Assignment 2

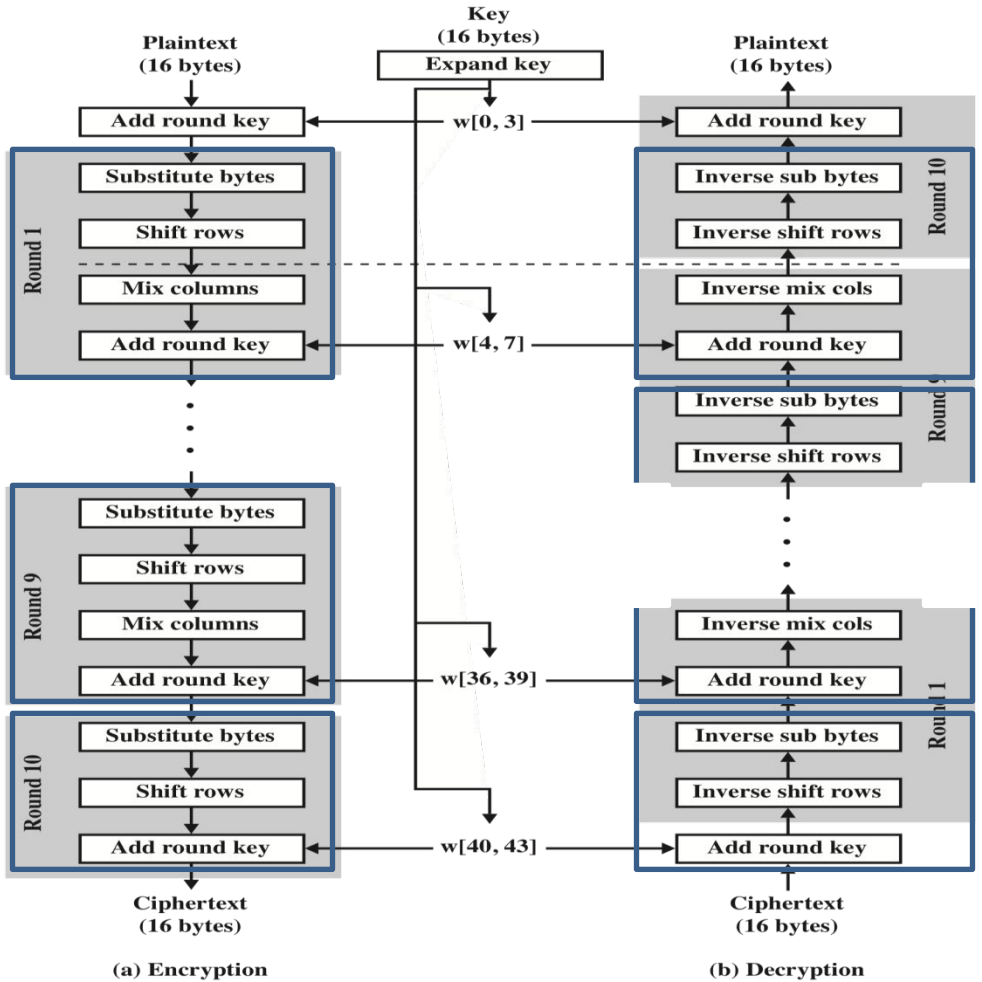
Network security

Project #2: Encryption and Decryption using AES algorithm

1. Hritik Goel (2018148)
2. Dushyant Panchal (2018033)

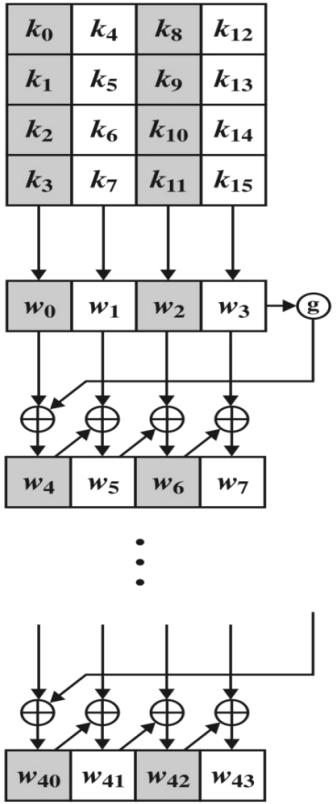
DESCRIPTION

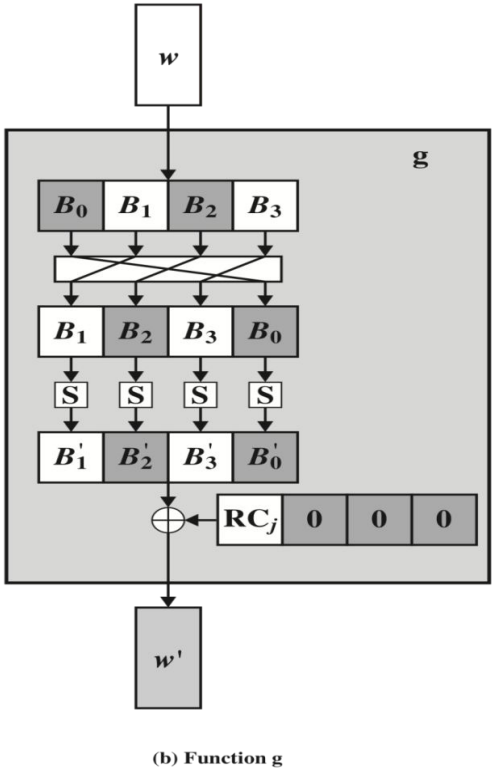
- Plain text : 128 bit
- # rounds : 10
- Key size : 128 bit
- All computations are in GF(2**8)
- Irreducible polynomial : x^8 + x^4 + x^3 + x + 1



Modules

- GET_SUBKEYS
