Vysoké učení technické v Brně
Fakulta informačních technologií

Kryptografie – 1. projekt

Dokumentace

13. duben 2018

Ján Jusko (xjusko00)

1 Úvod

Tento dokument popisuje riešenie prvého projektu v predmete Kryptografie (KRY). Jeho cieľom bolo zoznámiť sa s problematikou šifrovania a následne rozlúštiť pripravené textové súbory bez akejkoľvek pomoci alebo znalosti kľúča alebo algoritmu. Ďalej sa požadovalo vytvorenie implementácie programu ktorý získa počiatočný kľúč.

2 Vstupy & Výstupy

Vytvorený program na dešifrovanie pracuje so zložkou */in* v ktorej sú umiestnené súbory *bis.txt* a *bis.txt.enc*. Po spustení program *solution.py* vypíše na štandardný textový výstup počiatočný kľúč (resp. tajomstvo). V tomto prípade **KRY{xjusko00-170f4a4491f71e1}**.

3 Riešenie

3.1 Ručné riešenie

Názvy vstupných súborov *bis.txt* a *bis.txt.enc* napovedajú, že ide o ekvivalentný plaintext a zašifrovaný plaintext (ciphertext). Provedením operácie XOR nad obsahom týchto dvoch súborov dostávame *keystream* istej prúdovej synchronnej šifry. Krátkym experimentovaním zisťujem že ďalšou operáciou XOR nad získaným keystreamom a súborom *super_cipher.py.enc* dešifrujem obsah tohto súboru a získavam časť zdrojového kódu šifrovacieho algoritmu:

```
#!/usr/bin/env python3

import argparse
import sys

parser = argparse.ArgumentParser()
parser.add_argument("key")
args = parser.parse_args()

SUB = [0, 1, 1, 0, 1, 0, 1, 0]
N_B = 32
N = 8 * N_B

# Next keystream
def step(x):
  x = (x & 1) << N+1 | x << 1 | x >> N-1
  y = 0
  for i in range(N):
    y |= SUB[(x >> i) & 7] << i
  return y

# Keystream init
keystr = int.from_bytes(args.key.encode(),'little')
for i in range(N//2):
  keystr = step(keystr)

# Encrypt/decrypt stdin2stdout
plaintext = sys.stdin.buf
```

Program *solution.py* implementuje reverzný algoritmus k šifrovaciemu algoritmu objaveného v *super_cipher.py.enc*. Ukončením dešifrovacieho cyklu dostávame inicializačný kľúč, ktorým bol vytvorený *keystream*.

3.2 Riešenie SAT

Riešenie pomocou SAT solvera nebolo implementované.

4 Záver

Projekt bol vypracovaný v jazyku Python3. Testovaný na referenčnom stroji *merlin*. Riešenie úspešne splnilo časť zadania - a to ručné riešenie.