Name : Alaa Salah Abd El-Fattah

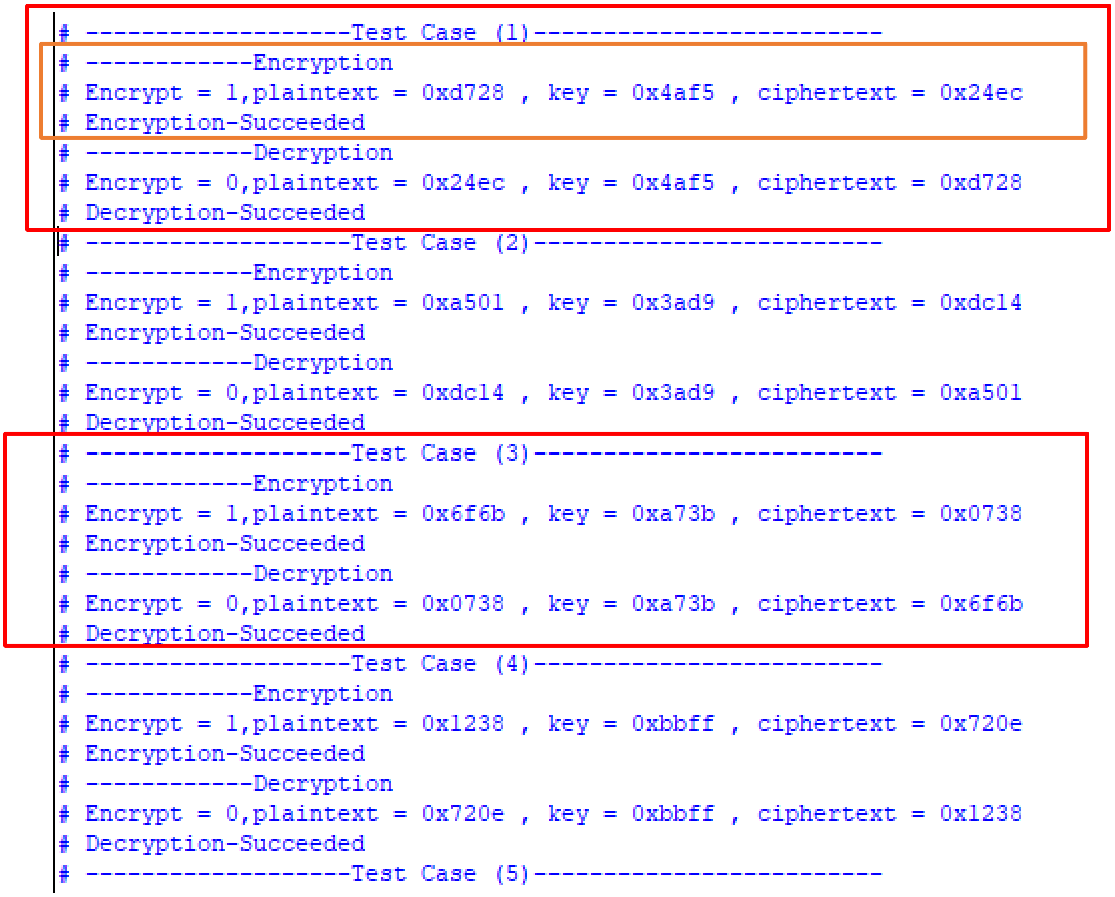
ID : 1900916

S-AES

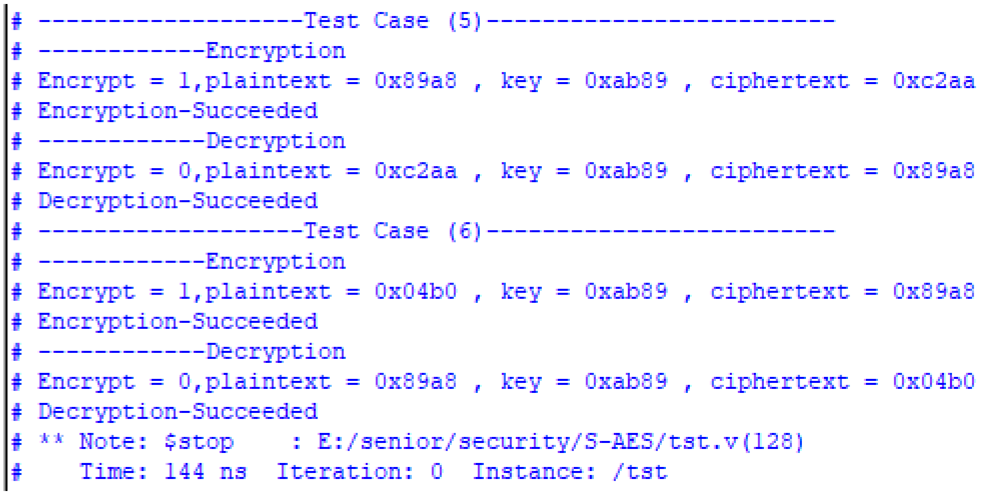
Simplified-AES using Verilog

Alaa Salah
[Email address]

