```
sage: K.<x>=GF(2^8, name='x', modulus=x^8+x^4+x^3+x+1)
sage: (x^7+x^6+x)^-1
x^5 + x^3 + x^2 + x + 1
sage: (x^7+x^6+x)*(x^5+x^3+x^2+x+1)
1
```

Outline

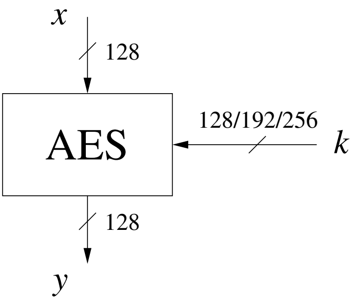
The AES process

- 1997: NIST publishes request for proposal
- 1998: 15 submissions. Five claimed attacks.
- 1999: NIST chooses 5 finalists:

  `Mars, RC6, Rijndael, Serpent, Twofish`
- 2000: NIST chooses **Rijndael** as AES (designed in Belgium)

Key sizes: $128, 192, 256$ bits. Block size: 128 bits

AES



K	# rounds $= n_r$
128	10
192	12
256	14

AES encryption block diagram

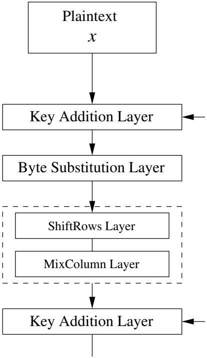


Figure: Round 1

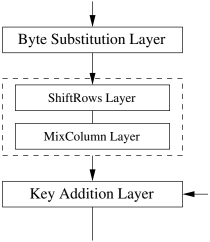


Figure: Round 2

. . .

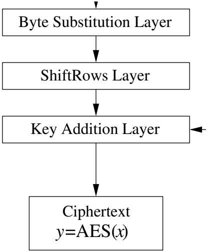
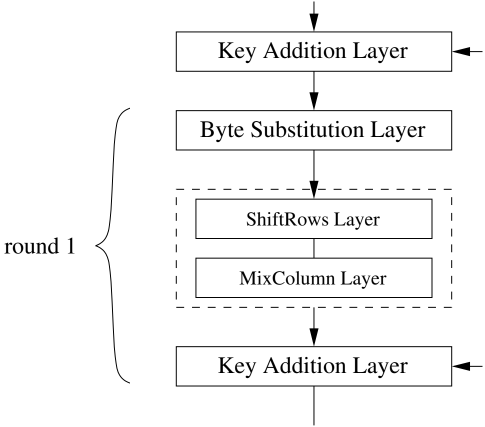
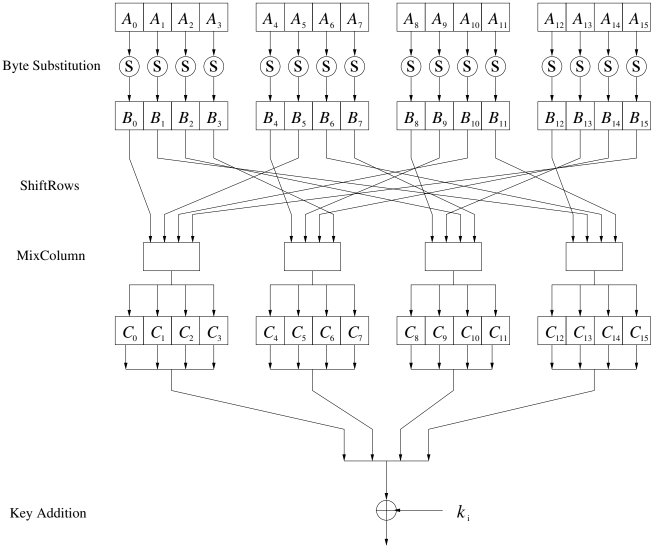


