CSE 4215

Chapter 3

Advanced Encryption Standard

Lecture 5

AES: Basics

Galois Finite Field

Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer.

A Galois field, GF(p^n), is a finite field with p^n elements.

When $n = 1$, we have GF(p) field. This field can be the set Z_p, {0, 1, …, p − 1}, with two arithmetic operations.

Example-1

A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication.

GF(2)

{0, 1} + ×

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

a	0	1
−a	1	0

a	0	1
a^{-1}	—	1

Inverses

Example-2

We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
−a	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

In cryptography, we often need to use four operations (addition, subtraction, multiplication, and division). In other words, we need to use fields. We can work in GF(2^n) and uses a set of 2^n elements. The elements in this set are n-bit words.

AES: Basics

Example-3

Let us define a $GF(2^2)$ field in which the set has four 2-bit words: {00, 01, 10, 11}. We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied.

Elements: 0, 1, x, x+1

IP: x^2+x+1

Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Polynomial

A polynomial of degree $n-1$ is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x^1 + a_0x^0$$

where x^i is called the ith term and a_i is called coefficient of the ith term.

Representation of an 8-bit word by a polynomial

n-bit word	1	0	0	1	1	0	0	1

Polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

First simplification: $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification: $x^7 + x^4 + x^3 + 1$

AES: Basics

Modulus

For the sets of polynomials in GF(2^n), a group of polynomials of degree n is defined as the modulus. Such polynomials are referred to as **irreducible polynomials.**

Degree	*Irreducible Polynomials*
1	$(x+1)$, (x)
2	(x^2+x+1)
3	(x^3+x^2+1), (x^3+x+1)
4	$(x^4+x^3+x^2+x+1)$, (x^4+x^3+1), (x^4+x+1)
5	(x^5+x^2+1), $(x^5+x^3+x^2+x+1)$, $(x^5+x^4+x^3+x+1)$, $(x^5+x^4+x^3+x^2+1)$, $(x^5+x^4+x^2+x+1)$

Example: Addition

Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in GF(2^8). We use the symbol $\oplus$ to show that we mean polynomial addition. The following shows the procedure:

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\hline
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Example: Multiplication

1. The coefficient multiplication is done in GF(2).
2. The multiplying x^i by x^j results in x^{i+j}.
3. The multiplication may create terms with degree more than $n - 1$, which means the result needs to be reduced using a modulus polynomial.

Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$. Note that we use the symbol $\otimes$ to show the multiplication of two polynomials.

Solution

$$P_1 \otimes P_2 = x^5(x^7+x^4+x^3+x^2+x) + x^2(x^7+x^4+x^3+x^2+x) + x(x^7+x^4+x^3+x^2+x)$$
$$P_1 \otimes P_2 = x^{12}+x^9+x^8+x^7+x^6+x^9+x^6+x^5+x^4+x^3+x^8+x^5+x^4+x^3+x^2$$
$$P_1 \otimes P_2 = (x^{12}+x^7+x^2) \bmod (x^8+x^4+x^3+x+1) = x^5+x^3+x^2+x+1$$

To find the final result, divide the polynomial of degree 12 by the polynomial of degree 8 (the modulus) and keep only the remainder.

AES: Introduction

- The **Advanced Encryption Standard** (AES), was established by the U.S. National Institute of Standards and Technology (NIST) in 2001
- AES has been adopted by the U.S. government and is now used worldwide.
- It supersedes the Data Encryption Standard (DES), which was published in 1977.
- The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.
- AES is a block Cipher

Encryption and Data Protection overview

The secure boot chain, system security and app security capabilities all help to ensure that only trusted code and apps run on a device. Apple devices have additional encryption features to safeguard user data even when other parts of the security infrastructure have been compromised (for example, if a device is lost or is running untrusted code). All these features benefit both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

iOS and iPadOS devices use a file encryption methodology called Data Protection, while the data on Mac computers is protected with a volume encryption technology called FileVault. Both models similarly root their key management hierarchies in the dedicated silicon of the Secure Enclave (on devices that include an SEP) and both models leverage a dedicated AES engine to support line-speed encryption and to ensure that long-lived encryption keys never need to be provided to the kernel OS or CPU (where they might be compromised).

IMPORTANT: SecureAccess has been replaced with PrivateAccess. All current SecureAccess users are advised to back up their SecureAccess vault data and upgrade to PrivateAccess.

