TKK DN2

Janez Justin, 63180016

April 8, 2021

1 Geffejev generator

Reševal sem nalogo pod opombo 1, torej s poznanim začetkom kriptograma.

1.1 Podatki

Niz bitov predstavim kot seznam, ki vsebuje 0 in 1. Začetni ključ (in tekoče zaporedje zadnjih m rezultatov registra) predstavim, kot seznam dolžine m, če je register predstavljen s polinomom dolžine m. Polinome sem vgradil kar v funkcije, ki predstavljajo posamezen register.

1.2 Registra 1 in 3

Izkorstim dejstvo, da se $\frac{3}{4}$ izhodov registra 1 ali 3 ponovi v izhodu generatorja. Naj bodo:

- s poznan začetek besedila dolžine n oz. $5n$ poznanih bitov
- c_s prvih $5n$ bitov kripograma
- $d = s \oplus c_s$

Potem se mora izhod registra 1 in 3 z d ujemati v približno $\frac{3n}{4}$ bitih. Pretečem vse ključe in gledam pri katerem ključu je najboljše ujemanje. Najboljši ujemanji predstavim kot ključa registra 1 in 3.
Kasneje se je izkazalo, da ta pristop ni "primeren". Program namreč najde ključ 3. registra, ki od pričakovanega ujemanja odstopa za samo 1, pravi ključ pa odstopa za 2. Zato sem namesto zgolj "optimalnega" ključa vrnil seznam potencialnih ključev(ki od pričakovanega neujemanja odstopajo za manj kot neko konstanto), ki jih potem vse pregledam za iskanje ključa 2.

1.3 Register 2

V funkciji za iskanje ključa registra 2 gledam pri katerem ključu se bo v kombinaciji z že najdenima ključoma 1 in 3 generiralo zaporednje enako d-ju. S takim ključom lahko dekriptiram dani kriptogram v besedilo.
Ključa 1 in 3 sta lahko katerakoli kombinacija ključev najdenih v prejšnji točki.

1.4 Rezultat

Priloženi kriptogram se prevede v:
**CRYPTOGRAPHYPRIORTOTHEMODERNAGEWASEFFECTI
VELYSYNONYMOUSWITHENCRYPTIONTHECONVERSIONO
FINFORMATIONFROMAREADABLESTATETOAPPARENTNO
NSENSETHEORIGINATOROFANENCRYPTEDMESSAGEALIC
ESHAREDTHEDECODINGTECHNIQUENEEDEDTORECOVER
THEORIGINALINFORMATIONONLYWITHINTENDEDRECIP
IENTSBOBTHEREBYPRECLUDINGUNWANTEDPERSONSEV
EFROMDOINGTHESAMETHECRYPTOGRAPHYLITERATURE
OFTENUSESALICEAFORTHESENDERBOBBFORTHEINTEND
EDRECIPIENTANDEVEEAVESDROPPERFORTHEADVERSAR
YSINCETHEDEVELOPMENTOFROTORCIPHERMACHINESIN
WORLDWARIANDTHEADVENTOFCOMPUTERSINWORLDW
ARIITHEMETHODSUSEDTOCARRYOUTCRYPTOLOGYHAVE
BECOMEINCREASINGLYCOMPLEXANDITSAPPLICATIONM
OREWIDESPREAD**
s ključi:
1: 01110
2: 1101001
3: 11110011010