AES (step-by-step)

The most common modern encryption method

Cipher | Description | Background | Security

Inspect the encryption of AES step by step. Tap on each byte to see the bytes it depends on.

Configuration AES-128

AES Variants and Test Vectors

Number of Rounds: 10 [−] [+]

S-Box

Permutation

Chaining: None | CBC | ECB

Initial Vector (CBC only)

Key

`61626563 61646c6f 61626563 61646c6f`

Expanded Key

Input

`68656c6c 6f776f72 6c646973 6261636b`

Encoding Rounds

Round 1

input to Round 1

`0907090f 0e13031d 0d060c10 03050f04`

after S-Box: ON

`01c50176 ab7d7ba4 d76ffeca 7b6b76f2`

after permutation: ON

`017dfef2 ab6f7676 d76b01a4 7bc57bca`

after mult: ON

`8910967f fc99b213 ada6495b 13ad0dbc`

250a8ef

ON

aa225bf3 becf13f0 8e928ddb 51fda553

Round 2

input to Round 2

aa225bf3 becf13f0 8e928ddb 51fda553

after S-Box: ON

ac93390d ae8a7d8c 194f5db9 d15406ed

after permutation: ON

ac8a5ded ae4f060d 1954398c d1937db9

after mult: ON

76a9b0f9 9d37faba 7b76b045 d3d268ef

used subkey:

72f012a0 30a6b343 139277c3 51c2df2c

after mix with key: ON

0459a259 ad9149f9 68e4c786 8210b7c3

Round 3

input to Round 3

0459a259 ad9149f9 68e4c786 8210b7c3

after S-Box: ON

f2cb3acb 95813b99 4569c644 13caa92e

after permutation: ON

f281c62e 9569a9cb 45ca3a99 13cb3b44

after mult: ON

8f949616 e86cf3e9 6c1d4b16 1f97624d

used subkey:

536e6371 63c8d032 705aa7f1 219878dd

after mix with key: ON

dcfaf567 8ba423db 1c47ece7 3e0f1a90

Round 4

input to Round 4

	ON
276a260	
after permutation:	ON
8649ce60 3da0a285 9c76e6b9 b22d2694	
after mult:	ON
623de8d6 a61e5654 e6f8ed46 ba1674f5	
used subkey:	
1dd2a28c 7e1a72be 0e40d54f 2fd8ad92	
after mix with key:	ON
7fef4a5a d80424ea e8b83809 95ced967	

Round 5

input to Round 5	
7fef4a5a d80424ea e8b83809 95ced967	
after S-Box:	ON
d2dfd6be 61f23687 9b6c0701 2a8b3585	
after permutation:	ON
d2f20785 616c35be 9b8bd687 2adf3601	
after mult:	ON
30a1ba89 fd58be9d fa7035fe 19d49a95	
used subkey:	
6c47ed99 125d9f27 1c1d4a68 33c5e7fa	
after mix with key:	ON
5ce65710 ef0521ba e66d7f96 2a117d6f	

Round 6

input to Round 6	
5ce65710 ef0521ba e66d7f96 2a117d6f	
after S-Box:	ON
4a8e5bca df6bfdf4 8e3cd290 e582ffa8	
after permutation:	ON
4a6bd2a8 df3cffca 8e825bf4 e58efd90	
after mult:	ON
53597d2c d4774336 3588bda3 356e217c	

756f2ef
ON
b98abd76 2cf91c4b d11ba8b6 e238d393

Round 7

input to Round 7
b98abd76 2cf91c4b d11ba8b6 e238d393
after S-Box: ON
567e7a38 71999cb3 3eafc24e 980766dc
after permutation: ON
5699c2dc 71af6638 3e077ab3 987e9c4e
after mult: ON
02fe2f02 56a65a2a bc0d0342 7b9517cd
used subkey:
1b5a1f54 e3d44029 0747553c d011a7d3
after mix with key: ON
19a43056 b5721a03 bb4a567e ab84b01e

Round 8

input to Round 8
19a43056 b5721a03 bb4a567e ab84b01e
after S-Box: ON
d44904b1 d540a27b ead6b1f3 625fe772
after permutation: ON
d440b172 d5d6e7b1 ea5f047b 6249a2f3
after mult: ON
b0ee7b72 86e11e2c 51233088 4efe7ab0
used subkey:
19067924 fad2390d fd956c31 2d84cbe2
after mix with key: ON
a9e80256 7c332721 acb65cb9 637ab152

Round 9

input to Round 9

ON

bdac800

after permutation: ON

d3c34a00 104ec8b1 91da77fd fb9bcc56

after mult: ON

a99084e7 8b7e1dcf c65ab9e4 c1cf19ed

used subkey:

5d19e1fc a7cbd8f1 5a5eb4c0 77da7f22

after mix with key: ON

f489651b 2cb5c53e 9c040d24 b61566cf

Round 10

input to Round 10

f489651b 2cb5c53e 9c040d24 b61566cf

after S-Box: ON

bfa74daf 71d5a6b2 def2d736 4e59338a

after permutation: ON

bfd5d78a 71f233af de594db2 4ea7a636

used subkey:

3ccb7209 9b00aaf8 c15e1e38 b684611a

after mix with key: ON

831ea583 eaf29957 1f07538a f823c72c

Encoded

831ea583 eaf29957 1f07538a f823c72c

Decoding Rounds

Round 10

input to Round 10

bfd5d78a 71f233af de594db2 4ea7a636

after permutation: ON

bfa74daf 71d5a6b2 def2d736 4e59338a

after S-Box: ON

f489651b 2cb5c53e 9c040d24 b61566cf

used subkey:

ON

1cf19ed

after mult: ON

d3c34a00 104ec8b1 91da77fd fb9bcc56

Round 9

input to Round 9

d3c34a00 104ec8b1 91da77fd fb9bcc56

after permutation: ON

d39b77b1 10c3ccfd 914e4a56 fbdac800

after S-Box: ON

a9e80256 7c332721 acb65cb9 637ab152

used subkey:

19067924 fad2390d fd956c31 2d84cbe2

after mix with key: ON

b0ee7b72 86e11e2c 51233088 4efe7ab0

after mult: ON

d440b172 d5d6e7b1 ea5f047b 6249a2f3

Round 8

input to Round 8

d440b172 d5d6e7b1 ea5f047b 6249a2f3

after permutation: ON

d44904b1 d540a27b ead6b1f3 625fe772

after S-Box: ON

19a43056 b5721a03 bb4a567e ab84b01e

used subkey:

1b5a1f54 e3d44029 0747553c d011a7d3

after mix with key: ON

02fe2f02 56a65a2a bc0d0342 7b9517cd

after mult: ON

5699c2dc 71af6638 3e077ab3 987e9c4e

Round 7

87e9c4e

ON

567e7a38 71999cb3 3eafc24e 980766dc

after S-Box: ON

b98abd76 2cf91c4b d11ba8b6 e238d393

used subkey:

ead3c05a f88e5f7d e4931515 d756f2ef

after mix with key: ON

53597d2c d4774336 3588bda3 356e217c

after mult: ON

4a6bd2a8 df3cffca 8e825bf4 e58efd90

Round 6

input to Round 6

4a6bd2a8 df3cffca 8e825bf4 e58efd90

after permutation: ON

4a8e5bca df6bfdf4 8e3cd290 e582ffa8

after S-Box: ON

5ce65710 ef0521ba e66d7f96 2a117d6f

used subkey:

6c47ed99 125d9f27 1c1d4a68 33c5e7fa

after mix with key: ON

30a1ba89 fd58be9d fa7035fe 19d49a95

after mult: ON

d2f20785 616c35be 9b8bd687 2adf3601

Round 5

input to Round 5

d2f20785 616c35be 9b8bd687 2adf3601

after permutation: ON

d2dfd6be 61f23687 9b6c0701 2a8b3585

after S-Box: ON

7fef4a5a d80424ea e8b83809 95ced967

used subkey:

	ON
	a1674f5
after mult:	ON
8649ce60 3da0a285 9c76e6b9 b22d2694	

Round 4

input to Round 4
8649ce60 3da0a285 9c76e6b9 b22d2694
after permutation: ON
862de685 3d4926b9 9ca0ce94 b276a260
after S-Box: ON
dcfaf567 8ba423db 1c47ece7 3e0f1a90
used subkey:
536e6371 63c8d032 705aa7f1 219878dd
after mix with key: ON
8f949616 e86cf3e9 6c1d4b16 1f97624d
after mult: ON
f281c62e 9569a9cb 45ca3a99 13cb3b44

Round 3

input to Round 3
f281c62e 9569a9cb 45ca3a99 13cb3b44
after permutation: ON
f2cb3acb 95813b99 4569c644 13caa92e
after S-Box: ON
0459a259 ad9149f9 68e4c786 8210b7c3
used subkey:
72f012a0 30a6b343 139277c3 51c2df2c
after mix with key: ON
76a9b0f9 9d37faba 7b76b045 d3d268ef
after mult: ON
ac8a5ded ae4f060d 1954398c d1937db9

Round 2

1937db9
ON
ac93390d ae8a7d8c 194f5db9 d15406ed
after S-Box: ON
aa225bf3 becf13f0 8e928ddb 51fda553
used subkey:
2332cd8c 4256a1e3 2334c480 4250a8ef
after mix with key: ON
8910967f fc99b213 ada6495b 13ad0dbc
after mult: ON
017dfef2 ab6f7676 d76b01a4 7bc57bca

Round 1

input to Round 1
017dfef2 ab6f7676 d76b01a4 7bc57bca
after permutation: ON
01c50176 ab7d7ba4 d76ffeca 7b6b76f2
after S-Box: ON
0907090f 0e13031d 0d060c10 03050f04
used subkey:
61626563 61646c6f 61626563 61646c6f
after mix with key: ON
68656c6c 6f776f72 6c646973 6261636b

Decoded

68656c6c 6f776f72 6c646973 6261636b

Share link