VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

B.Tech. Winter Semester 2024-25

School Of Computer Science and Engineering (SCOPE)

Digital Assignment - V

Cryptography and Network Security Lab

Apurva Mishra: 22BCE2791

Date: 23 February, 2025

Contents

1 RC4

1.1 Code

Code 0: main.c

```c
#include <stdint.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define N 256

void swap(uint8_t *a, uint8_t *b) {
  int tmp = *a;
  *a = *b;
  *b = tmp;
}

void initialization(char *key, uint8_t *S, uint8_t *T) {
  int len = strlen(key);
  int j = 0;
  for (int i = 0; i < N; i++) {
    S[i] = i;
    T[i] = key[i % len];
  }
}

void permutation(char *key, uint8_t *S, uint8_t *T) {

  int j = 0;
  int len = strlen(key);

  for (int i = 0; i < N; i++) {
    j = (j + S[i] + T[i]) % N;

    swap(&S[i], &S[j]);
  }
}

void stream_generation(uint8_t *S, char *plaintext, uint8_t *ciphertext) {

  int i = 0;
  int j = 0;

  for (size_t n = 0, len = strlen(plaintext); n < len; n++) {
    i = (i + 1) % N;
    j = (j + S[i]) % N;

    swap(&S[i], &S[j]);
    int t = (S[i] + S[j]) % N;
    int k = S[t];

```

```c
    ciphertext[n] = k ^ plaintext[n];
  }

}

void RC4(char *key, char *plaintext, uint8_t *ciphertext) {

  uint8_t S[N];
  uint8_t T[N];

  initialization(key, S, T);
  permutation(key, S, T);
  stream_generation(S, plaintext, ciphertext);

}

int main(int argc, char *argv[]) {

  if (argc < 3) {
    printf("Usage: %s <key> <plaintext>", argv[0]);
    return -1;
  }

  uint8_t *ciphertext = malloc(sizeof(int) * strlen(argv[2]));

  RC4(argv[1], argv[2], ciphertext);

  for (size_t i = 0, len = strlen(argv[2]); i < len; i++)
    printf("%X", ciphertext[i]);

  return 0;
}
```

1.2 Output

```
da/ass5/q1 via C v16.0.0-clang
❯ cc main.c -o main

da/ass5/q1 via C v16.0.0-clang
❯ ./main "Secret" "Hello, world!"
4CB176953845B2E2E05C4ECD

da/ass5/q1 via C v16.0.0-clang
❯
```