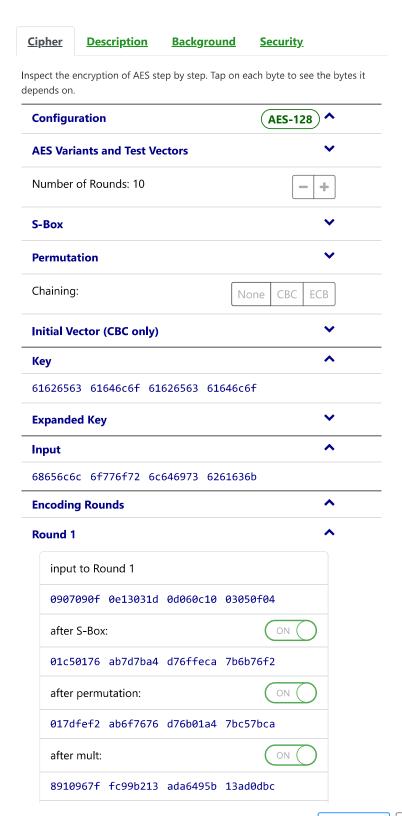


Portal CT1 CT2 JCT







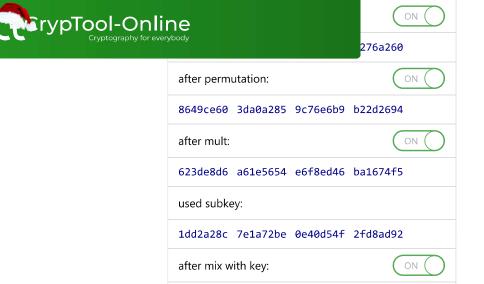


aa225bf3 becf13f0 8e928ddb 51fda553



## **Round 3** input to Round 3 0459a259 ad9149f9 68e4c786 8210b7c3 after S-Box: ON ( f2cb3acb 95813b99 4569c644 13caa92e ON after permutation: f281c62e 9569a9cb 45ca3a99 13cb3b44 ON ( after mult: 8f949616 e86cf3e9 6c1d4b16 1f97624d used subkey: 536e6371 63c8d032 705aa7f1 219878dd after mix with key: dcfaf567 8ba423db 1c47ece7 3e0f1a90





#### **Round 5**

input to Round 5

7fef4a5a d80424ea e8b83809 95ced967

after S-Box:

d2dfd6be 61f23687 9b6c0701 2a8b3585

after permutation:

d2f20785 616c35be 9b8bd687 2adf3601

after mult:

30a1ba89 fd58be9d fa7035fe 19d49a95

used subkey:

6c47ed99 125d9f27 1c1d4a68 33c5e7fa

after mix with key:

5ce65710 ef0521ba e66d7f96 2a117d6f

7fef4a5a d80424ea e8b83809 95ced967

### **Round 6**

input to Round 6

5ce65710 ef0521ba e66d7f96 2a117d6f

after S-Box:

4a8e5bca df6bfdf4 8e3cd290 e582ffa8

after permutation:

0N

A6bd2a8 df3cffca 8e825bf4 e58efd90

after mult:

0N

S3597d2c d4774336 3588bda3 356e217c



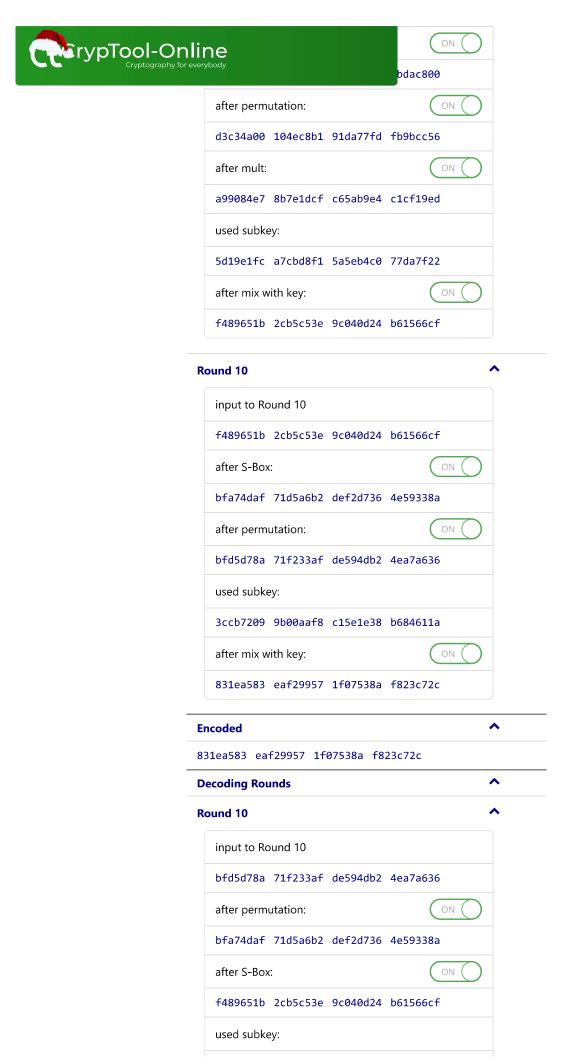


b98abd76 2cf91c4b d11ba8b6 e238d393

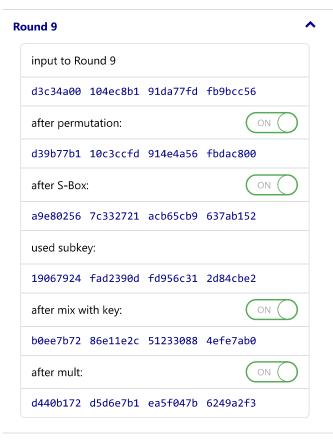


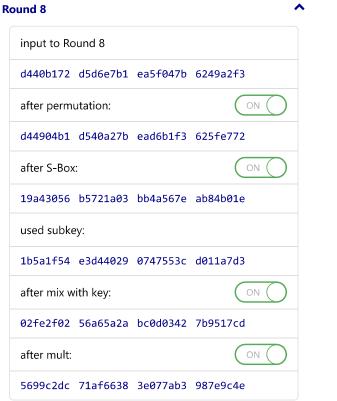
## **Round 8** input to Round 8 19a43056 b5721a03 bb4a567e ab84b01e after S-Box: ON ( d44904b1 d540a27b ead6b1f3 625fe772 ON after permutation: d440b172 d5d6e7b1 ea5f047b 6249a2f3 ON ( after mult: b0ee7b72 86e11e2c 51233088 4efe7ab0 used subkey: 19067924 fad2390d fd956c31 2d84cbe2 after mix with key: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

Round 9 input to Round 9

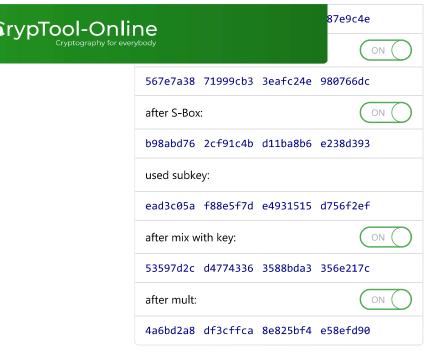








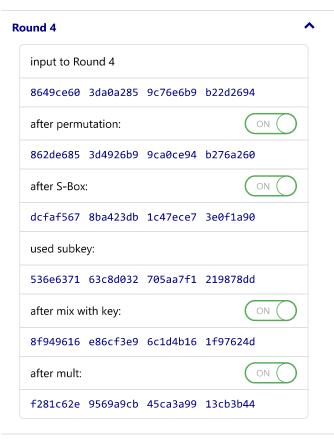
**Round 7** 

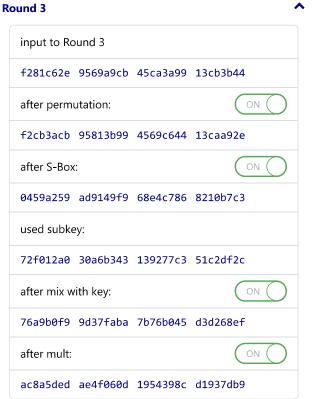


# **Round 6** input to Round 6 4a6bd2a8 df3cffca 8e825bf4 e58efd90 ( ON after permutation: 4a8e5bca df6bfdf4 8e3cd290 e582ffa8 after S-Box: 5ce65710 ef0521ba e66d7f96 2a117d6f used subkey: 6c47ed99 125d9f27 1c1d4a68 33c5e7fa ( ON ( after mix with key: 30a1ba89 fd58be9d fa7035fe 19d49a95 after mult: ON ( d2f20785 616c35be 9b8bd687 2adf3601

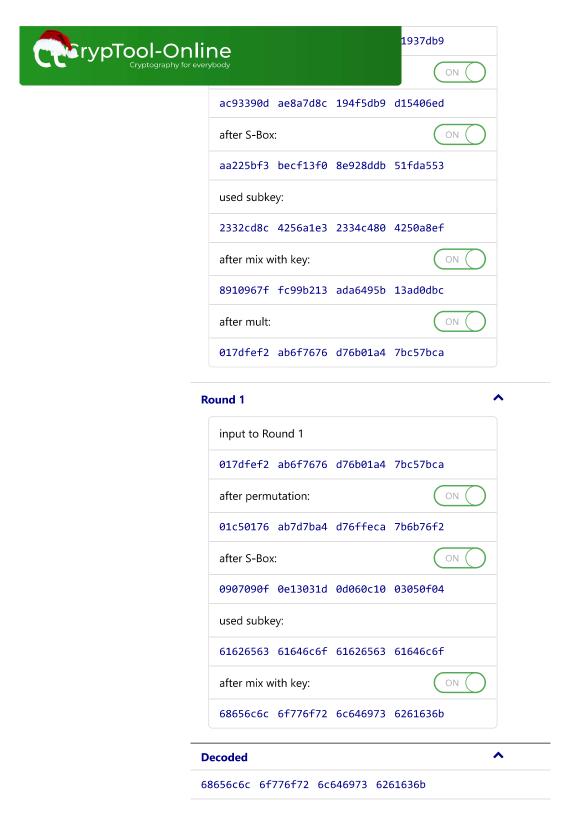








Round 2



Share link