Course: Modern Cryptography

Design Principles of Block Ciphers/Pseudorandom Permutations (AES)

Shashank Singh

IISER Bhopal

Sept 18, 2025

Brief history of block ciphers

- 1972: The National Institute of Standards and Technology (NIST) solicits proposals for encryption algorithms for the protection of computer data.
- 1973-1974: IBM develops DES.
- 1975: The National Security Agency (NSA) “fixed” DES.
- 1977: DES adopted as a US Federal Information Processing Standard (FIPS 46).
- 1981: DES adopted as a US banking standard (ANSI X3.92).
- 1988: Triple-DES standardized (ANSI X9.52).
- 1997: NIST begins the AES (Advanced Encryption Standard) competition.
- 1999: 5 finalists for AES announced.
- 2001: Rijndael adopted for AES (FIPS 197).
- 2024: No significant weaknesses have been found with AES

---

https://cryptography101.ca/wp-content/uploads/2025/09/V2-slides-Crypto101.pdf

Some desirable properties of block ciphers

Security:

- Diffusion: each ciphertext bit should depend on all plaintext bits.
- Confusion: the relationship between key and ciphertext bits should be complicated.
- Key length: should be small, but large enough to preclude exhaustive key search.

Some desirable properties of block ciphers

Security:

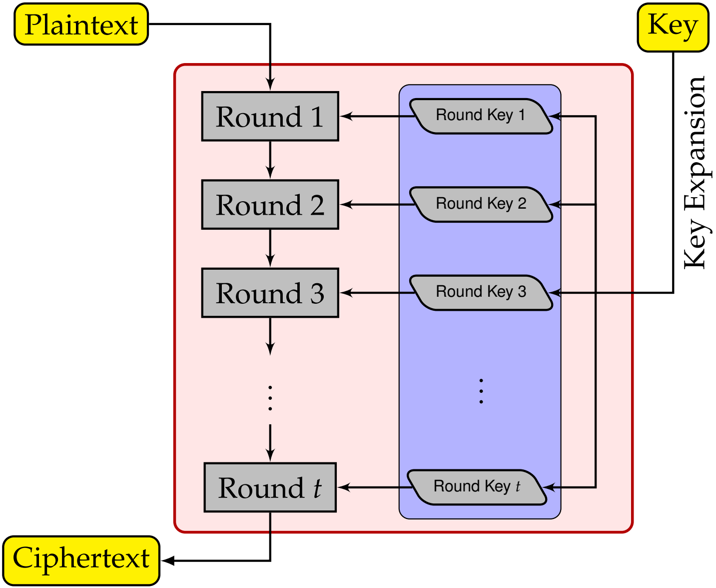
- Diffusion: each ciphertext bit should depend on all plaintext bits.
- Confusion: the relationship between key and ciphertext bits should be complicated.
- Key length: should be small, but large enough to preclude exhaustive key search.

Efficiency:

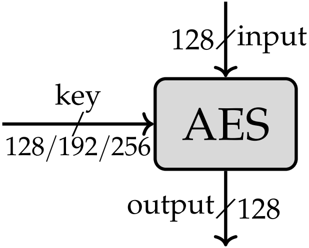
- Simplicity: easier to implement and analyze.
- Speed: high encryption and decryption rates. should be complicated.
- Platform: suitable for hardware and software.

https://cryptography101.ca/wp-content/uploads/2025/09/V2-slides-Crypto101.pdf

Block Cipher Internals



AES BLOCK CIPHER



Key	Rounds
128	10
192	12
256	14

- ☞ We will primarily focus on the design of 128 bit AES only.
- ☞ Internally, the AES operations are performed on a two-dimensional array of bytes called the State.