SecureAccess to PrivateAccess Migration

Back up or Restore Data in SanDisk SecureAccess

SanDisk® SecureAccess™

SanDisk SecureAccess is a fast, simple way to store and protect critical and sensitive files on SanDisk USB flash drives.

Access to your private vault is protected by a personal password, and your files are automatically encrypted - so even if you share your SanDisk® USB flash drive or it becomes lost or stolen, access to your files are safe.

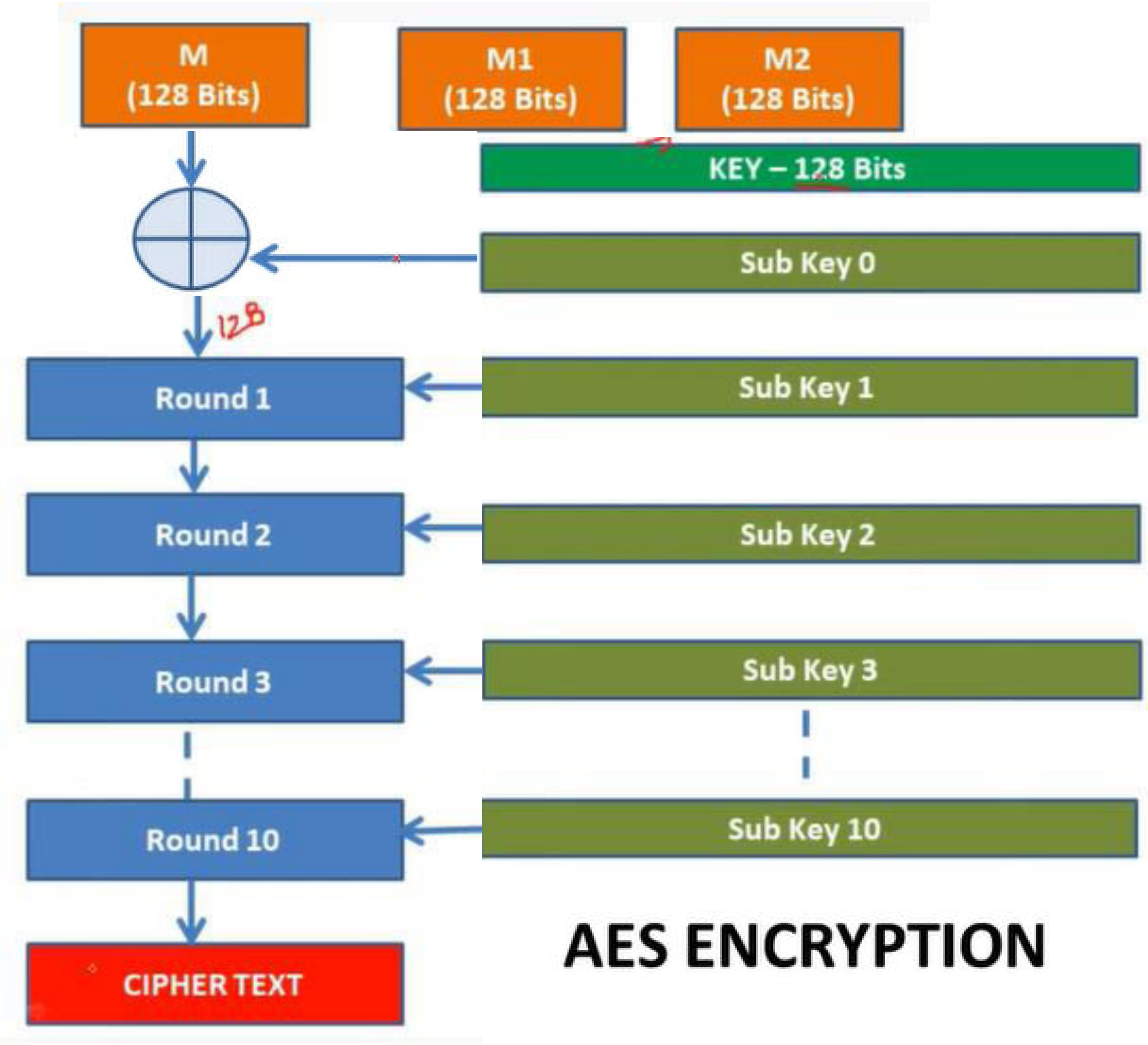
NOTE: SecureAccess is not required to use your flash drive as a storage device on Mac or PC. SecureAccess is a complimentary data encryption and password protection application.