Figure: Round n_r

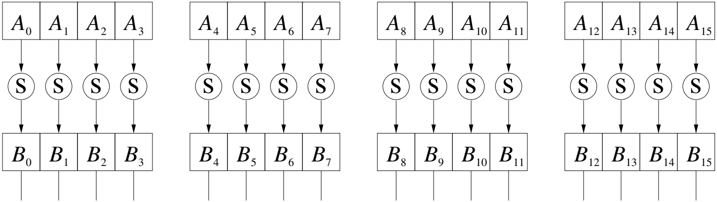
AES encryption block diagram: Round 1



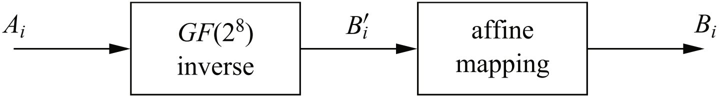
AES round function



Byte Substitution Layer



- Question: How are *S*-boxes built?
- Answer: Two-step mathematical transformation:



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

Example

- Consider

$$A_i = (11000010)2 = (C2)_{hex} \quad \in GF(2^8)$$

- We have

$$A_i^{-1} = B_i' = (2F) = (00101111)_2 \qquad \in GF(2^8)$$

- Applying the B_i' as input to the affine transformation, we get

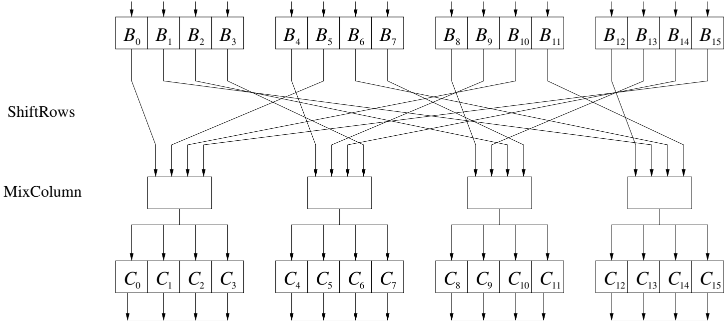
$$B_i = (0010\ 0101)_2 = (25)_{hex}$$

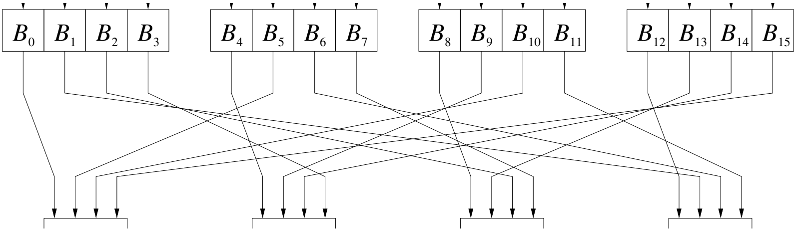
S-box: $S((C2)_{hex}) = S(C,2) = (25)_{hex}$.

										y							
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
x	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Diffusion Layer

Shift Rows and Mix Column





$$
\begin{array}{|c|c|c|c|}
\hline
B_0 & B_4 & B_8 & B_{12} \\
\hline
B_1 & B_5 & B_9 & B_{13} \\
\hline
B_2 & B_6 & B_{10} & B_{14} \\
\hline
B_3 & B_7 & B_{11} & B_{15} \\
\hline
\end{array}
\quad \to \quad
\begin{array}{|c|c|c|c|}
\hline
B_0 & B_4 & B_8 & B_{12} \\
\hline
B_5 & B_9 & B_{13} & B_1 \\
\hline
B_{10} & B_{14} & B_2 & B_6 \\
\hline
B_{15} & B_3 & B_7 & B_{11} \\
\hline
\end{array}
$$

Mix Column

- A linear transformation which mixes each column of the state matrix:

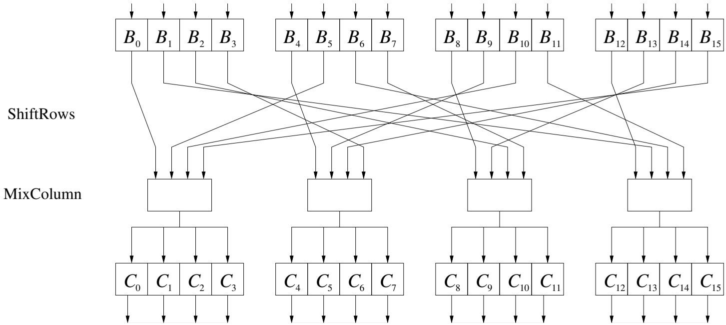
$$\text{MixColumn}(B) = C$$

- Each 4-byte column is considered as a vector and multiplied by a fixed 4×4 matrix:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

- Multiplication and addition of the coefficients is done in $GF(2^8)$.

