Elektronska sigurnost i špijunaža

Priručnik za samogradnju

Luka Matić

Agencija Eho
www.infoelektronika.net

ISBN-978-86-80134-41-3

Elektronska sigurnost i špijunaža

Naslov originala: A Handbook on DIY Electronic Security and Espionage
Autor i prevod: Luka Matić

Izdaje i štampa: Agencija Eho, Niš
e-mail: *redakcija@infoelektronika.net*

Tiraž: 200

Godina izdanja: 2022

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

004.3

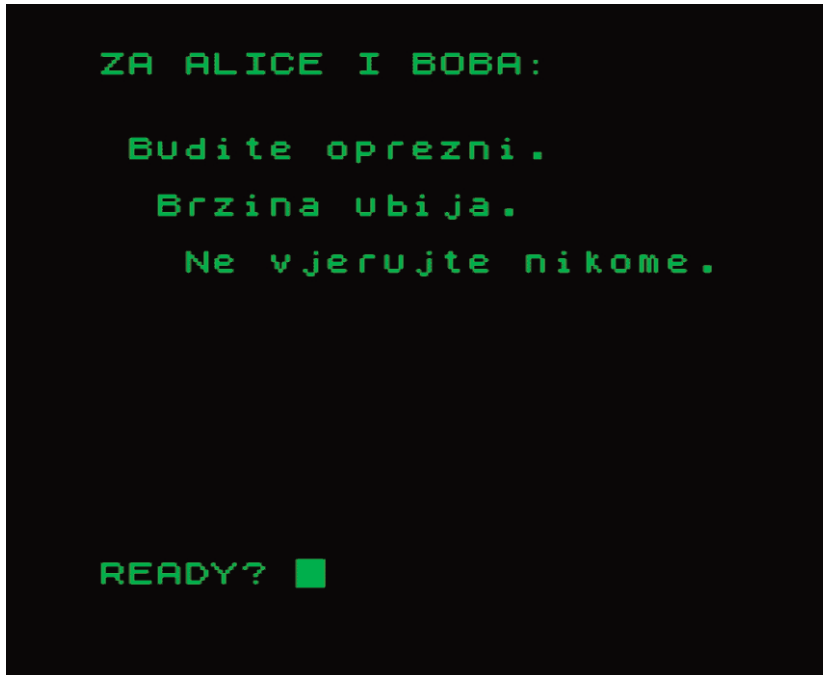
MATIĆ, Luka, 1976-
Elektronska sigurnost i špijunaža : priručnik za samogradnju / Luka Matić. - Niš : Agencija Eho, 2022 (Niš : Agencija Eho). - 235 str. : ilustr. ; 24 cm

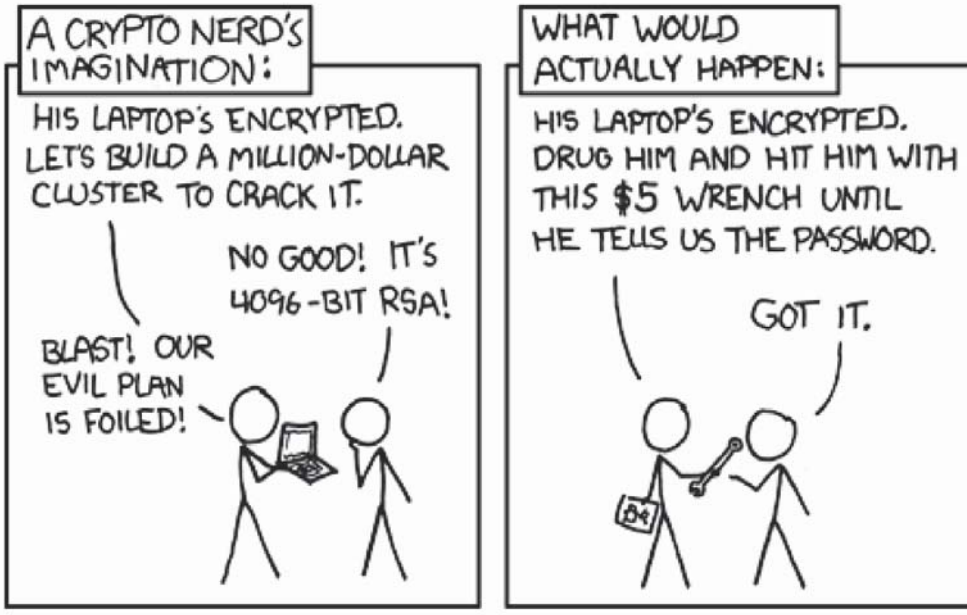
Prevod dela: A Handbook on DIY Electronic Security and Espionage. - Tiraž 200. - Napomene uz tekst. - Bibliografija.