SecureAccess v3.02 features
- Quicker start-up
- Improved password settings
- Faster Encryption with multi-thread processing
- Encrypted Backup and Restore data stored in vault

Critical:
- The "forgot password" option does not allow you to reset your password. Please keep your SecureAccess vault password secure to ensure access to your vault.
- If the password cannot be remembered, with or without the password hint available, the files on the drive are not accessible and cannot be retrieved.
- SecureAccess utilizes 128-bit AES encryption.
- Ejecting a drive abruptly might result in **data corruption** and vault might not behave as expected.

AES: Introduction

- AES encrypts messages in blocks of 128 bits.
- AES allows three different key lengths 128, 192 and 256 bits.
- The number of rounds in Encryption and Decryption is dependent on the key length.
    - 128 bit – 10 rounds
    - 192 bit – 12 rounds
    - 256 bit – 14 rounds



AES: Key Expansion

Key in Text – satishcjisboring

Key (128 bits) –

01110011011000010111010001101001011100110
11010000110001101101010011010010111001101
10001001101111011100100110100101101110011
00111

Key in Hex

73 61 74 69 73 68 63 6a 69 73 62 6f 72 69 6e 67

s a t i s h c j i s b o r i n g

Key in Hex

73	61	74	69	73	68	63	6a	69	73	62	6f	72	69	6e	67
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}	b_{16}

$$\begin{bmatrix} b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \\ b_4 & b_8 & b_{12} & b_{16} \end{bmatrix} \Rightarrow \begin{bmatrix} 73 & 73 & 69 & 72 \\ 61 & 68 & 73 & 69 \\ 74 & 63 & 62 & 6e \\ 69 & 6a & 6f & 67 \end{bmatrix}$$

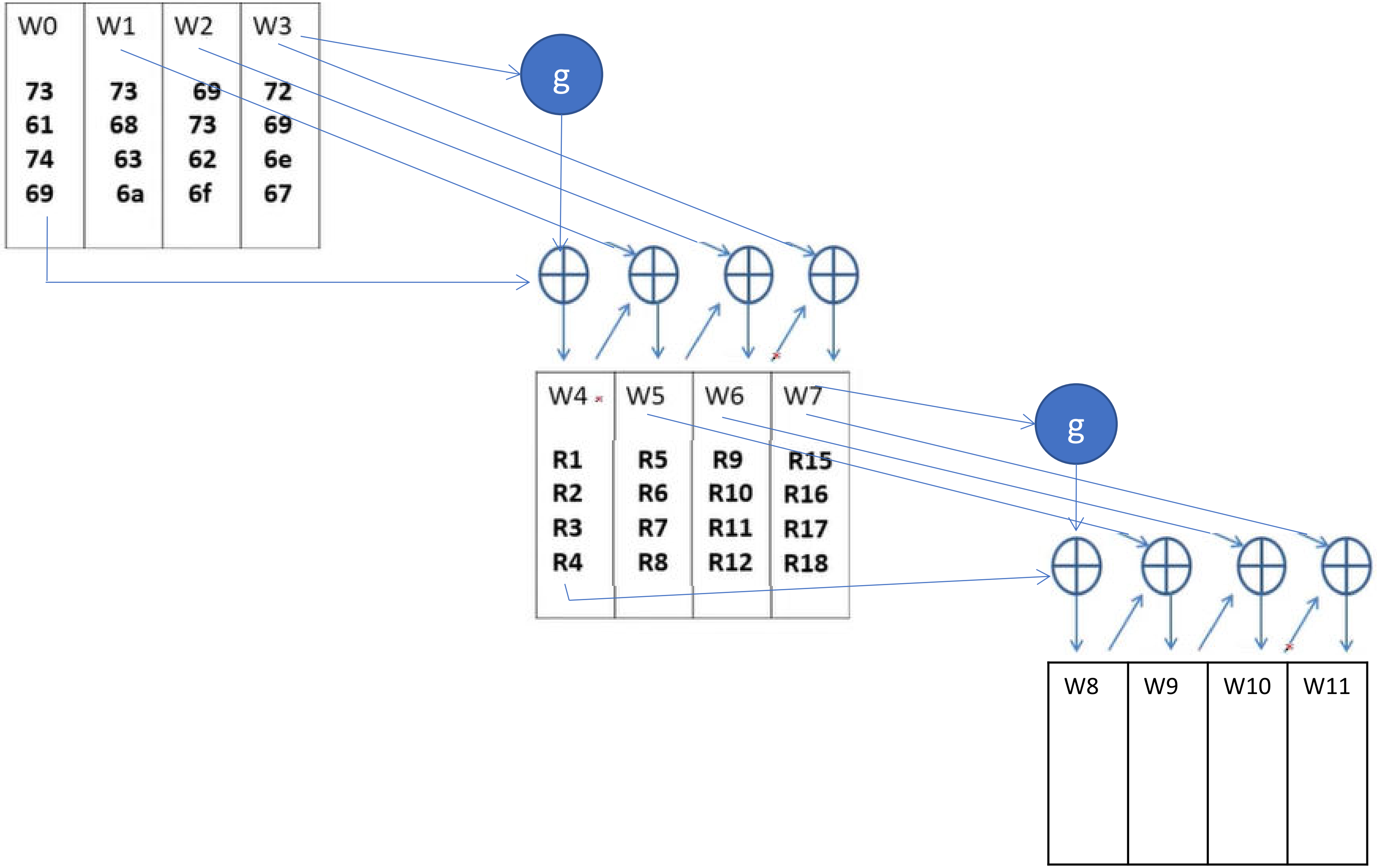
Word 0 (w0): $b_1b_2b_3b_4 \rightarrow$ 32 bits
Word 1 (w1): $b_5b_6b_7b_8 \rightarrow$ 32 bits
Word 2 (w2): $b_9b_{10}b_{11}b_{12} \rightarrow$ 32 bits
Word 3 (w3): $b_{13}b_{14}b_{15}b_{16} \rightarrow$ 32 bits