Table: Key-Block-Round Combinations

	Key Length (Nk words)	**Block Size** (Nb words)	**Number of Rounds** (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Source: `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf`

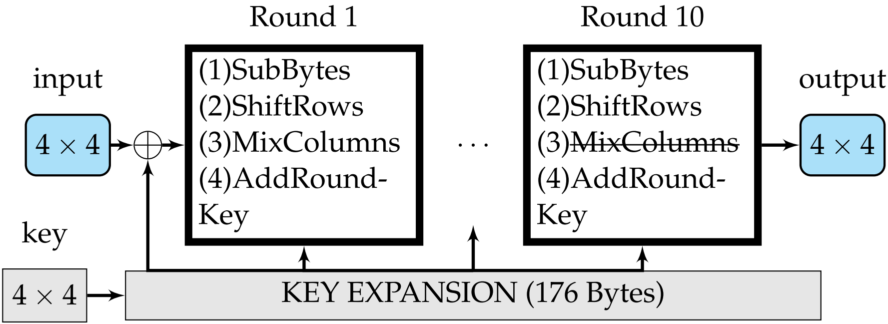
Algorithm 1: Figure 5. Pseudo Code for the Cipher.

Input : byte `in[4*Nb]`, byte `out[4*Nb]`, word `w[Nb*(Nr+1)]`

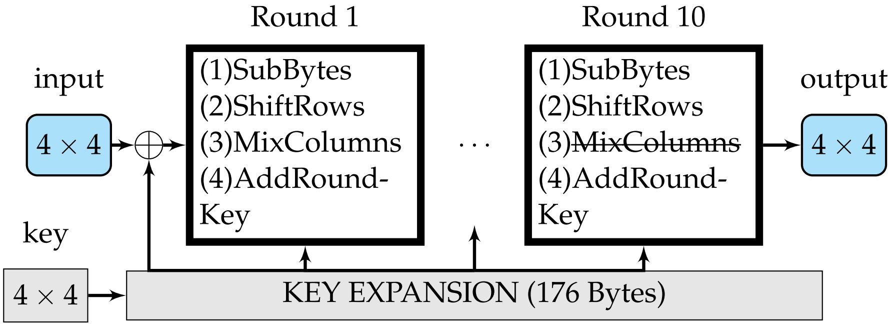
Output: Encrypted output block `out`

```
byte state[4][Nb];
state ← in;
AddRoundKey(state, w[0..Nb-1])
for round = 1 to Nr - 1 do
    SubBytes(state);
    ShiftRows(state);
    MixColumns(state);
    AddRoundKey(state, w[round*Nb .. (round+1)*Nb - 1])
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, w[Nr*Nb .. (Nr+1)*Nb - 1]);
out ← state;
```

AES-128 Encryption



AES-128 Encryption



in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

→

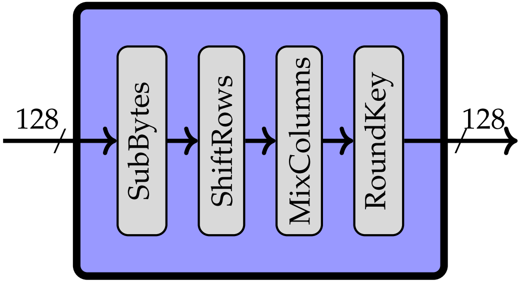
State

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$
w_0	w_1	w_2	w_3

→

out_0	out_4	out_8	out_{12}
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

A round in AES



- The basic unit for processing in the AES algorithm is a byte.
- All byte values will be represented as the concatenation of its individual bit between braces in the order $\{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}$.
- It is often convenient to denote byte values using hexa-decimal notation e.g., $\{01100011\}$ can be represented as 63.
- These bytes are also interpreted as finite field elements using a polynomial representation:

$$b(x) = \sum_{i=0}^{7} b_i x^i \in \mathbb{F}_{2^8}\langle x \rangle = \frac{\mathbb{F}_2[X]}{\langle X^8 + X^4 + X^3 + X + 1 \rangle}$$

- A word $w_0 = \left[s_{0,0}\ s_{1,0}\ s_{0,2}\ s_{0,3}\right]$ i.e., 4 bytes is represented as polynomial

$$w_0(Y) = s_{0,0} + s_{1,0}\,Y + s_{0,2}\,Y^2 + s_{0,3}\,Y^3 \in \mathbb{F}_{2^8}[Y]$$

- The multiplication "$\cdot$" of $\mathfrak{a}(Y), \mathfrak{b}(Y) \in \mathbb{F}_{2^8}[Y]$ is defined modulo $Y^4 + 1$. (Note that $Y^4 + 1$ is not irreducible)

