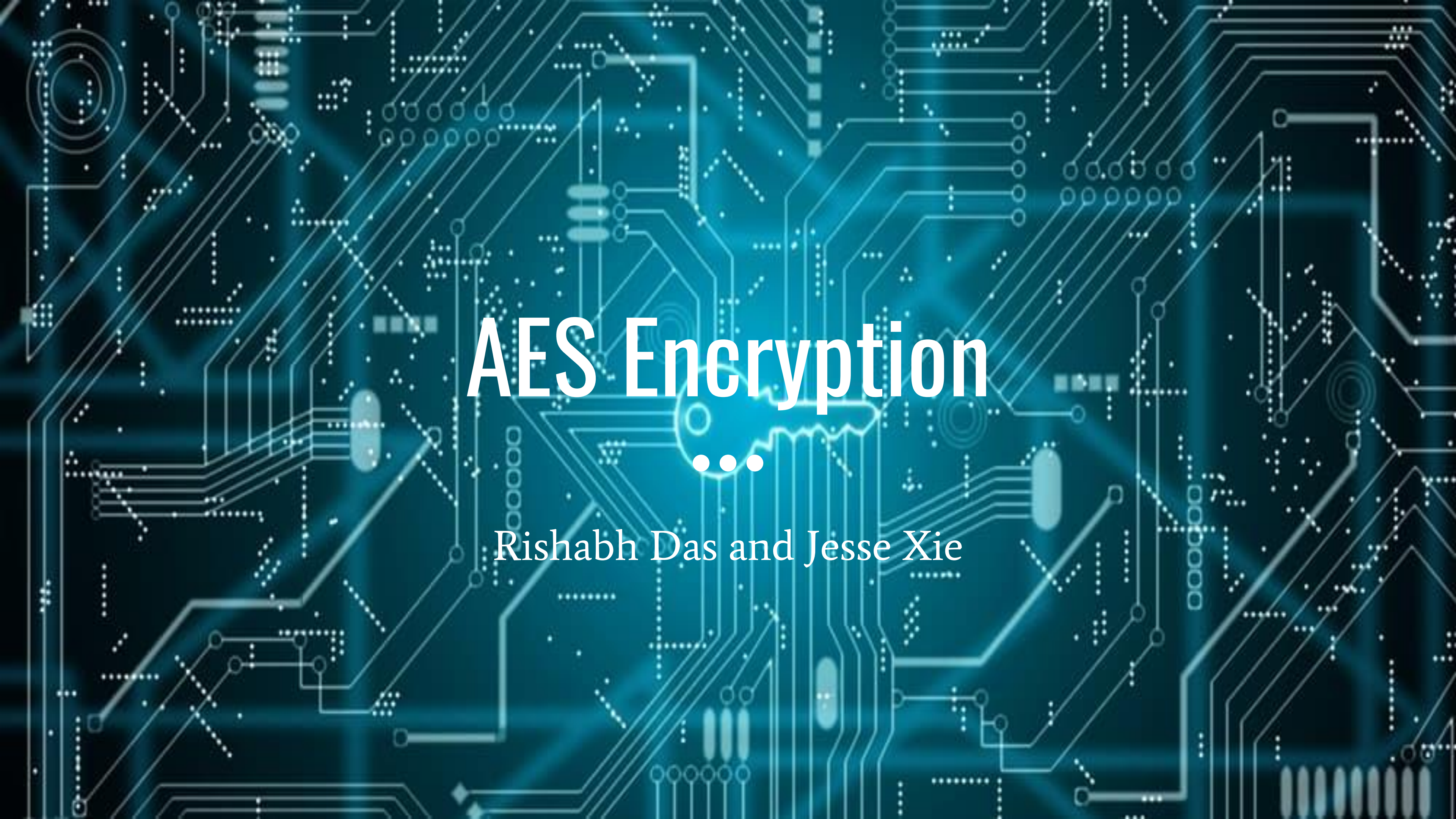


AES Encryption

Rishabh Das and Jesse Xie

What is AES Encryption?