W0	W1	W2	W3	W4	W5	W6	W7	......	....	W43
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} b_{16}							

We need fill up w4 to w43

AES ENCRYPTION

AES: Key Expansion



……. and so on

AES: Key Expansion

Find the function g

$W4 = W0 \oplus g(W3)$

W3	RotWord	SubWord	
72	69	F9	
69	6E	9F	
6E	67	85	
67	72	40	

- RotWord performs a one-byte circular left shift on a word
- This means that an input [B0, B1, B2, B3] transformed into [B1, B2, B3, B0]

- SubWord performs a bye substitution on each byte of its input word using the S-box table. ForRotword 69, select row 6 and col 9 which is F9

AES S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES: Key Expansion

Find the function g

W4= W0 ⊕ g(W3)

W3	RotWord (X1)	SubWord (Y1)	
72	69	F9	
69	6E	9F	
6E	67	85	
67	72	40	

- The Y1 is XORed with round constant Rcon[j]

R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Y1 11111001100111111000010101000000
R1 00000001000000000000000000000000
g(w3) 11111000100111111000010101000000
g(w3) - F8 9F 85 40

W0 - 01110011011000010111010001101001
G(w3) - 11111000100111111000010101000000
Result - 10001011111111101111000100101001
Result - 8b fe f1 29

