Network Security Assignment-1
AES Encryption Algorithm

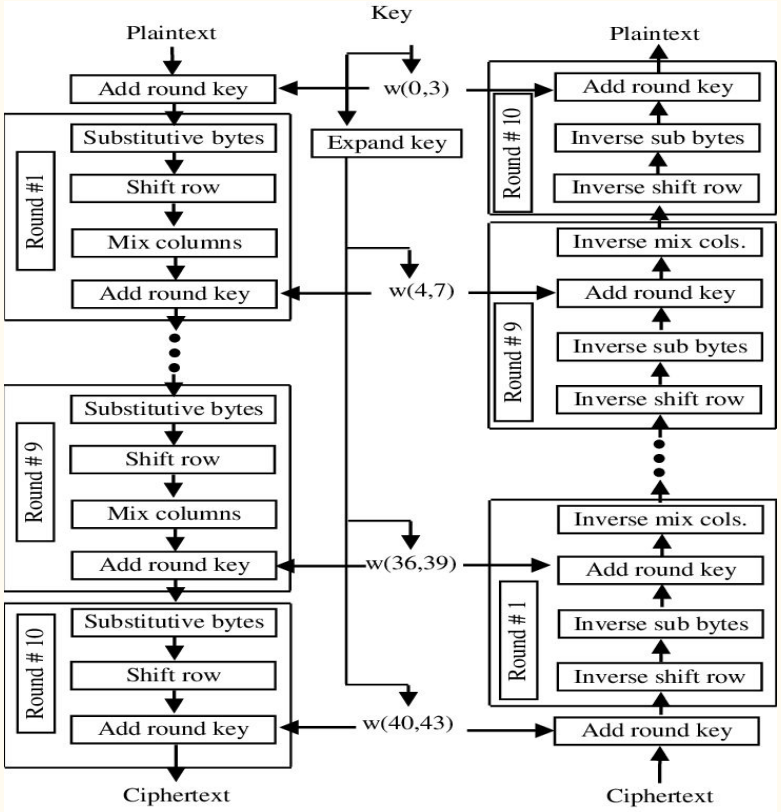
Apoorv Singh(2017027), Rohan Dev Verma(2017088)

About AES

The Advanced Encryption Standard, or AES, is a **symmetric block cipher** chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

The features of AES are as follows-:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java



Implementation Details

- The AES encryption algorithm consists of 10 rounds and is implemented in C++.

- RandomGenerator.py randomly generates the key and the plaintext. Both the key and the plaintext are in the form of 128 bit binary strings. This is stored in the file plaintext.txt

- For multiplication in GF(2^3), we used multiplication tables from a GitHub repository. Link: https://github.com/ceceww/aes

- For matrix multiplication in Shift-Column operation, we used standard simplified formulas. Link: https://en.wikipedia.org/wiki/Rijndael_MixColumns.

Results

- The decrypted ciphertext obtained by applying the encryption algorithm to the plaintext is the same as the input plaintext.

- The text obtained after a round of encryption is the same after the corresponding round of decryption, i.e., text after round 5 of encryption, for instance, is the same as text after round 4 of decryption.

- A small change in plaintext leads to a completely different ciphertext(Avalanche effect).

Observations

```
Key: 3566bbdf 42826d 864ea56d 582d09a
Original Plaintext: 9533e1b1 ee1f471e ac7d3c8 183fdc70
```

```
Key in encryption round 0: 3566bbdf 42826d 864ea56d 582d09a
Cipher after round 0: a0555a6e ea374573 8c8976a5 1dbdcea

Key in encryption round 1: 27163b4 233e1d9 a570a4b4 a0f2742e
Cipher after round 1: f6169b38 a56a7c37 d2b657d9 841fa47

Key in encryption round 2: ac843254 8fba338d 2aca9739 8a38e317
Cipher after round 2: d58f3f90 7b5028ea 5121c3ba d8ec84cb

Key in encryption round 3: af95c22a 202ff1a7 ae5669e 80dd8589
Cipher after round 3: 6d5def6c 416e33a6 8ab158 17f2f89e

Key in encryption round 4: 66265e7 462d9440 4cc8f2de cc157757
Cipher after round 4: d3942356 ecf975d 57af8290 4a49e87

Key in encryption round 5: 2ff73eac 69daaaec 25125832 e972f65
Cipher after round 5: 8548b31d 4fe1f83e b419a05a 9da1ea23

Key in encryption round 6: cae273b2 a338d95e 862a816c 6f2dae9
Cipher after round 6: 2a83ad44 f4396bc9 ec629c0 daaaf99f

Key in encryption round 7: 526721a f13eab44 77142a28 18398421
Cipher after round 7: cbe8a234 d159a485 9d856056 5c961424

Key in encryption round 8: c0598fb7 316724f3 4673edb 5e4a8afa
Cipher after round 8: 5e96bae1 d614aec fccf16a6 844718f

Key in encryption round 9: d27a2ef 3c40861c 7a3388c7 247923d
Cipher after round 9: a30e49 88e43063 c01122df c35816d2

Key in encryption round 10: 8d5085d9 b1103c5 cb238b2 ef5a893f
Cipher after round 10: 8739166c 759244fe 714920f9 c1398da1
```

```
Key in decryption round 0: 8d5085d9 b1103c5 cb238b2 ef5a893f
Decrypted text after round 0: a30e49 88e43063 c01122df c35816d2

Key in decryption round 1: d27a2ef 3c40861c 7a3388c7 247923d
Decrypted text after round 1: 5e96bae1 d614aec fccf16a6 844718f

Key in decryption round 2: c0598fb7 316724f3 4673edb 5e4a8afa
Decrypted text after round 2: cbe8a234 d159a485 9d856056 5c961424

Key in decryption round 3: 526721a f13eab44 77142a28 18398421
Decrypted text after round 3: 2a83ad44 f4396bc9 ec629c0 daaaf99f

Key in decryption round 4: cae273b2 a338d95e 862a816c 6f2dae9
Decrypted text after round 4: 8548b31d 4fe1f83e b419a05a 9da1ea23

Key in decryption round 5: 2ff73eac 69daaaec 25125832 e972f65
Decrypted text after round 5: d3942356 ecf975d 57af8290 4a49e87

Key in decryption round 6: 66265e7 462d9440 4cc8f2de cc157757
Decrypted text after round 6: 6d5def6c 416e33a6 8ab158 17f2f89e

Key in decryption round 7: af95c22a 202ff1a7 ae5669e 80dd8589
Decrypted text after round 7: d58f3f90 7b5028ea 5121c3ba d8ec84cb

Key in decryption round 8: ac843254 8fba338d 2aca9739 8a38e317
Decrypted text after round 8: f6169b38 a56a7c37 d2b657d9 841fa47

Key in decryption round 9: 27163b4 233e1d9 a570a4b4 a0f2742e
Decrypted text after round 9: a0555a6e ea374573 8c8976a5 1dbdcea

Key in decryption round 10: 3566bbdf 42826d 864ea56d 582d09a
Decrypted text after round 10: 9533e1b1 ee1f471e ac7d3c8 183fdc70
```