ISBN 978-86-80134-41-3

a) Хардвер -- Сигурност

COBISS.SR-ID 74729225


ZA ALICE I BOBA:
Budite oprezni.
Brzina ubija.
Ne vjerujte nikome.
READY?



Autor se iskreno zahvaljuje XKCD-u (xkcd.com)
na dopuštenju da koristimo njihov strip 538 u ovoj knjizi.

Predgovor autora

Ako ovo čitate, to znači da je još jedan ozbiljan izdavač (Infoelektronika, nakon Elektora), odlučio objaviti ovu knjigu bez cenzure. Inzistirao sam (kod oba izdavača) na tome da se svi tekstovi koji se tiču teorije (i prakse) međunarodnih zavjera zadrže nepromijenjeni. Bez toga, ova knjiga gubi svaki smisao. Ako mislite da država, nevladine organizacije, projektanti i proizvođači vaših elektroničkih uređaja, masovni mediji, zdravstveni sustav i ostali poštuju vašu sigurnost i privatnost, i da im možete vjerovati, do sada ste već trebali odustati od daljnjeg čitanja. Zašto učiti o elektroničkoj sigurnosti i projektirati i sastavljati vlastite uređaje, kada netko drugi to može umjesto vas, a neke od njih uredno plaćate svaki put kada platite porez?

Tehnologije koje su se pokazale kao prijevare na nivou zakona fizike i mikrovalne elektronike (tzv. nevidljivi *stealth* avioni), tehnologije koje se nepotrebno i dalje „poboljšavaju" (ekrani s vertikalnom frekvencijom od 800-1000 Hz i više), tehnologije trojaniziranih čipova i kriptografija u Crnim kutijama (kojima biste trebali slijepo vjerovati), ugledne „privatne" firme u vlasništvu troslovnih agencija, operativni sustavi napravljeni kao neprikriveni špijunski alati (Windows 10) i novi PC-računalni hardver bez drivera za starije sustave, agresivno forsiranje invazije privatnosti putem IoT-a i 5G mreža, sustavno uklanjanje osjetljivih korisnih informacija s interneta (nekada davno, u mojoj mladosti, to je bio slobodan medij) i ostali apsurdi današnje „visoke tehnologije", su me svaki na svoj način inspirirali da napišem ovu knjigu.

Pametnim korištenjem low-tech pristupa možemo zaobići mnoge tipične high-tech zamke i to bi trebala biti osnovna strategija.

Otkrivanje i prepoznavanje zavjera nije nužno vezano za visoko-rizične špijunske aktivnosti (kao u slučaju Edwarda Snowdena), krađe super-tajnih dokumenata (Wikileaks) ili pristup ultra-visokoj tehnologiji. Većina zavjera nisu uopće ni pametno isplanirane, a kamoli provedene u praksi. Neke se mogu razbiti fizikom na nivou osnovne škole (npr. 9/11). Uglavnom se zasnivaju na upornom ponavljanju lažnih vijesti putem masovnih medija, i (još uvijek) pretjeranom povjerenju većine ljudi. Kritičan resurs koji većini ljudi danas nedostaje je vrijeme, a ne novac ili inteligencija. U nedostatku vremena, čovjek ne može racionalno procesirati ni osnovne logičke zaključke. Pažljivo čitanje i usporedba novih i starijih knjiga, i ostalih izvora informacija je često sasvim dovoljno, pod uvjetom da uhvatite dovoljno vremena. Profesor Stevan Dedijer, naš najpoznatiji špijun (riječ „špijun" na hrvatskom i na srpskom jeziku često automatski nosi negativne konotacije, no to mi ovdje nikako nije namjera) je zastupao tezu da se sve može saznati iz novina, ali ih treba naučiti čitati pažljivo.