- Also known as Rijndael
- Cipher that was developed in 1998 by Vincent Rijmen and Joan Daemen
- Was adopted by U.S. Federal Government in 2002, succeeded DES
- Most popular symmetric encryption algorithm
- 128, 192, 256 bit variants
- Impossible to decipher without key (even 128 bits)
- With quantum computer: six months Without: billions/trillions of years

Our Example

We will be working with the key “An EncryptionKey” and secret message “A Secret Message”. In hex, these are

Input

```
A Secret Message → 41 20 53 65 63 72 65 74 20 4d 65 73 73 61 67 65
```

Key

```
An EncryptionKey → 41 6e 20 45 6e 63 72 79 70 74 69 6f 6e 4b 65 79
```

Blocks of 16

The first step is to break of the input text into blocks of 16, and arrange each block into a 4 by 4 grid.

$$a_0 \quad a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7 \quad a_8 \quad a_9 \quad a_{10} \quad a_{11} \quad a_{12} \quad a_{13} \quad a_{14} \quad a_{15}$$

$$\Big\downarrow$$

$$\begin{bmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{bmatrix}$$

Blocks of 16

A Secret Message →

41	63	20	73
20	72	4d	61
53	65	65	67
65	74	73	65

An EncryptionKey →

41	6e	70	6e
6e	63	74	4b
20	72	69	65
45	79	6f	79

Initial XOR

To start our encryption process, we have to XOR our inputted block with our key block.

$$\begin{matrix} \texttt{41} & \texttt{63} & \texttt{20} & \texttt{73} \\ \texttt{20} & \texttt{72} & \texttt{4d} & \texttt{61} \\ \texttt{53} & \texttt{65} & \texttt{65} & \texttt{67} \\ \texttt{65} & \texttt{74} & \texttt{73} & \texttt{65} \end{matrix} \quad \text{XOR} \quad \begin{matrix} \texttt{41} & \texttt{6e} & \texttt{70} & \texttt{6e} \\ \texttt{6e} & \texttt{63} & \texttt{74} & \texttt{4b} \\ \texttt{20} & \texttt{72} & \texttt{69} & \texttt{65} \\ \texttt{45} & \texttt{79} & \texttt{6f} & \texttt{79} \end{matrix} \quad \longrightarrow \quad \begin{matrix} \texttt{00} & \texttt{0d} & \texttt{50} & \texttt{1d} \\ \texttt{4e} & \texttt{11} & \texttt{39} & \texttt{2a} \\ \texttt{73} & \texttt{17} & \texttt{0c} & \texttt{02} \\ \texttt{20} & \texttt{0d} & \texttt{1c} & \texttt{1c} \end{matrix}$$

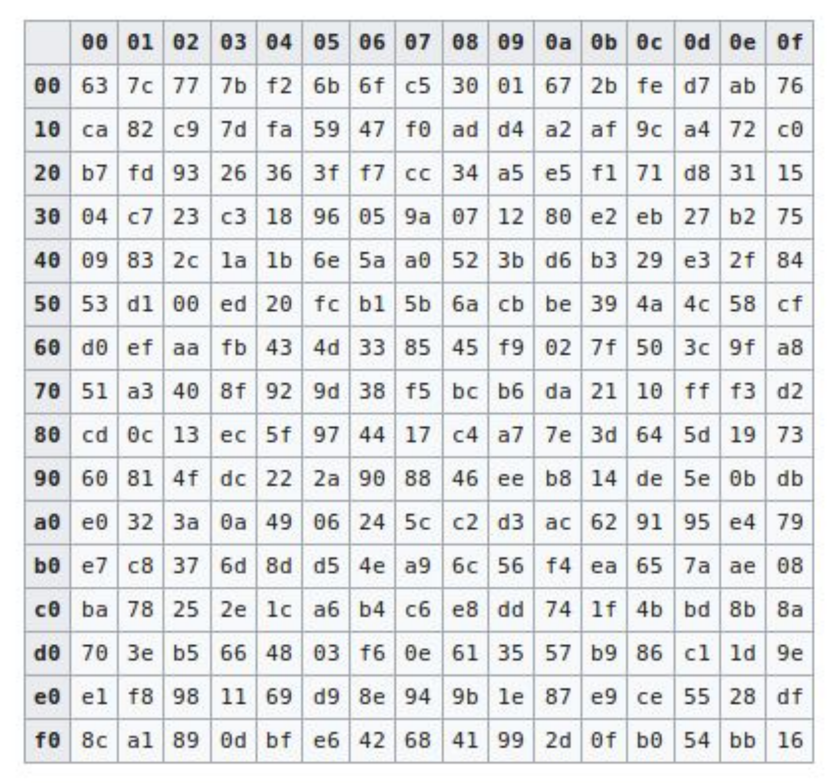
The Four Main Steps

There are four main components to AES Encryption:

- Substitute Bytes
- Shift Rows
- Mix Columns
- Round Key

Substitute Bytes

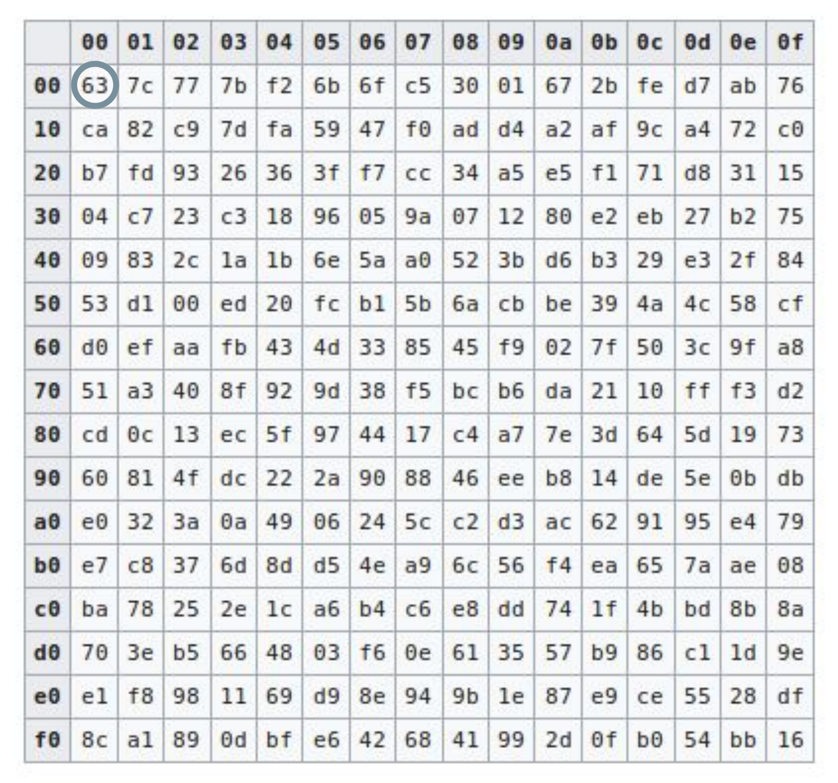
Each byte is then substituted with another byte. There is a way to calculate exactly what it is substituted with, but the only important thing is that it’s just a lookup table, so it’s very fast.



	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

Substitute Bytes

00	4e	73	20
0d	11	17	0d
50	39	0c	1c
1d	2a	02	1c



	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

Substitute Bytes

```
00  0d  50  1d          63  d7  53  a4

4e  11  39  2a          2f  82  12  e5
                  →
73  17  0c  02          8f  f0  fe  77

20  0d  1c  1c          b7  d7  9c  9c
```

Shift Row

After we substitute the bytes, we then shift each row a specific amount of spaces based on which row it is in. The first row will remain the same, the second shifted left by one, the third shifted left by two, and the fourth shifted left by three.

Shift Row

$$\begin{matrix} \texttt{63} & \texttt{d7} & \texttt{53} & \texttt{a4} \\ \texttt{2f} & \texttt{82} & \texttt{12} & \texttt{e5} \\ \texttt{8f} & \texttt{f0} & \texttt{fe} & \texttt{77} \\ \texttt{b7} & \texttt{d7} & \texttt{9c} & \texttt{9c} \end{matrix} \longrightarrow \begin{matrix} \texttt{63} & \texttt{d7} & \texttt{53} & \texttt{a4} \\ \texttt{82} & \texttt{12} & \texttt{e5} & \texttt{2f} \\ \texttt{fe} & \texttt{77} & \texttt{8f} & \texttt{f0} \\ \texttt{9c} & \texttt{b7} & \texttt{d7} & \texttt{9c} \end{matrix}$$

Mix Columns

We then multiply our current block with a fixed matrix. The value after mixing the columns will be the sum of the values in a column with the value being mixed multiplied by the corresponding values in a row of the matrix.

It’s important to note that the multiplication we do is not ordinary multiplication, but a special multiplication, with its own rules. This makes this process even more difficult to crack.