W4=W0 ⊕ G(W3)=8b fe f1 29

W4	W5	W6	W7
8b fe f1 29	R5 R6 R7 R8	R9 R10 R11 R12	R15 R16 R17 R18

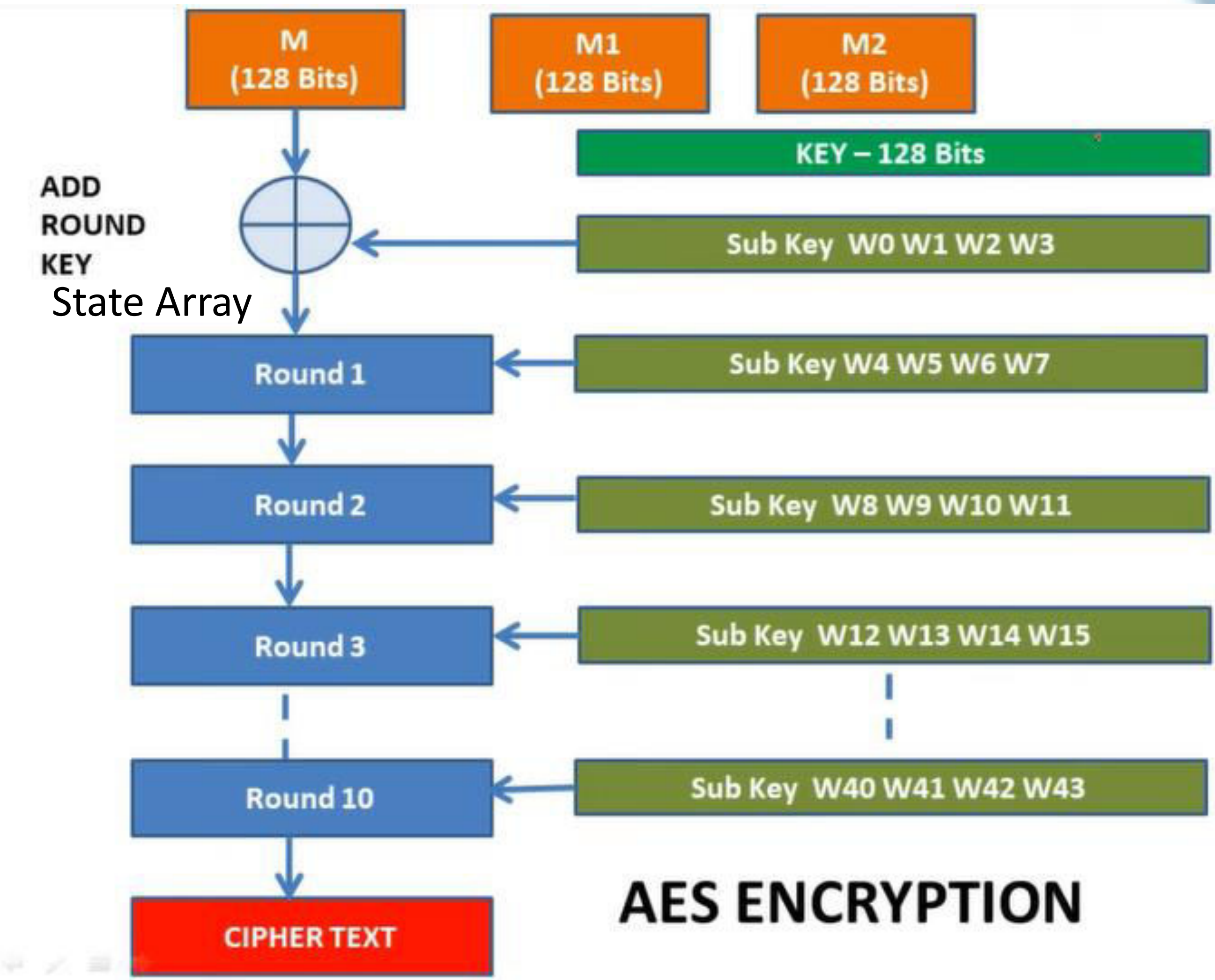
AES: Key Expansion

Sub key 1

W4	W5	W6	W7
8b	f8	91	e3
Fe	96	e5	8c
F1	92	f0	9e
29	43	2c	4b

$W5 = W4 \oplus W1$
$W6 = W5 \oplus W2$
$W7 = W6 \oplus W3$

[W5,W6,W7,W8] is the input of round 2 for Sub key 2 and so on



AES: Message Block

M
(128 Bits)

secretmessagenow

73 65 63 72 65 74 6d 65 73 73 61 67 65 6e 6f 77

Use 4x4 matrix to represent the message

$$\begin{bmatrix} 73 & 65 & 73 & 65 \\ 65 & 74 & 73 & 6e \\ 63 & 6d & 61 & 6f \\ 72 & 65 & 67 & 77 \end{bmatrix}$$

XOR message with key

$$\begin{bmatrix} 73 & 65 & 73 & 65 \\ 65 & 74 & 73 & 6e \\ 63 & 6d & 61 & 6f \\ 72 & 65 & 67 & 77 \end{bmatrix} \oplus \begin{bmatrix} 73 & 73 & 69 & 72 \\ 61 & 68 & 73 & 69 \\ 74 & 63 & 62 & 6e \\ 69 & 6a & 6f & 67 \end{bmatrix}$$

