Assignment 2

AES Algorithm Implementation

By: Dheeraj - 2017044, Sehaj Singh - 2017099

Details of Implementation

- The plaintext provided is broken down into blocks of 16 bytes and then further converted into hex format
- The 16-byte key provided is also converted into hex format and all the keys required for 10 rounds of encryption are generated.
- Each block of plaintext is taken and is fed into the encryption algorithm which does 10-round encryption. Each of the first 9 rounds consists of 4 main steps, i.e, “Substitute Bytes”, “Shift-Rows”, “Mix Columns” and “Add-Round Key” (one of the generated keys). The 10th round is special because it consists of only 3 steps. It doesn’t perform the “Mix-Columns” step. The sequence of each step is important and should be followed.
- Before the 10 rounds, there is a 0th round in which the original key is added (XOR’ed) to the plaintext.
- Finally while decrypting, the inverse of the 4 steps are performed and the generated keys are also used in reverse order. Doing so, we get the plaintext again.

Interesting Results

- The intermediate ciphertexts during encryption rounds (10 in number) are also seen in the reverse order during the decryption rounds (10 in number) and finally the plaintext matches the one the sender sent.
- A small change in plaintext leads to a change in the ciphertext to a much larger extent. This effect is called the Avalanche effect that is also seen in the DES algorithm.

Additional Details

- We used Python language to implement the AES Algorithm.
- To perform arithmetic operations in Galois fields, we used a python library called ‘pyfinite’. For certain transformations, we used a ‘numpy’ library.
- Additional references: Lecture slides