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

Mix Columns

63	d7	53	a4
82	12	e5	2f
fe	77	8f	f0
9c	b7	d7	9c

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

```
(63 x 02) ^

(82 x 03) ^

(fe x 01) ^

(9c x 01) = 39
```

Mix Columns

63	d7	53	a4		39	43	ca	4e
82	12	e5	2f	→	f9	dd	df	6d
fe	77	8f	f0		b9	e9	d1	cf
9c	b7	d7	9c		fa	72	2a	0b

Add Round Key

After the previous three steps, we incorporate the round key. The round key changes each round.

```
 Round 0: 41 6e 20 45 6e 63 72 79 70 74 69 6f 6e 4b 65 79
 Round 1: f3 23 96 da 9d 40 e4 a3 ed 34 8d cc 83 7f e8 b5
 Round 2: 23 b8 43 36 be f8 a7 95 53 cc 2a 59 d0 b3 c2 ec
 Round 3: 4a 9d 8d 46 f4 65 2a d3 a7 a9 00 8a 77 1a c2 66
 Round 4: e0 b8 be b3 14 dd 94 60 b3 74 94 ea c4 6e 56 8c
 Round 5: 6f 09 da af 7b d4 4e cf c8 a0 da 25 0c ce 8c a9
 Round 6: c4 6d 09 51 bf b9 47 9e 77 19 9d bb 7b d7 11 12
 Round 7: 8a ef c0 70 35 56 87 ee 42 4f 1a 55 39 98 0b 47
 Round 8: 4c c4 60 62 79 92 e7 8c 3b dd fd d9 02 45 f6 9e
 Round 9: 39 86 6b 15 40 14 8c 99 7b c9 71 40 79 8c 87 de
Round 10: 6b 91 76 a3 2b 85 fa 3a 50 4c 8b 7a 29 c0 0c a4
```

Add Round Key

$$\begin{matrix} \texttt{39} & \texttt{43} & \texttt{ca} & \texttt{4e} \\ \texttt{f9} & \texttt{dd} & \texttt{df} & \texttt{6d} \\ \texttt{b9} & \texttt{e9} & \texttt{d1} & \texttt{cf} \\ \texttt{fa} & \texttt{72} & \texttt{2a} & \texttt{0b} \end{matrix} \quad \text{XOR} \quad \begin{matrix} \texttt{f3} & \texttt{9d} & \texttt{ed} & \texttt{83} \\ \texttt{23} & \texttt{40} & \texttt{34} & \texttt{7f} \\ \texttt{96} & \texttt{e4} & \texttt{8d} & \texttt{e8} \\ \texttt{da} & \texttt{a3} & \texttt{cc} & \texttt{b5} \end{matrix} \quad \longrightarrow \quad \begin{matrix} \texttt{ca} & \texttt{de} & \texttt{27} & \texttt{cd} \\ \texttt{da} & \texttt{9d} & \texttt{eb} & \texttt{12} \\ \texttt{2f} & \texttt{0d} & \texttt{5c} & \texttt{27} \\ \texttt{20} & \texttt{d1} & \texttt{e6} & \texttt{be} \end{matrix}$$

Repeat the Four Main Steps

After the first round, we have to repeat the four main steps eight more times, each time switching the round key.

Round 2

```
ca   de   27   cd         cd   df   bb   11

da   9d   eb   12         0   d4   88   4c
                    →
2f   0d   5c   27         14   12   47   14

20   d1   e6   be         f9   e2   b6   b7
```

Round 10

On round 10, the mix columns step is skipped as it does not make the end result more secure.

$$\begin{matrix} \mathtt{e9} & \mathtt{83} & \mathtt{76} & \mathtt{97} \\ \mathtt{bf} & \mathtt{fe} & \mathtt{d4} & \mathtt{3f} \\ \mathtt{db} & \mathtt{85} & \mathtt{58} & \mathtt{68} \\ \mathtt{8f} & \mathtt{30} & \mathtt{3} & \mathtt{5a} \end{matrix} \longrightarrow \begin{matrix} \mathtt{75} & \mathtt{c7} & \mathtt{68} & \mathtt{a1} \\ \mathtt{2a} & \mathtt{cd} & \mathtt{39} & \mathtt{c8} \\ \mathtt{1c} & \mathtt{bf} & \mathtt{32} & \mathtt{9b} \\ \mathtt{1d} & \mathtt{49} & \mathtt{7e} & \mathtt{df} \end{matrix}$$

Final encrypted message = 75 2a 1c 1d c7 cd bf 49 68 39 32 7e a1 c8 9b df

Decryption

The methods used to decrypt a message encrypted with AES are essentially the methods used to encrypt it but in reverse. The value from substitute bytes can be traced back from the table, shift row and mix columns can be repeated multiple times to produce the original, and xor’ing by the same values twice also produces the original.

Future

- The 256-bit variant is significantly stronger than the 128-bit variant
- Most dangerous attacks against AES are not brute-force attacks, but rather, attacks that attempt to gain information through data leaks
- Still just a symmetric encryption system - key must be secure
- Is used and will continue to be used by countless devices and networks for the foreseeable future