Engleski original sam pisao za vrijeme tzv. Covid-krize (odnosno „plandemije") koju sam, naravno, iskoristio kao dodatnu inspiraciju. Pisanje knjige se svakako pokazalo kao puno bolja aktivnost za vrijeme kućne „izolacije", nego gledanje Netflixa ili vijesti državne televizije. Fokus masovnih medija se za vrijeme pisanja ovog prijevoda prebacio na rat u Ukrajini i rusku invaziju, tako da projekti vezani za katastrofične scenarije, jednostavnije varijante radio-komunikacijskih uređaja sličnih Telefunkenovom „FS-5000 Harpoon" sada, eto, mogu

opet postati aktualni, čak i za one koji nisu skloni učenju iz povijesti. Radio-telegraf se već odavno smatra dijelom prošlosti, ali mogao bi nažalost, vrlo lako postati i dio budućnosti.

Tu su zatim i, danas još uvijek aktivne, iako izrazito low-tech "brojčane" radio stanice (eng. *number stations*). Lako ćete ih naći na SW (kratkovalnom) području, s klasičnim analognim SW radio prijemnikom i malo boljom antenom. Možete koristiti i internetske online SDR prijemnike. Internet je pun informacija o brojčanim stanicama, tako da ćete brzo pronaći njihove RF frekvencije i raspored emitiranja, a fizičke lokacije puno teže. Iako low-tech, brojčane stanice su još uvijek najsigurniji način dalekometnog jednosmjernog (simpleksnog) prijenosa tajnih informacija, (kriptiranih Vernamovom šifrom) špijunima u stranim zemljama. **Dobro financirane troslovne agencije se još uvijek nisu odrekle ove izrazito sigurne, a jeftine low-tech tehnologije. Razmislite dobro o tome.**

U međuvremenu se, kao posljedica Covid-krize i nedostatka ukrajinskog neona pojavila i nestašica (novih i visoko-integriranih) čipova, što je još jedan, dodatni razlog razvoja low-tech strategije projektiranja sigurnosnih uređaja. Moguće rješenje za Europu bi bilo postupno obnavljanje vlastite proizvodnje čipova. Skupo, sporo i sada već teško izvedivo, protivno temeljnoj politici Europske Unije, a postoji i dodatni ozbiljni problem - prosječna starost europskog inženjera sa značajnim praktičnim, proizvodnim iskustvom u tom području danas je oko 70 godina.

Dodatni mehanizam koji koči većinu potencijalnih projektanata i korisnika low-tech kriptografskih uređaja je uporno uvjeravanje (naravno, redovito bez prihvatljivih inženjerskih argumenata), ponavljanje da ništa ne možete napraviti DIY, čak ni dobar generator stvarno slučajnih brojeva (TRNG), a kamoli uređaj za šifriranje, pogotovo jednokratnom (Vernamovom) šifrom. Jedina potencijalno neprobojna šifra, nezaobilazni alat svakog dobrog špijuna, se redovito jednostavno naziva „beskorisnom". Druga popularna varijanta takvih priča je da se zaštita svakog DIY uređaja može probiti u 5 minuta. Prvo izdanje knjige, moje članke u Elektoru i prototipove uređaja je pregledalo i recenziralo više nezavisnih stručnjaka, i nisu pronašli takve brze metode. Naravno, pod uvjetom da se precizno definirane OpSec procedure (operativna sigurnost, procedure postupanja s uređajima, kriptografskim ključevima i ostalim osjetljivim materijalima) za svaki uređaj dosljedno provode.

Moj kolega inženjer Paul Uszak, iz Birminghama (Engleska) , koji se bavi DIY generatorima slučajnih brojeva i vodi web stranicu *reallyreallyrandom.com* je zajednicu kriptografskih inženjera (u naletu inspiracije) nazvao „vrhunskim stručnjaci, ali još veći licemjeri". Uzmite to u obzir, pogotovo ako se ikada uključite u raspravu na jednom od njihovih foruma, kao što je npr. *crypto.stackexchange.com*, iz kojeg možete, bez obzira na sve, opet pokupiti gomilu korisnih informacija.

S druge strane, budite svjesni, da je elektronička sigurnost jako široko područje (špijunaža je još kompleksnija, s vrlo malom tolerancijom na pokušaje i pogreške), a svaki sigurnosni sustav je jak kao i njegova najslabija karika. Prije nego u praksi napravite bilo što ozbiljno, morat ćete steći puno šire znanje od ovoga koje može stati u knjigu od dvjestotinjak stranica.

