Tristan Erney

November 3rd, 2021

Intro to Cryptology

Hands On Exercise 10

1)

Xn+5 = C0Xn + C1Xn+1 + C2Xn+2 + C3Xn+3 + C4Xn+4

n = 1; X6 = C0 \* 0 + C1 \* 1 + C2 \* 0 + C3 \* 0 + C4 \* 0 = 0 = C1

n = 2; X7 = C0 \* 1 + C1 \* 0 + C2 \* 0 + C3 \* 0 + C4 \* 0 = 1 = C0

n = 3; X8 = C0 \* 0 + C1 \* 0 + C2 \* 0 + C3 \* 0 + C4 \* 1 = 0 = C4

n = 4; X9 = C0 \* 0 + C1 \* 0 + C2 \* 0 + C3 \* 1 + C4 \* 0 = 0 = C3

n = 5; X10  = C0 \* 0 + C1 \* 0 + C2 \* 1 + C3 \* 0 + C4 \* 0 = 1 = C2

n = 6; X11 = X6 + X8 = 0

n = 7; X12 = X7 + X9  = 1

n = 8; X13 = X8 + X10 = 1

n = 9; X14 = X9 + X11 = 0

Next 4 in the sequence is 0110

2)

Xn+2 = C0Xn + C1Xn+1 + 2 (mod 5)

n = 1; X3 = C0X1 + C1X2 + 2 = 1 => C0(0) + C1(1) + 2 = 1 => C1 = -1 = 4 (mod 5)

n = 2; X4 = C0X2 + C2X3 + 2 = 0 => C0(1) + C1(1) + 2 = 0 => C0 + 4 + 2 = 0 =>

C0 = -6 = 4 (mod 5)

C0 = 4, C1 = 4

Xn+2 = 4Xn + 4Xn+1 + 2 (mod 5)

3)

K :: 1, 2

P :: Hi

Generating Stream...

S[0] :: 0; T[0] = K[0 % 2] :: 1

S[1] :: 1; T[1] = K[1 % 2] :: 2

S[2] :: 2; T[2] = K[2 % 2] :: 1

S[3] :: 3; T[3] = K[3 % 2] :: 2

Stream :: [ 0 3 2 1 ]

C :: Hj

Generating Stream...

S[0] :: 0; T[0] = K[0 % 2] :: 1

S[1] :: 1; T[1] = K[1 % 2] :: 2

S[2] :: 2; T[2] = K[2 % 2] :: 1

S[3] :: 3; T[3] = K[3 % 2] :: 2

Stream :: [ 0 3 2 1 ]

P` :: Hi

rc4.cpp

#include <iostream>

#include <stdlib.h>

#include <stdint.h>

#include <string.h>

#define swap(a, b) \

{ \

uint8\_t tmp = a; \

a = b; \

b = tmp; \

}

char\* rc4(const char\* P, char\* K, size\_t s) {

char\* C = (char\*)malloc(strlen(P));

uint8\_t\* S = (uint8\_t\*)malloc(sizeof(uint8\_t) \* s),

\* T = (uint8\_t\*)malloc(sizeof(uint8\_t) \* s);

std::cout << "Generating Stream...\n";

size\_t i, j;

for (i = 0; i < s; i += 1) {

S[i] = i;

T[i] = K[i % strlen(K)];

std::cout << "\tS[" << i << "] :: " << (int)S[i] << "; T[" << i << "] = K[" << i << " % " << strlen(K) << "] :: " << (int)T[i] << "\n";

}

for (i = 0; i < s; i += 1) {

j = (j + S[i] + T[i]) % s;

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

}

std::cout << "Stream :: [ ";

for (int i = 0; i < (int)s; i += 1) {

std::cout << (int)S[i] << " ";

}

std::cout << "]\n\n";

i = j = 0;

for (int x = 0; x < (int)strlen(P); x += 1) {

i = (i + 1) % s;

j = (j + S[i]) % s;

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

int t = (S[i] + S[j]) % s;

int k = S[t];

C[x] = P[x] ^ k;

}

return C;

}

int main() {

char K[2] = {1, 2};

std::cout << "K :: " << (int)K[0] << ", " << (int)K[1] << "\n";

const char\* P = "Hi";

std::cout << "P :: " << P << "\n";

char\* C = rc4(P, K, 4);

std::cout << "C :: " << C << "\n";

char\* P\_ = rc4(C, K, 4);

std::cout << "P` :: " << P\_ << "\n";

return 0;

}