TKK DN2

Janez Justin, 63180016

April 8, 2021

1 Geffejev generator

1.1 Podatki

Niz bitov predstavim kot seznam, ki vsebuje 0 in 1. Začetni ključ predstavim, kot seznam dolžine m, kjer je register predstavljen s polinomom stopnje m. Polinome sem "vgradil" kar v funkcije, ki predstavljajo posamezen register.

1.2 Registra 1 in 3

Ker se $\frac{3}{4}$ izhodov registrov ponovi v generatorju, upam na to, da se ob "najuspešnejšem" ključu generira zaporednje, ki ga prištejem kriptogramu, kar mi izpljune besedilo z najvecjim številom legalnih znakov (torej najmanj peterk bitov, ki predstavljajo števila med 26 in 32). Tako pregledam vse ključe in izbrem tistega, pri katerem dobim najmanj ilegalnih znakov.

1.3 Regsiter 2

Pretečem vse ključe in izberem tistega, s katerim lahko odkriptiram besedilo brez ilegalnih znakov.

1.4 Opombe

- Znalo bi se zgoditi, da bi moral za registra 1 in 3 shraniti nekaj najboljših ključev in pregledati njihove kombinacije.
- Pri registru 2 je možno, da bi za kakšen drug kriptogram dobili več možnih besedil. Ta problem bi bil rešljiv s kriptoanalizo teh besedil.

1.5 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