Neki projektanti hi-tech sigurnosnih čipova (HSM- *high security module*), koji su neizbježni u sigurnosnim alatima kao što su npr. bankovne kartice i elektronički dokumenti, su pogrešno shvatili ono što sam napisao u engleskom izdanju ove knjige. Razvoj takvog hardvera (na kojem se ozbiljno radi tek zadnjih 20 godina) zahtjeva veliko znanje i iskustvo. Projektiranje hardvera (npr. kreditne kartice) koji bi trebao zadržati tajne (npr. PIN u kreditnoj kartici) u slučaju krađe kartice je izrazito teško i takvi uređaji nikako ne spadaju u kategoriju skupih hi-tech prijevara. Htio sam samo reći da treba pokušati izbjeći HSM-ove tamo gdje je to moguće. Na taj način jednostavno izbjegavamo koristiti nešto što u potpunosti ne razumijemo, za što nam nedostaju visoko-specijalizirana znanja i uređaji, potrebni za projektiranje i sastavljanje, ali i pouzdano sigurnosno testiranje takvih uređaja.

Nakon čitanja potpoglavlja 7.3, neki recenzenti (pogotovo oni s iskustvom u projektiranju HSM-ova) su počeli sumnjati u moje stručno znanje, ali i mentalno zdravlje. Tekst ima samo 10 stranica (zajedno sa slikama) i bilo mi je potrebno u prosjeku 5-10 dodatnih objašnjenja putem emaila da bih razjasnio da nitko ne očekuje od Funcarda da čuva tajne informacije (privatne ključeve) u slučaju krađe. Cijeli smisao projekta je u tome da je fizičko skrivanje Funcarda na tajnom mjestu puno pouzdanije nego vjerovanje bilo kakvom umreženom računalu (od web servera do smartfona), da nikada nikome neće razotkriti vaše privatne ključeve. Interni mikro-sklopovi Funcarda su jednostavni, dobro poznati i mala je vjerojatnost da sadrže hardverske trojance. Molim vas, obratite posebnu pažnju na tih 10 stranica.

U nastavku slijedi predgovor našeg najboljeg i najstrožeg recenzenta. Wim Ton je iskusni inženjer projektant sigurnosnih elektroničkih uređaja, koji je radio za nizozemsku NLNCSA još za vrijeme Hladnog rata. Od njega sam dobio vrlo korisne profesionalno-paranoidne (ovaj pojam će kasnije biti detaljno objašnjen) informacije, koje sam iskoristio za poboljšanje ovog dopunjenog izdanja, ali i za projektiranje mojih novih uređaja. Jedna od najbitnijih je bila slijedeća - unutar NLNCSA nisu vjerovali ni nizozemskim, a kamoli američkim proizvođačima elektroničkih uređaja - zato su za generiranje slučajnih brojeva (za kriptografiju) koristili istovremeno najmanje 3 uređaja, od 3 različita proizvođača, čije signale su miješali i kombinirali.

Ako smatrate da sam negdje pogriješio, ili da se neki uređaj/metoda može poboljšati, spreman sam prihvatiti argumentirane kritike. Možete me slobodno kontaktirati.

Autor

Predgovor recenzenta

Pojavom sve moćnijih komunikacijskih uređaja raste i potreba za informacijskom sigurnošću. U prošlosti je informacijska sigurnost i njeno zaobilaženje bila mračna umjetnost, kojom su se uglavnom bavile obavještajne organizacije. Njihovi klijenti su bili ograničeni na vojsku i diplomatske službe. Mnoge su zemlje u 17. stoljeću uspostavile te tzv. "crne kabinete". Oslanjanje današnjeg društva na obradu informacija znači da sigurnost informacija više nije od interesa samo za obavještajne organizacije, već i za kriminalce, aktiviste i mnoge druge subjekte.

Budući da sam radio u području sigurnosti, za vladinu organizaciju NLNCSA i za nekoliko proizvođača uređaja kao što su NXP i Landis + Gyr, naslov knjige mi je odmah privukao pozornost. Također sam već vidio Lukine projekte vezane za elektroničku sigurnost u časopisu Elektor i zanimalo me što on još može ponuditi. Luka je jedan od rijetkih autora koji je opisao sigurnosne uređaje koji se mogu izraditi amaterskim sredstvima.

Upozorenje za „*spoiler*": unatoč naslovu, knjiga ima vrlo malo veze sa špijunažom, osim ako se bilo kakvo zaobilaženje tajnosti i povjerljivosti ne smatra špijunažom.

Većina ljudi poznaje informacijsku sigurnost iz računalnog okruženja: lokot na web adresama, kompliciranе lozinke i autorizacija u dva faktora. Ova knjiga se bavi nekim od manje poznatih aspekata informacijske sigurnosti, uglavnom onima koji su bliski hardveru.