Mix Column



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

Example

- Assume that the input state to the MixColumn layer is

$$B = (25, 25, \ldots, 25).$$

- In this special case, only two multiplications in $GF(2^8)$ have to be done. These are $02 \cdot 25$ and $03 \cdot 25$:

$$\begin{aligned}
02 \cdot 25 &= x \cdot (x^5 + x^2 + 1) \\
&= x^6 + x^3 + x, \\
03 \cdot 25 &= (x + 1) \cdot (x^5 + x^2 + 1) \\
&= (x^6 + x^3 + x) + (x^5 + x^2 + 1) \\
&= x^6 + x^5 + x^3 + x^2 + x + 1
\end{aligned}$$

Example (cont.)

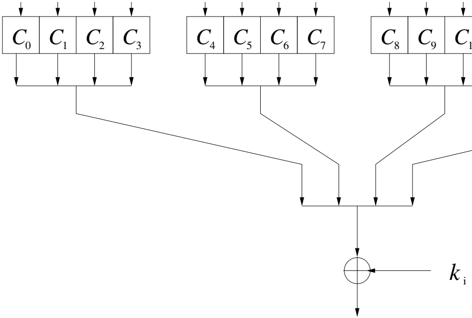
- The output bytes of C result from the following addition in $GF(2^8)$:

$$
\begin{array}{rcccc}
01 \cdot 25 = & & x^5+ & x^2+ & 1 \\
01 \cdot 25 = & & x^5+ & x^2+ & 1 \\
02 \cdot 25 = & x^6+ & x^3+ & x & \\
03 \cdot 25 = & x^6+ & x^5+x^3 & x^2+x+ & 1 \\
\hline
C_i = & & x^5+ & x^2+ & 1
\end{array}
$$

- This leads to the output state

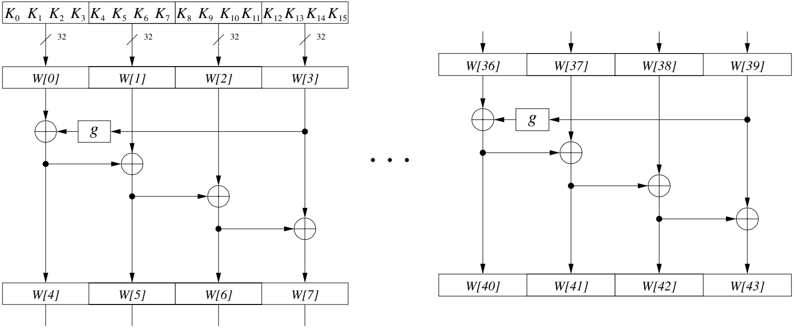
$$C = (25, 25, \ldots, 25).$$

Key Addition Layer



- Input: 16-byte matrix C and 16-byte subkey k_i
- Output: $C \oplus k_i$
- Subkeys are generated in the Key Schedule.

Key Schedule for 128-Bit Key AES

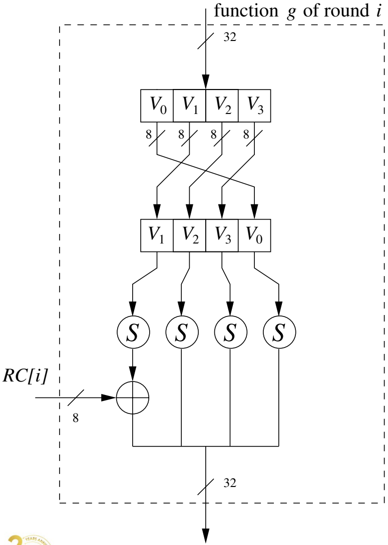


- There are 10 rounds and 11 Key Addition Layers; each Key Addition Layer requires a 128 bit subkey;
- These subkeys are split into $W[0]$, $W[1]$, $\ldots$, $W[43]$, and are computed on $GF(2^8)$ by