73 → 01110011
73 → 01110011
Result 00000000

Resultant Matrix

$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix}$$

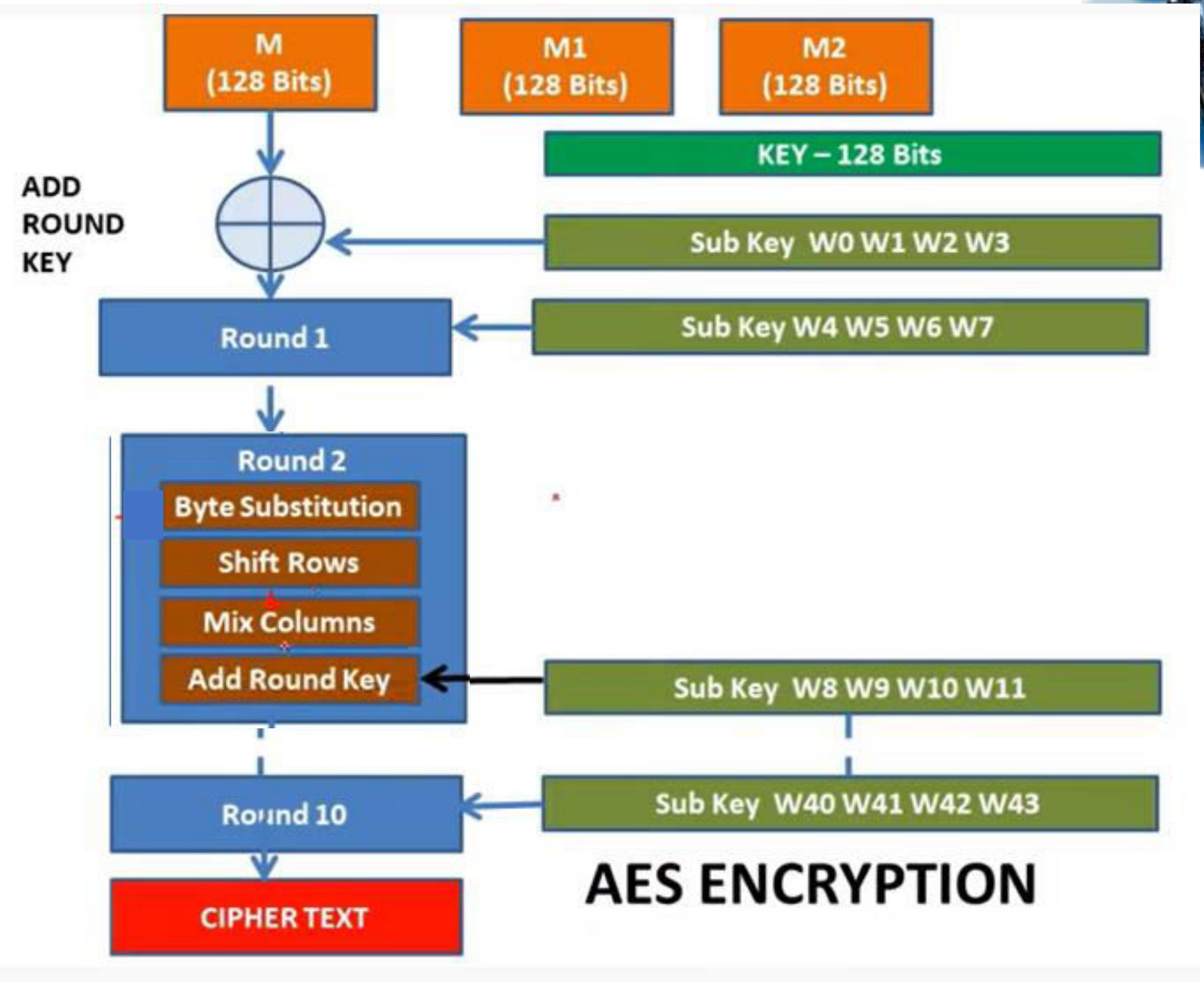
Resultant Matrix is called **state array**

AES: Round Function

Consists of Four Steps

1. Substitute Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key

Round 10 only skip Mix Columns



AES: Round Function (Byte Substitution)

- Does a simple replacement of each byte of the block data using an S-box
- Left four bits determine row, right four bits determine the column

$$\begin{bmatrix} 00 & 16 & 1a & 17 \\ 04 & 1c & 00 & 07 \\ 17 & 0e & 03 & 01 \\ 1b & 0f & 0f & 10 \end{bmatrix} \Rightarrow \begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

AES S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES: Round Function (Shift Rows)

Shift Rows simply byte shifts the rows

- First row: no change
- Second row: one byte cyclical left shift
- Third row: two byte cyclical left shift
- Fourth row: three byte cyclical left shift

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & c5 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ \boxed{9c \quad 63 \quad c5 \quad f2} \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix}$$

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ \boxed{7b \quad 7c \quad f0 \quad ab} \\ af & 76 & 76 & ca \end{bmatrix}$$

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ \boxed{ca \quad af \quad 76 \quad 76} \end{bmatrix}$$