Sample Run 1

```
Input Plaintext:abcdefghijklmnop
Input 16 byte key for encrypting the plaintext:qazwsxedcrfvtgby



plaintext in blocks of bytes:
 [[['61', '62', '63', '64'], ['65', '66', '67', '68'], ['69', '6A', '6B', '6C'], ['6D', '6E', '6F', '70']]]

key in blocks of bytes:
 [['71', '61', '7A', '77'], ['73', '78', '65', '64'], ['63', '72', '66', '76'], ['74', '67', '62', '79']]
Keys Generation process initiating...
11 roundkeys are:
 [['71', '61', '7A', '77'], ['73', '78', '65', '64'], ['63', '72', '66', '76'], ['74', '67', '62', '79']]
[['F5', 'CB', 'CC', 'E5'], ['86', 'B3', 'A9', '81'], ['E5', 'C1', 'CF', 'F7'], ['91', 'A6', 'AD', '8E']]
[['D3', '5E', 'D5', '64'], ['55', 'ED', '7C', 'E5'], ['B0', '2C', 'B3', '12'], ['21', '8A', '1E', '9C']]
[['A9', '2C', '0B', '99'], ['FC', 'C1', '77', '7C'], ['4C', 'ED', 'C4', '6E'], ['6D', '67', 'DA', 'F2']]
[['24', '7B', '82', 'A5'], ['D8', 'BA', 'F5', 'D9'], ['94', '57', '31', 'B7'], ['F9', '30', 'EB', '45']]
[['30', '92', 'EC', '3C'], ['E8', '28', '19', 'E5'], ['7C', '7F', '28', '52'], ['85', '4F', 'C3', '17']]
[['94', 'BC', '1C', 'AB'], ['7C', '94', '05', '4E'], ['00', 'EB', '2D', '1C'], ['85', 'A4', 'EE', '0B']]
[['9D', '94', '37', '3C'], ['E1', '00', '32', '72'], ['E1', 'EB', '1F', '6E'], ['64', '4F', 'F1', '65']]
[['99', '35', '7A', '7F'], ['78', '35', '48', '0D'], ['99', 'DE', '57', '63'], ['FD', '91', 'A6', '06']]
[['03', '11', '15', '2B'], ['7B', '24', '5D', '26'], ['E2', 'FA', '0A', '45'], ['1F', '6B', 'AC', '43']]
[['4A', '80', '0F', 'EB'], ['31', 'A4', '52', 'CD'], ['D3', '5E', '58', '88'], ['CC', '35', 'F4', 'CB']]

Key generation completed.
```

```
starting encryption
plain text before initial permutation of encryption:
['61', '62', '63', '64'] ['65', '66', '67', '68'] ['69', '6A', '6B', '6C'] ['6D', '6E', '6F', '70']
Plain text after initial permutation of encryption:
['10', '03', '19', '13'] ['16', '1E', '02', '0C'] ['0A', '18', '0D', '1A'] ['19', '09', '0D', '09']
Plain text after round 1 :
['3A', '86', 'C2', '07'] ['4E', 'AA', '71', 'C8'] ['02', '3D', '03', '6C'] ['7A', 'BF', '11', 'BA']
Plain text after round 2 :
['A8', 'E4', '08', 'DB'] ['25', 'D4', '3F', 'A0'] ['8B', 'CC', 'A5', '6D'] ['B1', '76', '2D', 'AE']
Plain text after round 3 :
['0C', '90', 'BA', '59'] ['3E', 'A2', '78', 'C7'] ['AE', '10', '9A', 'FA'] ['14', 'DE', 'D5', 'D5']
Plain text after round 4 :
['36', '21', '28', '38'] ['2A', '49', 'CD', '50'] ['52', '48', '6A', 'FE'] ['27', 'F8', '65', 'D6']
Plain text after round 5 :