- For the polynomial

$$a(Y) = \{03\}\,Y^3 + \{01\}\,Y^2 + \{01\}\,Y + \{03\} \in \mathbb{F}_{2^8}[Y]$$

and $a^{-1}(Y)$ exists, and

$$a^{-1}(Y) = \{0B\}\,Y^3 + \{0D\}\,Y^2 + \{09\}\,Y + \{0E\} \in \mathbb{F}_{2^8}[Y]$$

SUBBYTE()

Input State **After SubBytes**

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \xrightarrow{\text{SubByte}} \begin{bmatrix} S(a_{00}) & S(a_{01}) & S(a_{02}) & S(a_{03}) \\ S(a_{10}) & S(a_{11}) & S(a_{12}) & S(a_{13}) \\ S(a_{20}) & S(a_{21}) & S(a_{22}) & S(a_{23}) \\ S(a_{30}) & S(a_{31}) & S(a_{32}) & S(a_{33}) \end{bmatrix}$$

$S : \{0,1\}^8 \mapsto \{0,1\}^8$ is a fixed, public, invertible, non-linear function.

SubByte()..

- Let $a \in \{0,1\}^8$. Consider a as an element of GF(2^8).
- Let $b = a^{-1}$ if $a \neq 0$, and $b = a$ if $a = 0$. Let $b = (b_0 b_1 \ldots b_7)$.
- Compute

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

- $S(a) = b' = (b'_0, b'_1 \ldots b'_7)$.

SUBBYTE() USING TABLE

Table: AES S-box (SubBytes Table)

	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
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

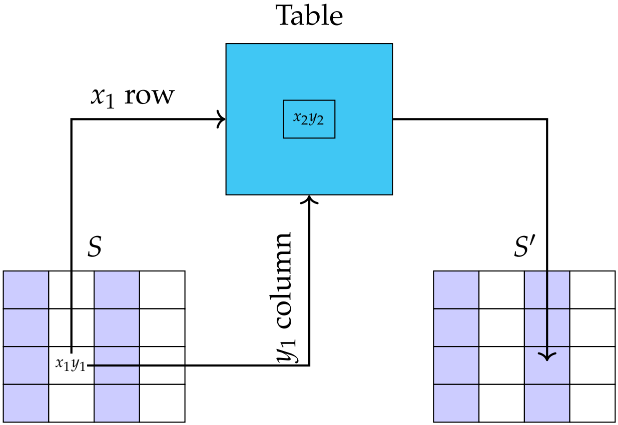
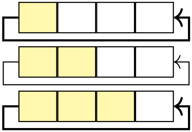


Table
x_1 row
x_2y_2
S
y_1 column
S'
x_1y_1

ShiftRow()

S

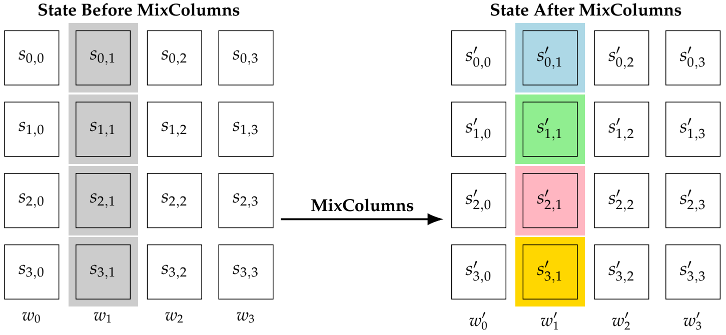
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$



S'

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

MIX COLUMNS()



$$
\begin{aligned}
s'_{0,c} &= \{02\} \cdot s_{0,c} \oplus \{03\} \cdot s_{1,c} \oplus s_{2,c} \oplus s_{3,c} \\
s'_{1,c} &= s_{0,c} \oplus \{02\} \cdot s_{1,c} \oplus \{03\} \cdot s_{2,c} \oplus s_{3,c} \\
s'_{2,c} &= s_{0,c} \oplus s_{1,c} \oplus \{02\} \cdot s_{2,c} \oplus \{03\} \cdot s_{3,c} \\
s'_{3,c} &= \{03\} \cdot s_{0,c} \oplus s_{1,c} \oplus s_{2,c} \oplus \{02\} \cdot s_{3,c},
\end{aligned}
$$

where $\cdot$ denotes multiplication over the finite field $GF(2^8)$.