1. Snippets : (6-test cases)



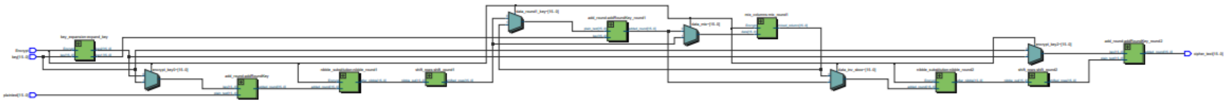
```
# --------------------Test Case (1)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0xd728 , key = 0x4af5 , ciphertext = 0x24ec
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0x24ec , key = 0x4af5 , ciphertext = 0xd728
# Decryption-Succeeded
# --------------------Test Case (2)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0xa501 , key = 0x3ad9 , ciphertext = 0xdc14
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0xdc14 , key = 0x3ad9 , ciphertext = 0xa501
# Decryption-Succeeded
# --------------------Test Case (3)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0x6f6b , key = 0xa73b , ciphertext = 0x0738
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0x0738 , key = 0xa73b , ciphertext = 0x6f6b
# Decryption-Succeeded
# --------------------Test Case (4)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0x1238 , key = 0xbbff , ciphertext = 0x720e
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0x720e , key = 0xbbff , ciphertext = 0x1238
# Decryption-Succeeded
# --------------------Test Case (5)-------------------------
```



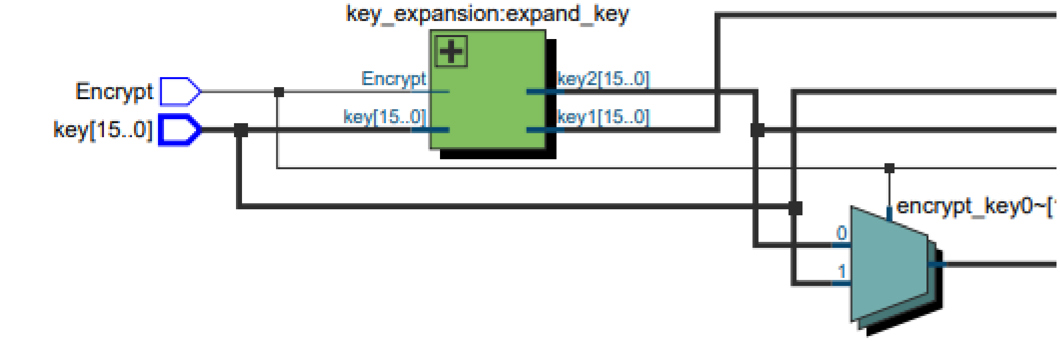
```
# --------------------Test Case (5)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0x89a8 , key = 0xab89 , ciphertext = 0xc2aa
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0xc2aa , key = 0xab89 , ciphertext = 0x89a8
# Decryption-Succeeded
# --------------------Test Case (6)-------------------------
# ------------Encryption
# Encrypt = 1,plaintext = 0x04b0 , key = 0xab89 , ciphertext = 0x89a8
# Encryption-Succeeded
# ------------Decryption
# Encrypt = 0,plaintext = 0x89a8 , key = 0xab89 , ciphertext = 0x04b0
# Decryption-Succeeded
# ** Note: $stop    : E:/senior/security/S-AES/tst.v(128)
#    Time: 144 ns  Iteration: 0  Instance: /tst
```

2. Model sim used to run and simulate the code

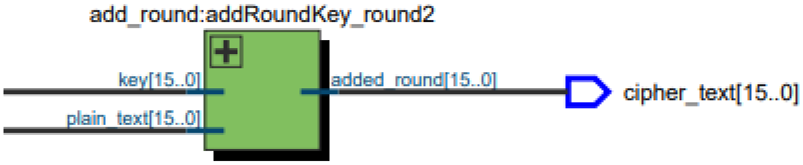
3. Netlist (schematic) using Quartus tool :



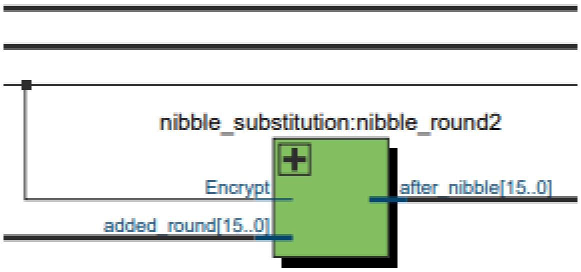
1. Key expansion :



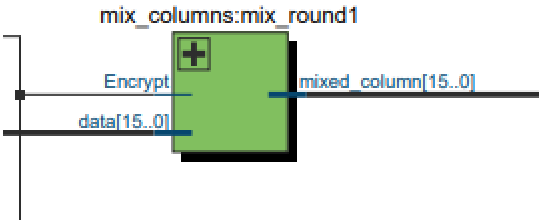
2. Add round key :



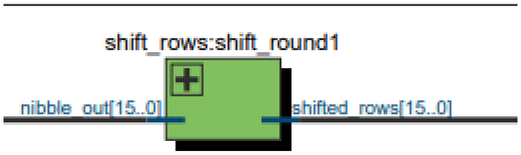
3. Nibble sub :



4. Mixed columns :



5. Shift rows


shift_rows:shift_round1
nibble_out[15..0]
shifted_rows[15..0]