['83', '11', 'D7', 'FD'] ['85', 'B9', '3D', 'C0'] ['D8', 'F2', 'F4', '81'] ['1C', '05', '45', '75']
Plain text after round 6 :
['8F', 'BB', '7F', '4C'] ['F3', 'EC', '3B', 'A3'] ['CB', 'F4', 'EE', 'B5'] ['10', '42', 'AA', '09']
Plain text after round 7 :
['1B', '19', 'D9', '4D'] ['A4', 'AE', 'B8', '24'] ['73', 'CB', '8D', 'A5'] ['F9', 'A2', '6A', '99']
Plain text after round 8 :
['58', '40', 'A2', 'EB'] ['2A', 'A7', '24', '16'] ['D1', '4C', 'D2', '8A'] ['D9', '09', '39', '02']
Plain text after round 9 :
['F1', '70', 'CB', '92'] ['2A', '4C', '95', 'E0'] ['E0', 'CF', '88', 'B2'] ['26', '68', '7E', 'DF']
Plaintext after round 10 (special) :
['EB', 'A9', 'CB', '75'] ['D4', '2E', 'A1', '82'] ['32', '1B', '47', '69'] ['3B', '64', 'DE', 'FC']
The final cyphertext is:  EBA9CB75D42EA182321B47693B64DEFC
```

```
Decrypting the cypher text:
Cipher text before first (special) round of decryption:
['EB', 'A9', 'CB', '75'] ['D4', '2E', 'A1', '82'] ['32', '1B', '47', '69'] ['3B', '64', 'DE', 'FC']
Cipher text after first round of decryption:
['F1', '70', 'CB', '92'] ['2A', '4C', '95', 'E0'] ['E0', 'CF', '88', 'B2'] ['26', '68', '7E', 'DF']
Cypher text after round 2 :
['58', '40', 'A2', 'EB'] ['2A', 'A7', '24', '16'] ['D1', '4C', 'D2', '8A'] ['D9', '09', '39', '02']
Cypher text after round 3 :
['1B', '19', 'D9', '4D'] ['A4', 'AE', 'B8', '24'] ['73', 'CB', '8D', 'A5'] ['F9', 'A2', '6A', '99']
Cypher text after round 4 :
['8F', 'BB', '7F', '4C'] ['F3', 'EC', '3B', 'A3'] ['CB', 'F4', 'EE', 'B5'] ['10', '42', 'AA', '09']
Cypher text after round 5 :
['83', '11', 'D7', 'FD'] ['85', 'B9', '3D', 'C0'] ['D8', 'F2', 'F4', '81'] ['1C', '05', '45', '75']
Cypher text after round 6 :
['36', '21', '28', '38'] ['2A', '49', 'CD', '50'] ['52', '48', '6A', 'FE'] ['27', 'F8', '65', 'D6']
Cypher text after round 7 :
['0C', '90', 'BA', '59'] ['3E', 'A2', '78', 'C7'] ['AE', '10', '9A', 'FA'] ['14', 'DE', 'D5', 'D5']
Cypher text after round 8 :
['A8', 'E4', '08', 'DB'] ['25', 'D4', '3F', 'A0'] ['8B', 'CC', 'A5', '6D'] ['B1', '76', '2D', 'AE']
Cypher text after round 9 :
['3A', '86', 'C2', '07'] ['4E', 'AA', '71', 'C8'] ['02', '3D', '03', '6C'] ['7A', 'BF', '11', 'BA']
Cypher text after round 10 :
['10', '03', '19', '13'] ['16', '1E', '02', '0C'] ['0A', '18', '0D', '1A'] ['19', '09', '0D', '09']
Cipher text after final permutation round (adding original key) :
['61', '62', '63', '64'] ['65', '66', '67', '68'] ['69', '6A', '6B', '6C'] ['6D', '6E', '6F', '70']
Full deciphered (Hex) message:  61626364656666768696A6B6C6D6E6F70

Finally Cypher to plain text (Readable):  abcdefghijklmnop
```