MixColumns()

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

$$w'_j(Y) = w_j(Y) * a(Y) \pmod{Y^4 + 1} \text{ where,}$$

$$a(Y) = \{03\}Y^3 + \{01\}Y^2 + \{01\}Y + \{02\}$$

$$a(Y)^{-1} = \{0b\}Y^3 + \{0d\}Y^2 + \{09\}Y + \{0e\}$$

ADROUNDKEYS()

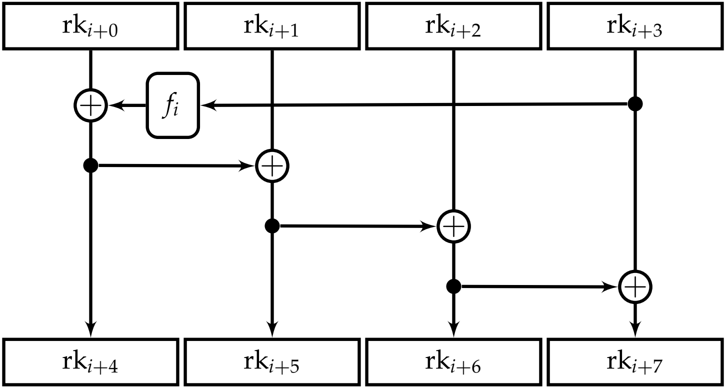
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,0}$
$k_{2,2}$	$k_{2,3}$	$k_{2,0}$	$k_{2,1}$
$k_{3,3}$	$k_{3,0}$	$k_{3,1}$	$k_{3,2}$

$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$	$S'_{1,0}$
$S'_{2,2}$	$S'_{2,3}$	$S'_{2,0}$	$S'_{2,1}$
$S'_{3,3}$	$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$

AES Key Expansion

$$k = \underbrace{k_0|k_1|k_2|k_3}_{\mathrm{rk}_0} \,|\, \underbrace{k_4|k_5|k_6|k_7}_{\mathrm{rk}_1} \,|\, \underbrace{k_8|k_9|k_{10}|k_{11}}_{\mathrm{rk}_2} \,|\, \underbrace{k_{12}|k_{13}|k_{14}|k_{15}}_{\mathrm{rk}_3}$$



AES Key Expansion..

The function $f_i : \{0,1\}^{32} \mapsto \{0,1\}^{32}$ are defined as follows:

- The input is divided into four bytes: $(a|b|c|d)$
- Left-rotate the bytes: $(b|c|d|a)$
- Apply the AES S-box to each byte:
- XOR the leftmost byte with the constant ℓ_i and output the result: $(S(b) \oplus \ell_i|S(c)|S(d)|S(a))$ The constants ℓ_i (in hexadecimal):

$$\ell_0 = \texttt{0x01}, \ell_1 = \texttt{0x02}, \ell_2 = \texttt{0x04}, \ell_3 = \texttt{0x08}, \ell_4 = \texttt{0x10}$$
$$\ell_5 = \texttt{0x20}, \ell_6 = \texttt{0x40}, \ell_7 = \texttt{0x80}, \ell_8 = \texttt{0x1b}, \ell_9 = \texttt{0x36}$$

https://cryptography101.ca/wp-content/uploads/2025/09/V2-slides-Crypto101.pdf

Appendix B – Cipher Example

The following diagram shows the values in the State array as the Cipher progresses for a block length and a Cipher Key length of 16 bytes each (i.e., $Nb = 4$ and $Nk = 4$).

```
Input =       32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
```

The Round Key values are taken from the Key Expansion example in Appendix A.