  - It takes initial key (seed) and number of rounds as input.
  - Returns the key list consisting of keys for each of the rounds.

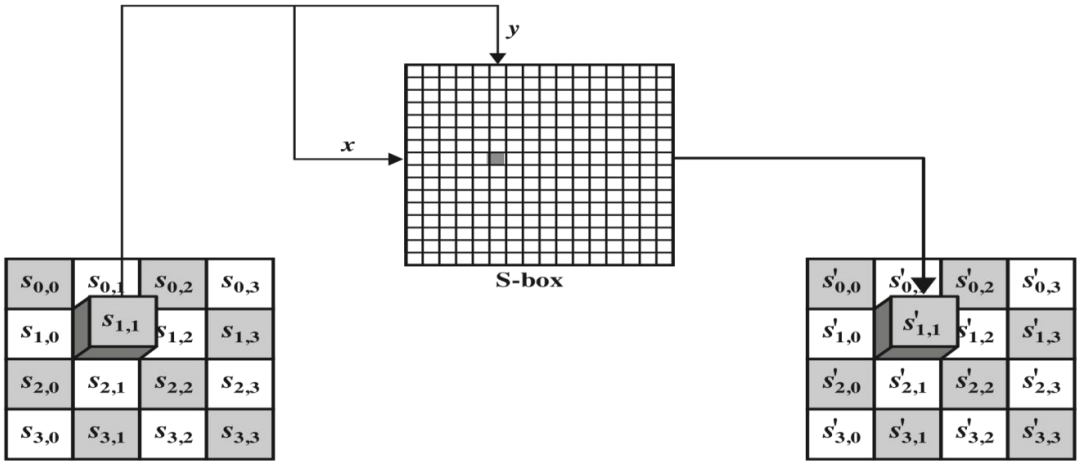




(b) Function g

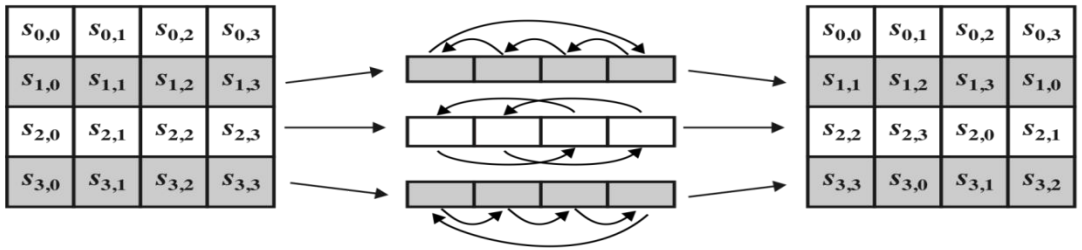
Modules

- SUBSTITUTE_BYTES
  - Performs the transformation of the 4x4 input state matrix.
  - For each element, calls “SUBSTITUTE” which replaces the byte using S-Boxes/Inverse-S-Boxes implemented as a lookup-table.