Final Matrix

AES: Round Function (Mix Columns)

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

Multiply the matrix with standard matrix

$$\begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix}$$

r_1=(02x63)+(03x9c)+(01x7b)+(01xca)

Using Finite Field Arithmetic, $G_F(2^8)$

02=0000 0010=X^7x0+X^6x0+X^5x0+X^4x0+X^3x0+X^2x0+X^1x1+X^0x0
=X

63=0110 0011=X^7x0+X^6x1+X^5x1+X^4x0+X^3x0+X^2x0+X^1x1+X^0x1
=X^6+X^5+X^1+1

Now

02x63=X*(X^6+X^5+X^1+1)
=X^7+X^6+X^2+X
=1100 0110
=C6

AES: Round Function (Mix Columns)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

r_1=(02x63)+(03x9c)+(01x7b)+(01xca)

(02x63)=(0000 0010)(0110 0011)=$X*(X^6+X^5+X^1+1)$

(03x9c)=(0000 0011)(1001 1100)=$(X+1)*(X^7+X^4+X^3+X^2)$

(01x7b)=(0000 0001)(0111 1011)=$1*(X^6+X^5+X^4+X^3+X+1)$

(01xca)=(0000 0001)(1100 1010)=$1*(X^7+X^6+X^3+X)$

(02x63)+(03x9c)+(01x7b)+(01xca)= $(X^7+X^6+X^2+X)+$

$(X^8+X^5+X^4+X^3 +X^7+X^4+X^3+X^2)+$

$(X^6+X^5+X^4+X^3+X+1)+$

$(X^7+X^6+X^3+X)$

$= X^8+X^7+X^6+X^4+X+1$

=111010011

Same term cancel out

To avoid X^8, divide 111010011 by irreducible polynomial

$P(x)= X^8+X^4+X^3+X+1$=100011011, we get

r1=1100 1000=c8

AES: Round Function (Mix Columns)

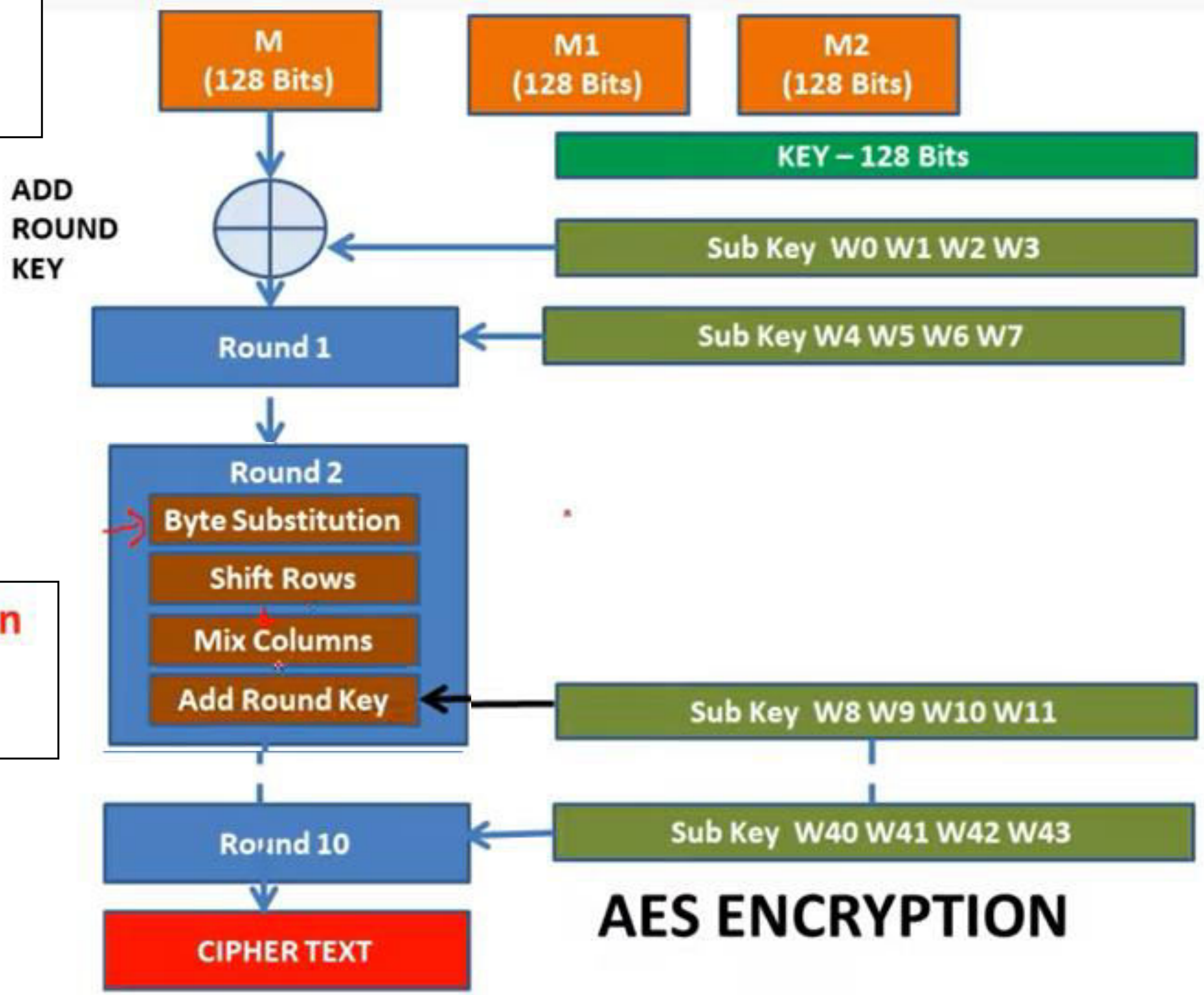
- XOR the state array with 128 bits of round key
- For round 1 it is w4,w5,w6,w7 (sub key) is used