Round Number	Start of Round				After SubBytes				After ShiftRows				After MixColumns					Round Key Value				
	32	88	31	e0														2b	28	ab	09	
input	43	5a	31	37													⊕	7e	ae	f7	cf	=
	f6	30	98	07														15	d2	15	4f	
	a8	8d	a2	34														16	a6	88	3c	
	19	a0	9a	e9	d4	e0	b8	1e	d4	e0	b8	1e	04	e0	48	28		a0	88	23	2a	
1	3d	f4	c6	f8	27	bf	b4	41	bf	b4	41	27	66	cb	f8	06	⊕	fa	54	a3	6c	=
	e3	e2	8d	48	11	98	5d	52	5d	52	11	98	81	19	d3	26		fe	2c	39	76	
	be	2b	2a	08	ae	f1	e5	30	30	ae	f1	e5	e5	9a	7a	4c		17	b1	39	05	
	a4	68	6b	02	49	45	7f	77	49	45	7f	77	58	1b	db	1b		f2	7a	59	73	
2	9c	9f	5b	6a	de	db	39	02	db	39	02	de	4d	4b	e7	6b	⊕	c2	96	35	59	=
	7f	35	ea	50	d2	96	87	53	87	53	d2	96	ca	5a	ca	b0		95	b9	80	f6	
	f2	2b	43	49	89	f1	1a	3b	3b	89	f1	1a	f1	ac	a8	e5		f2	43	7a	7f	

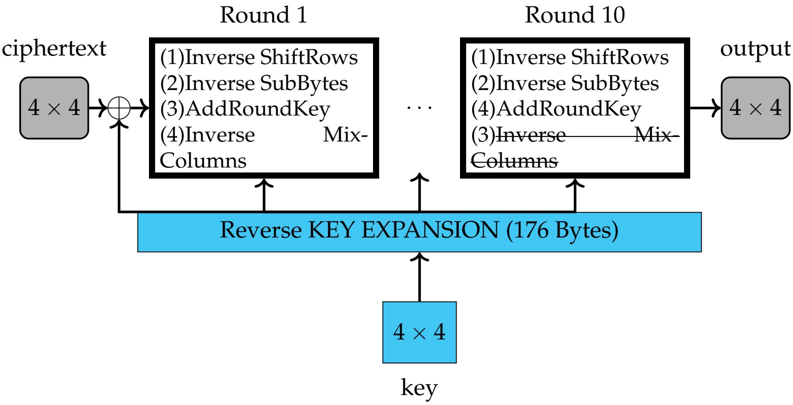
Source: `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf`

8	5a	19	a3	7a		be	d4	0a	da		be	d4	0a	da		00	b1	54	fa	⊕	ea	b5	31	7f	=
	41	49	e0	8c		83	3b	e1	64		3b	e1	64	83		51	c8	76	1b		d2	8d	2b	8d	
	42	dc	19	04		2c	86	d4	f2		d4	f2	2c	86		2f	89	6d	99		73	ba	f5	29	
	b1	1f	65	0c		c8	c0	4d	fe		fe	c8	c0	4d		d1	ff	cd	ea		21	d2	60	2f	
9	ea	04	65	85		87	f2	4d	97		87	f2	4d	97		47	40	a3	4c	⊕	ac	19	28	57	=
	83	45	5d	96		ec	6e	4c	90		6e	4c	90	ec		37	d4	70	9f		77	fa	d1	5c	
	5c	33	98	b0		4a	c3	46	e7		46	e7	4a	c3		94	e4	3a	42		66	dc	29	00	
	f0	2d	ad	c5		8c	d8	95	a6		a6	8c	d8	95		ed	a5	a6	bc		f3	21	41	6e	
10	eb	59	8b	1b		e9	cb	3d	af		e9	cb	3d	af						⊕	d0	c9	e1	b6	=
	40	2e	a1	c3		09	31	32	2e		31	32	2e	09							14	ee	3f	63	
	f2	38	13	42		89	07	7d	2c		7d	2c	89	07							f9	25	0c	0c	
	1e	84	e7	d2		72	5f	94	b5		b5	72	5f	94							a8	89	c8	a6	

output	39	02	dc	19
	25	dc	11	6a
	84	09	85	0b
	1d	fb	97	32

Source: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

AES Decryption



In this course:

- 2^{40} operations is considered very easy.
- 2^{56} operations is considered easy.
- 2^{64} operations is considered feasible.
- 2^{80} operations is considered barely feasible.
- 2^{128} operations is considered infeasible.

The Bitcoin network is performing about 2^{80} hash operations per hour.

WIKIPEDIA
The Free Encyclopedia
Brute-force attack

The Landauer limit from thermodynamics suggests that exhaustively trying 2^{128} symmetric keys would require $\gg 3000$ gigawatts of power for one year, which is $\gg 100\%$ of the world's energy production.

---

a screenshot from Alfred's slides.