TEMPEST je tradicionalni način prisluškivanja monitora i komunikacijskih veza. Signali sa strmim rubovima proizvode mnogo viših harmonika koji se mogu primiti čak i na određenoj udaljenosti uz odgovarajuću opremu. To je podskup onoga što se trenutno naziva "analiza bočnog/rezidualnog kanala" (*side-channel analysis*) , gdje napadač pokušava dobiti zaštićene informacije preko nekog drugog kanala, poput potrošnje snage, vremena, zvuka, svjetlosti itd.

Remanencija podataka vas može vrlo neugodno iznenaditi ako niste oprezni. Svi ste čuli za oporavak datoteka nakon brisanja (*unerase/undelete*), čak i kada su uklonjene iz kante za smeće. RAM može sadržavati informacije i nakon isključenja napajanja. Također je predstavljena i legalna/legitimna uporaba tih procedura: izvlačenje podataka iz neispravnih (E)EPROM-ova.

U obradi Morseovog telegrafa Luka spominje radiogoniometriju (lociranje odašiljača) i „rukopis" telegrafskog operatera. Ovaj "rezidualni kanal" je lijep primjer "analize prometa" (*traffic analysis*). Često je sadržaj poruke nedostupan, jer je šifriran ili je na stranom jeziku. Analiza prometa bilježi tko govori, odakle i koliko dugo. U suvremenim raspravama o privatnosti, te informacije se nazivaju "metapodaci".

Knjiga se dotiče kriptografije. Glavni fokus je na algoritmu "jednokratne šifre" (ili OTP-„*one time pad*"), što je jedini algoritam šifriranja za koji se može dokazati da je neprobojan. Kako bi se pomoglo s inače stvarno nespretnom/problematičnom distribucijom ključeva, knjiga opisuje konstrukciju i rad kutije zaštićene od neovlaštenog otvaranja i hardverski generator slučajnih brojeva. Za one koji žele produbiti znanje o generiranju slučajnih brojeva, BSI AIS20/31 i NIST SP800-22 su obavezna dodatna literatura. Jedini drugi algoritam šifriranja kojim se knjiga bavi je RSA. Čitatelji zainteresirani za kriptografiju trebali bi pročitati npr. "Primijenjenu kriptografiju" Brucea Schneiera. Implementacija i korištenje kriptografije samo na temelju ove knjige može vas uljuljati u lažni osjećaj sigurnosti.

I hardver može biti manje siguran od očekivanog. Luka to naziva "trojaniziranim" hardverom. Njegovo rješenje koristi tehnologiju iz 1980-ih, kao što su Z80 procesori i audio kazete. Čak i bez zlonamjernih predumišljaja, sigurnosne značajke modernih procesora, poput zaštite pri pokretanju (*boot protection*) i onemogućavanja sučelja za otklanjanje pogrešaka (*debug intercafe*) nisu savršene, a proizvođači su vrlo dobri u prikrivanju ovih in-

formacija. Jedan od rijetkih javnih izvora informacija o tome je UCAM-CL-TR-630 Sergeja P. Skorobogatova iz 2005. godine! Nedavno su alati poput "Chipwhisperera" i "Chipshootera" postali lako dostupni na tržištu. Takvi napadi zahtijevaju mnogo vremena i vještine, ali projektant svakog sustava mora biti svjestan ovih ranjivosti.

Za Zilog-Z80 su dati neki savjeti za sigurno programiranje i projektiranje sustava, te primjeri napada preljevom međuspremnika (*buffer-overflow*). Ovo nije uvijek primjenjivo na moderne AVR, PIC i ARM arhitekture. Za dodatne ideje, proučite mehanizme koji se koriste u vrhunskim (*high-end*) modernim pametnim karticama.

Informacijska sigurnost nije samo povjerljivost, unatoč tome što se tome obično pridaje najviše pozornosti. S obzirom na povijest informacijske sigurnosti, to nije iznenađujuće. Sa sve većim oslanjanjem na informacijsku tehnologiju, aspekti "integriteta" (*integrity*) i "dostupnosti" (*availability*) podataka se također moraju uzeti u obzir za određene aplikacije. Neraspoloživost poslovno kritičnih sustava nanosi veliku štetu svakoj organizaciji. Zanemarivanje aspekta "dostupnosti" odmah omogućuje unosan posao za kriminalce ucjenjivače - korištenjem *ransomware* alata. Integritet je također aspekt koji zaslužuje pozornost, između ostalog, za sustave automatskog/daljinskog upravljanja i sustave nadogradnje softvera bežičnim putem(„*over-the-air*").

