EX-4-ADVANCED-ENCRYPTION-STANDARD-DES-ALGORITHM

Aim:

To use Advanced Encryption Standard (AES) Algorithm for a practical application like URL Encryption.

ALGORITHM:

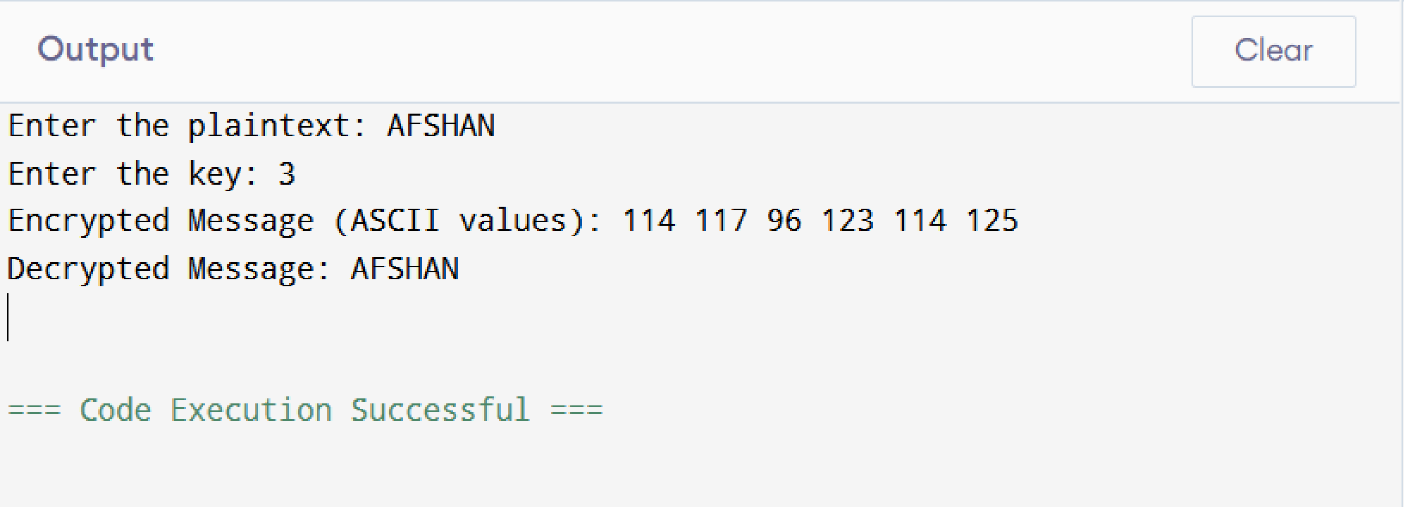
1. AES is based on a design principle known as a substitution–permutation.
2. AES does not use a Feistel network like DES, it uses variant of Rijndael.
3. It has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
4. AES operates on a 4 × 4 column-major order array of bytes, termed the state

PROGRAM:

```
Developed By: Muhammad Afshan A
Ref No.: 212223100035
```

```
#include <stdio.h>
#include <string.h>

void simpleAESEncrypt(char *plaintext, char *key, char *ciphertext) {
    int i;
    for (i = 0; i < strlen(plaintext); i++) {
        ciphertext[i] = plaintext[i] ^ key[i % strlen(key)];
    }
    ciphertext[i] = '\0';
}

void simpleAESDecrypt(char *ciphertext, char *key, char *decryptedText) {
    int i;
    for (i = 0; i < strlen(ciphertext); i++) {
        decryptedText[i] = ciphertext[i] ^ key[i % strlen(key)];
    }
    decryptedText[i] = '\0';
}

void printASCII(char *ciphertext) {
    printf("Encrypted Message (ASCII values): ");
    for (int i = 0; i < strlen(ciphertext); i++) {
        printf("%d ", (unsigned char)ciphertext[i]);
    }
    printf("\n");
}

int main() {
    char plaintext[100], key[100], ciphertext[100], decryptedText[100];

    printf("Enter the plaintext: ");
    scanf("%s", plaintext);

    printf("Enter the key: ");
    scanf("%s", key);

    simpleAESEncrypt(plaintext, key, ciphertext);
    printASCII(ciphertext);

    simpleAESDecrypt(ciphertext, key, decryptedText);
    printf("Decrypted Message: %s\n", decryptedText);

    return 0;
}
```

OUTPUT:



```
Enter the plaintext: AFSHAN
Enter the key: 3
Encrypted Message (ASCII values): 114 117 96 123 114 125
Decrypted Message: AFSHAN


=== Code Execution Successful ===
```

RESULT:

Hence,to use Advanced Encryption Standard (AES) Algorithm for a practical application like URL Encryption is done successfully.