CrypTool-Online
Cryptography for everybody

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

00010203 04050607 08090a0b 0c0d0e0f

Expanded Key

Input

42726967 6874206e 65772069 64656173

Encoding Rounds

Round 1

input to Round 1

42736b64 6c712669 6d7e2a62 68686f7c

after S-Box: ON

2c8f7f43 50a3f7f9 3cf3e5aa 4545a810

after permutation: ON

2ca3e510 50f3a843 3c457ff9 458ff7aa

after mult: ON

53556e12 450d2d2d 31ce9797 5de8daf8

used subkey:

d6aa74fd d2af72fa daa678f1 d6ab76fe

CrypTool-Online
Cryptography for everybody

ON

b43ac06

Round 2

Round 3

Round 4

Round 5

Round 6

Round 7

Round 8

Round 9

Round 10

Encoded

```
833616e5  cc4bd4dd  43b8b80a  e40c4968
```

Decoding Rounds

Round 10

Round 9

Round 8

Round 7

Round 6

Round 5

Round 4

Round 3

Round 2

Round 1

Decoded

```
42726967  6874206e  65772069  64656173
```

Share link