$$W[4i] = W[4(i-1)] + g(W[4i-1]).$$

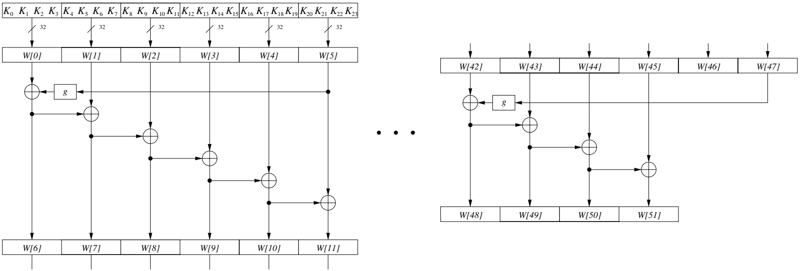
$$W[4i+j] = W[4i+j-1] + W[4(i-1)+j]$$

Function g of round i



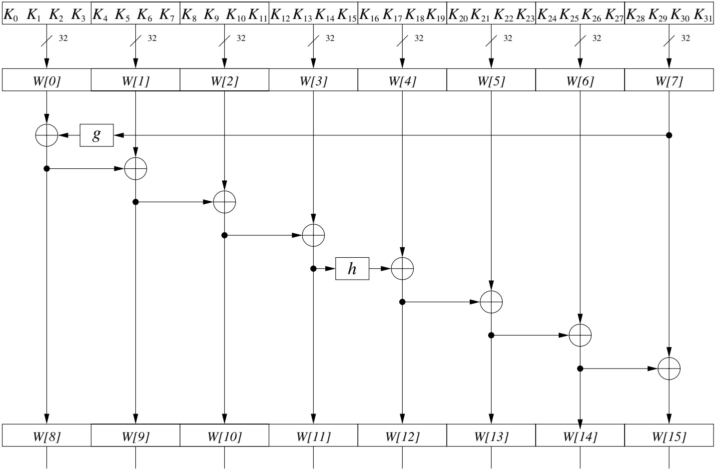
$$
\begin{aligned}
RC[1] &= x^0 = (00000001)_2, \\
RC[2] &= x^1 = (00000010)_2, \\
RC[3] &= x^2 = (00000100)_2, \\
&\vdots \\
RC[10] &= x^9 = (00110110)_2.
\end{aligned}
$$

AES-192: Key schedule

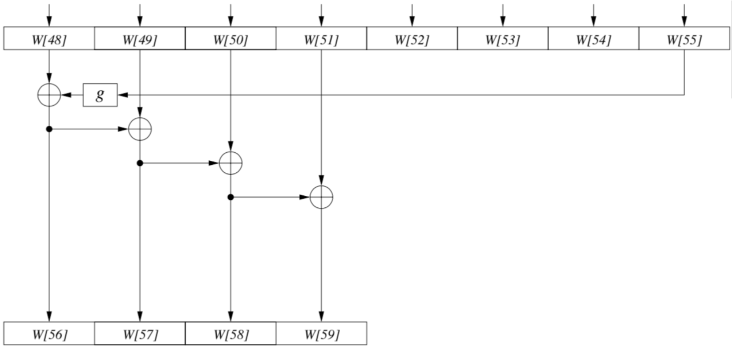


- AES-192 has 12 rounds and 13 Key Addition Layers
- Each Key Addition Layer requires a 128 bit subkey
- Thus, it needs 52 subkeys $W[0], \ldots, W[51]$.
- Each subkey is 32 bits $= 4$ bytes. $(4 \times 13 = 52)$.