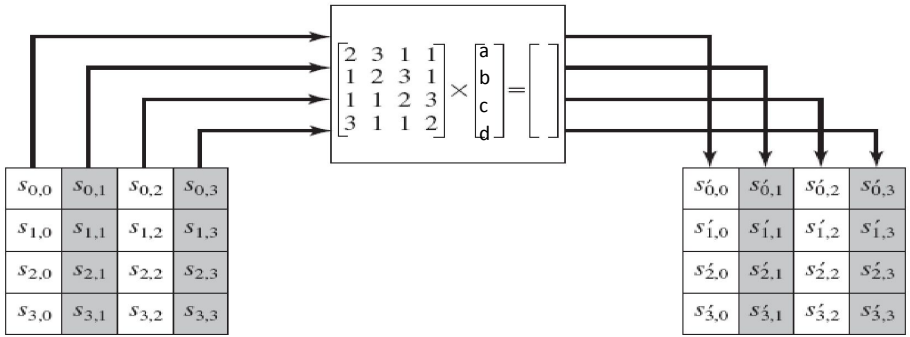
Modules

- SHIFT_ROWS
  - Performs the left shift row transformation on the input 4x4 state matrix.
  - Using numpy.roll for fast and easy implementation.



Modules

- MIX_COLUMNS
  - Performs the mix column transformation on the input 4x4 state matrix.
  - Using “galois” python library which is an extension to the numpy library, helps in faster matrix multiplication in Galois Field.
  - `GF = galois.GF(2**8, (1,0,0,0,1,1,0,1,1))`



Modules

- ADD_ROUND_KEY
  - Performs the add round key transformation on the input state matrix.
  - Nothing more than just element-wise, bitwise xor operation between the state matrix and the subkey.

Modules

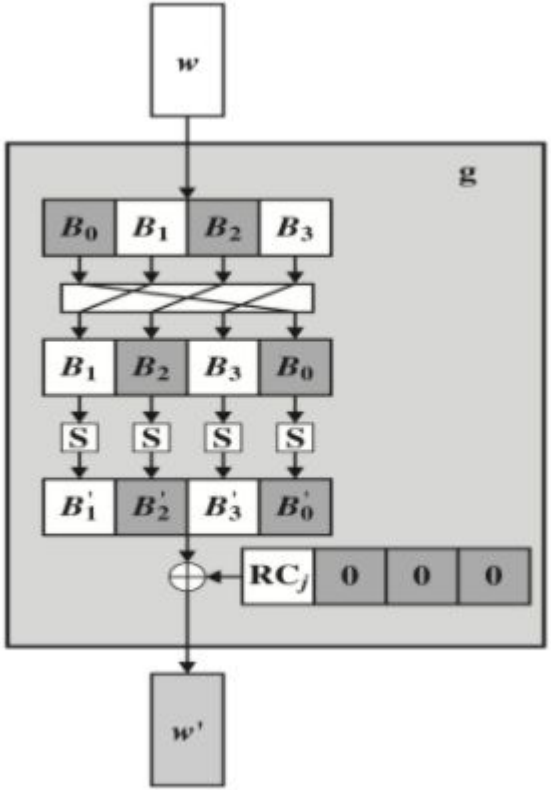
- ENCRYPT
  - ENCRYPT_ROUND implements a single round of encryption allowing to omit the MixColumns transformation (as needed for round 10).
  - ENCRYPT module performs the initial add round key, followed by the 10 calls to the ENCRYPT_ROUND module above, the tenth one specifying to omit the mix columns.

Modules

- DECRYPT
  - DECRYPT_ROUND implements a single round of decryption allowing to omit the InverseMixColumns transformation (as needed for round 1). All the transformations are inverses w.r.t the ENCRYPT_ROUND.
  - DECRYPT module performs 10 calls to the DECRYPT_ROUND module above, the first one omitting the inverse mix columns, followed by the final add round key operation.

Modules

- Other Helper Functions
  - Cal_decimal - converts binary to decimal
  - Cal_subKey - calculates the g function of last 32-bit of previous round sub-key
  - Print_hex - Prints a state as hex codes.



THANK YOU