Avalanche effect (ONLY THE LAST BIT OF PLAINTEXT IS CHANGED)

```
Key: 769c2c9 bb2675b f499c24f 134195b8
Original Plaintext: 5d39a29a 33577a93 bbf49be 1fa18448
```

```
Key in encryption round 0: 769c2c9 bb2675b f499c24f 134195b8
Cipher after round 0: 2ba5a053 88717dc8 ff268bf1 ce011f0

Key in encryption round 1: f4b66eb4 4f9069ef bb9aba0 a8483e18
Cipher after round 1: 42d1c921 b1d169c a715a450 1b1dba1

Key in encryption round 2: a44c376 eb94aa99 509d139 f8d53f21
Cipher after round 2: c5bd1511 cfc34edb 4fbb999b 5545b2aa

Key in encryption round 3: a3713e37 48e594ae 18789597 e0adaab6
Cipher after round 3: c4e9e45 d77b7e9 59721d5e b6c04ed4

Key in encryption round 4: 3edd70d6 7638e478 6e4071ef 8eeddb59
Cipher after round 4: 893cc6e7 eba946d9 23e73424 69e24755

Key in encryption round 5: 7b64bbcf d5c5fb7 631c2e58 edf1f51
Cipher after round 5: a4aae015 57e9de90 1de3bc74 4e1d9cc

Key in encryption round 6: fa82c79a f7de982d 94c2b675 79334374
Cipher after round 6: 641387ac 2afd3b62 b16dcf7 47ea578b

Key in encryption round 7: 7998552c 8e46cd1 1a847b74 63b7380
Cipher after round 7: b4cba4d d1a7a6b becaffe8 98156ef5

Key in encryption round 8: 509f36d7 ded9fbd6 c45d80a2 a7eab8a2
Cipher after round 8: 4576fac6 4256aaa2 7097388b f6a0993d

Key in encryption round 9: ccf3c8b 122af75d d67777ff 719dcf5d
Cipher after round 9: f8cab4c1 9390533c 58b0d2b5 2c7db175

Key in encryption round 10: a4794028 b653b775 6024c08a 11b9fd7
Cipher after round 10: e519f5b5 6ab47fd adb4d61 60cde22
```

```
Key: 769c2c9 bb2675b f499c24f 134195b8
Original Plaintext: 5d39a29a 33577a93 bbf49be 1fa18449
```

```
Key in encryption round 0: 769c2c9 bb2675b f499c24f 134195b8
Cipher after round 0: 2ba5a053 88717dc8 ff268bf1 ce011f1

Key in encryption round 1: f4b66eb4 4f9069ef bb9aba0 a8483e18
Cipher after round 1: 6ffcbe7b b1d169c a715a450 1b1dba1

Key in encryption round 2: a44c376 eb94aa99 509d139 f8d53f21
Cipher after round 2: d6399186 131f3178 3c2e7fe8 dc423c24

Key in encryption round 3: a3713e37 48e594ae 18789597 e0adaab6
Cipher after round 3: eb47ed48 4e98d97b 9cef947f 9dc61ddf

Key in encryption round 4: 3edd70d6 7638e478 6e4071ef 8eeddb59
Cipher after round 4: 814022b5 a417b1d6 7a33d235 2e652291

Key in encryption round 5: 7b64bbcf d5c5fb7 631c2e58 edf1f51
Cipher after round 5: 5cd6ae87 87f38c8d 7e4854 ca7e7a4

Key in encryption round 6: fa82c79a f7de982d 94c2b675 79334374
Cipher after round 6: a7396e4c 5786775c 84cab4e0 6ee485

Key in encryption round 7: 7998552c 8e46cd1 1a847b74 63b7380
Cipher after round 7: 1757ee34 7fd16638 97bf7b6 9f198c8f

Key in encryption round 8: 509f36d7 ded9fbd6 c45d80a2 a7eab8a2
Cipher after round 8: f2d8bd6c 7efde8ce 8e90c53 9a9c8c20

Key in encryption round 9: ccf3c8b 122af75d d67777ff 719dcf5d
Cipher after round 9: 707cf4d4 7be55cf7 6cccc27d cfbc17b5

Key in encryption round 10: a4794028 b653b775 6024c08a 11b9fd7
Cipher after round 10: f5a065fd 9718473d 30417fe2 9ba94528
```

THANK YOU

Apoorv Singh 2017027

Rohan Dev Verma 2017088