$$\begin{bmatrix} r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \\ r_4 & r_8 & r_{12} & r_{16} \end{bmatrix}$$

The last round for encryption does not involve the "Mix columns" step.

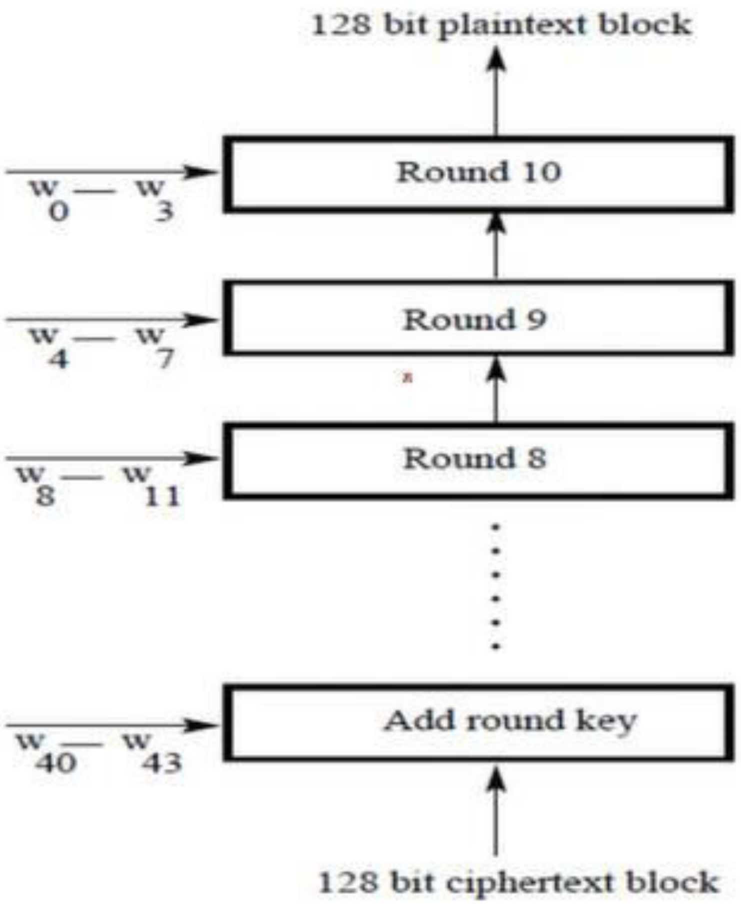
Final ciphertext

6441FAFDDCF9427BA266E9AFED3137CE6AF02B585
A195BF35ED2EF9DCF421946



AES: Decryption

Decryption



Round has the following steps

- Substitution Bytes
- Shift Rows
- Mixing Columns (Not applicable for Round 10)
- Add round key

- Substitution Bytes - An inverse S box is used for byte substitution
- Shift Rows – Rows are shifted right in decryption

  1st row – unchanged ,

  2nd row shifted right by 1

  3rd row shifted right by 2

  4th row shifted right by 3