Sample Run 2

```
Input Plaintext:My name is Sehaj
Input 16 byte key for encrypting the plaintext:&DheerajTeammate



plaintext in blocks of bytes:
 [[['4D', '79', '20', '6E'], ['61', '6D', '65', '20'], ['69', '73', '20', '53'], ['65', '68', '61', '6A']]]

key in blocks of bytes:
 [['26', '44', '68', '65'], ['65', '72', '61', '6A'], ['54', '65', '61', '6D'], ['6D', '61', '74', '65']]
Keys Generation process initiating...
11 roundkeys are:
 [['26', '44', '68', '65'], ['65', '72', '61', '6A'], ['54', '65', '61', '6D'], ['6D', '61', '74', '65']]
[['C8', 'D6', '25', '59'], ['AD', 'A4', '44', '33'], ['F9', 'C1', '25', '5E'], ['94', 'A0', '51', '3B']]
[['2A', '07', 'C7', '7B'], ['87', 'A3', '83', '48'], ['7E', '62', 'A6', '16'], ['EA', 'C2', 'F7', '2D']]
[['0B', '6F', '1F', 'FC'], ['8C', 'CC', '9C', 'B4'], ['F2', 'AE', '3A', 'A2'], ['18', '6C', 'CD', '8F']]
[['53', 'D2', '6C', '51'], ['DF', '1E', 'F0', 'E5'], ['2D', 'B0', 'CA', '47'], ['35', 'DC', '07', 'C8']]
[['C5', '17', '84', 'C7'], ['1A', '09', '74', '22'], ['37', 'B9', 'BE', '65'], ['02', '65', 'B9', 'AD']]
[['A8', '41', '11', 'B0'], ['B2', '48', '65', '92'], ['85', 'F1', 'DB', 'F7'], ['87', '94', '62', '5A']]
[['CA', 'EB', 'AF', 'A7'], ['78', 'A3', 'CA', '35'], ['FD', '52', '11', 'C2'], ['7A', 'C6', '73', '98']]
[['FE', '64', 'E9', '7D'], ['86', 'C7', '23', '48'], ['7B', '95', '32', '8A'], ['01', '53', '41', '12']]
[['08', 'E7', '20', '01'], ['8E', '20', '03', '49'], ['F5', 'B5', '31', 'C3'], ['F4', 'E6', '70', 'D1']]
[['B0', 'B6', '1E', 'BE'], ['3E', '96', '1D', 'F7'], ['CB', '23', '2C', '34'], ['3F', 'C5', '5C', 'E5']]

Key generation completed.
```

```
starting encryption
plain text before initial permutation of encryption:
['4D', '79', '20', '6E'] ['61', '6D', '65', '20'] ['69', '73', '20', '53'] ['65', '68', '61', '6A']
Plain text after initial permutation of encryption:
['6B', '3D', '48', '0B'] ['04', '1F', '04', '4A'] ['3D', '16', '41', '3E'] ['08', '09', '15', '0F']
Plain text after round 1 :
['98', 'DA', '1D', '77'] ['E9', '18', '3E', '76'] ['30', 'C4', 'C6', 'D3'] ['DD', '61', '74', 'C1']
Plain text after round 2 :
['86', 'BF', 'D7', '58'] ['F8', 'DD', 'BA', '15'] ['C0', '6C', '56', '21'] ['5E', '06', 'B4', '5C']
Plain text after round 3 :
['20', '30', '3D', 'D4'] ['19', 'CB', '32', '7E'] ['7B', '81', '18', 'A4'] ['B9', 'DE', '72', '7A']
Plain text after round 4 :
['70', '6D', 'F0', '8E'] ['70', '5A', '70', '5E'] ['9C', '31', 'B6', 'E3'] ['FF', 'AE', 'C8', '87']
Plain text after round 5 :
['E7', 'E4', 'CE', 'EA'] ['1B', 'F7', '02', 'CC'] ['73', '63', '6F', 'C4'] ['2A', 'E9', '02', 'D8']
Plain text after round 6 :
['EA', '87', '05', '15'] ['11', '14', '4D', 'E1'] ['62', '8F', '9A', '7E'] ['86', '26', '24', '48']
Plain text after round 7 :
['20', '02', '4F', 'D3'] ['9D', 'C4', 'BC', '5F'] ['23', '48', '89', '50'] ['DB', '61', 'F3', '5D']
Plain text after round 8 :
['44', '55', 'C3', '9C'] ['A7', '4C', '9F', '39'] ['56', '2E', 'A2', '0E'] ['C7', 'F8', 'B0', '76']
Plain text after round 9 :
['47', 'D8', '2E', '4F'] ['5C', 'F2', 'C2', 'DC'] ['73', 'E6', 'AB', '40'] ['0C', '1E', '01', 'EA']
Plaintext after round 10 (special) :
['10', '3F', '7C', '39'] ['74', '18', '61', '73'] ['44', '51', '1D', 'B2'] ['C1', 'A4', '79', 'EC']
The final cyphertext is:  103F7C397418617344511DB2C1A479EC
```

```
Decrypting the cypher text:
Cipher text before first (special) round of decryption:
['10', '3F', '7C', '39'] ['74', '18', '61', '73'] ['44', '51', '1D', 'B2'] ['C1', 'A4', '79', 'EC']
Cipher text after first round of decryption:
['47', 'D8', '2E', '4F'] ['5C', 'F2', 'C2', 'DC'] ['73', 'E6', 'AB', '40'] ['0C', '1E', '01', 'EA']
Cypher text after round 2 :
['44', '55', 'C3', '9C'] ['A7', '4C', '9F', '39'] ['56', '2E', 'A2', '0E'] ['C7', 'F8', 'B0', '76']
Cypher text after round 3 :
['20', '02', '4F', 'D3'] ['9D', 'C4', 'BC', '5F'] ['23', '48', '89', '50'] ['DB', '61', 'F3', '5D']
Cypher text after round 4 :
['EA', '87', '05', '15'] ['11', '14', '4D', 'E1'] ['62', '8F', '9A', '7E'] ['86', '26', '24', '48']
Cypher text after round 5 :
['E7', 'E4', 'CE', 'EA'] ['1B', 'F7', '02', 'CC'] ['73', '63', '6F', 'C4'] ['2A', 'E9', '02', 'D8']
Cypher text after round 6 :
['70', '6D', 'F0', '8E'] ['70', '5A', '70', '5E'] ['9C', '31', 'B6', 'E3'] ['FF', 'AE', 'C8', '87']
Cypher text after round 7 :
['20', '30', '3D', 'D4'] ['19', 'CB', '32', '7E'] ['7B', '81', '18', 'A4'] ['B9', 'DE', '72', '7A']
Cypher text after round 8 :
['86', 'BF', 'D7', '58'] ['F8', 'DD', 'BA', '15'] ['C0', '6C', '56', '21'] ['5E', '06', 'B4', '5C']
Cypher text after round 9 :
['98', 'DA', '1D', '77'] ['E9', '18', '3E', '76'] ['30', 'C4', 'C6', 'D3'] ['DD', '61', '74', 'C1']
Cypher text after round 10 :
['6B', '3D', '48', '0B'] ['04', '1F', '04', '4A'] ['3D', '16', '41', '3E'] ['08', '09', '15', '0F']
Cipher text after final permutation round (adding original key) :
['4D', '79', '20', '6E'] ['61', '6D', '65', '20'] ['69', '73', '20', '53'] ['65', '68', '61', '6A']
Full deciphered (Hex) message:  4D79206E616D65206973205365686 16A

Finally Cypher to plain text (Readable):  My name is Sehaj
```