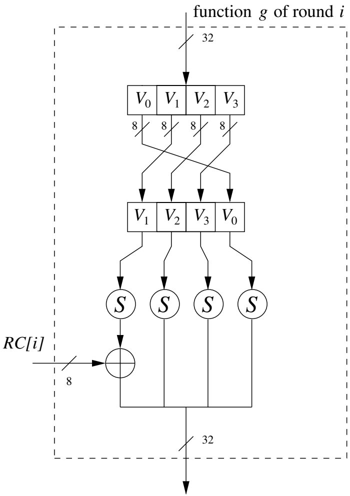
AES-256: Key schedule of Round 1

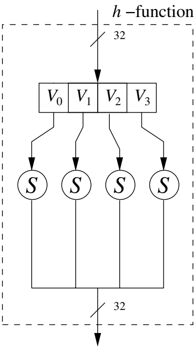


AES-256: Key schedule of final round



AES-256: g and h functions





Outline

AES decryption block diagram

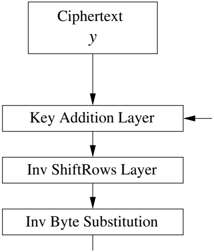


Figure: Round n

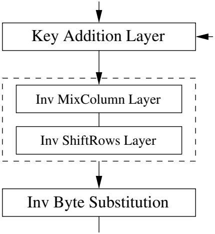


Figure: Round $n-1$

. . .

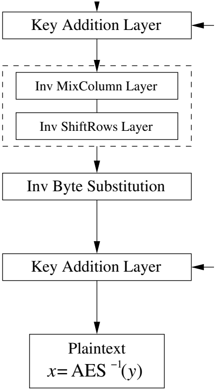


Figure: Round 1

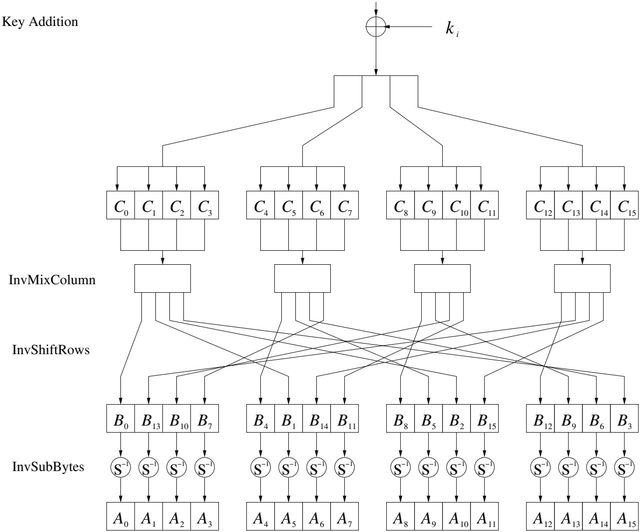


Figure: AES decryption round function $1, 2, \ldots, n_r - 1$

Inverse MixColumn Layer

- The inverse MixColumn step is applied to the state

$$\text{InvMixColumn}(C) = B$$

- Multiplication and addition of the coefficients is done in $GF(2^8)$;
- The inverse of its matrix must be used.

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix}$$

Inverse ShiftRows Sublayer

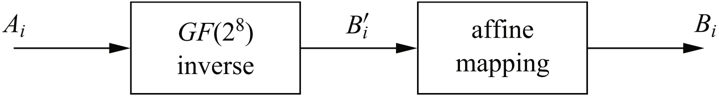
B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

$\longrightarrow$

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

Inverse Byte Substitution Layer

- We recall the SubBytes operation $S(A_i) = B_i$:



- To calculate InvSubBytes $S^{-1}(B_i) = A_i$, we do the reverse:

$$B_i \rightarrow B'_i \rightarrow A_i$$

InvSubBytes: $B_i \to B_i'$

$$\begin{pmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \mod 2,$$

InvSubByte: $B'_i \to A_i$

- We have $A_i = (B'_i)^{-1} \in GF(2^8)$
- For example, the inverse of

$$(2F)_{hex} = (00101111)_2 = x^5 + x^3 + x^2 + x + 1.$$

is

$$x^7 + x^6 + x = (11000010)_2 = (C2)_{hex}$$

Inverse AES S-Box

									y								
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
x	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Decryption Key Schedule

- Since decryption round one needs the last subkey,
- the second decryption round needs the second-to-last subkey and so on,
- In short, we need to compute the subkeys in reverse order.
- In practice this is mainly achieved by computing the entire key schedule first and storing all
  11 subkey (if for AES-128),
  13 subkey (if for AES-192), or
  15 subkey (if for AES-256).

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you!

soict.hust.edu.vn/ fb.com/groups/soict