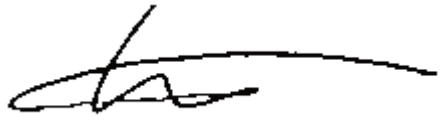
Prije primjene informacijske sigurnosti potrebno je definirati sigurnosni problem:

- Što je sve vrijedna imovina i koji aspekti svake imovine moraju biti zaštićeni?
- Protiv koje vrste napadača se imovina mora zaštititi, od znatiželjnog susjeda ili vješte obavještajne službe? Pogledajte publikacije Edwarda Snowdena o tome što možete očekivati od ovog drugog.
- Kakvo je okruženje: ima li napadač samo udaljeni ili izravan fizički pristup, može li se administratoru vjerovati?
- Zna li korisnik kako sigurno postaviti sustav i s njime sigurno rukovati i kako ga sigurno ukloniti ili uništiti?

"Security engineering" Rossa Andersona precizno opisuje takve procese. Za vrlo formalne procese, pogledajte "Common criteria".

"Elektronska sigurnost i špijunaža" je dobra polazna točka za početnike u svijetu sigurnosti. Čak i ako se ne odlučite sastaviti niti jedan od opisanih projekata, obrasci sigurnosnog razmišljanja će biti korisni za svakog čitatelja.

Wim Ton, 21.08.2022.



Sadržaj

Poglavlje 2 – Metode napada

Svaki kriptografski sustav se može napasti na mnogo različitih načina. Prvo moramo vidjeti kojim metodama napada se možemo suprotstaviti koristeći DIY metode, tako da projektiramo cijeli kripto-sustav i definiramo sigurnosne procedure koji jednostavno ne mogu biti napadnuti drugim metodama, onima protiv kojih se ne možemo boriti s DIY resursima.

2.1. Metode kojima se možemo suprotstaviti

Počet ćemo sa tehnikama kojima se možemo suprotstaviti DIY pristupom:

1.) **Matematička kriptoanaliza** je probijanje šifre korištenjem matematičkih/ statističkih proračuna da bi se postupno suzilo područje potrage i pronašao ključ.

2.) **Gruba sila (eng. *brute force*) –** slično prethodnoj metodi, ali manje sofisticirano – uzastopni pokušaji dekripcije svim mogućim ključevima, da bi se uz veliku procesorsku snagu, puno potrošene struje i vremena (i puno sreće) smisleni otvoreni tekst (možda) pojavio.

3.) **Prisluškivanje/sabotiranje/regeneriranje niza generatora slučajnih brojeva** –svaka dobra enkripcija je zasnovana na dobrim slučajnim brojevima. Ovdje Eva pokušava ukrasti/prisluškivati nizove Alisinih slučajnih brojeva, ili ih čak regenerirati, a Mallory pokušava petljati po Alisinom generatoru slučajnih brojeva (npr. podmetanjem „prežičenih" čipova u njen poštanski sandučić), ili ga ometati jakim RF signalima (eng. *jamming*) da bi on stvorio loše, odnosno predvidive nizove.

4.) **Napad prelijevanjem međuspremnika (eng. *buffer-overflow*) –** ako Alisino računalo nije pažljivo programirano/zaštićeno – odnosno ako ulazni bufferi za normalno formatirane ulazne podatke nisu dobro omeđeni/ograničeni u njegovoj memoriji, onda Mallory može ubaciti puno dulji niz podataka koji će se „preliti" – odnosno napuniti dio memorije koji je bio predviđen za npr. za stog (eng. *stack*) ili čak programski kod. Ovako Mallory može resetirati ili "zamrznuti" Alisin kompjuter, ukrasti podatke, podmetnuti i pokrenuti vlastiti kod, pa čak i preuzeti kontrolu nad Alisinim kompjuterom.

5.) **Napadi rezidualnim kanalima (eng. *side-channel attacks*) –**Eva može pratiti potrošnju struje (ili snage) Alisinog uređaja, akustičke ili električne rezidualne signale koje on emitira, mjeriti vrijeme potrebno za obradu različitih ulaznih podataka, itd… Nakon pažljive obrade prikupljenih podataka, Eva može doći do Alisinih osjetljivih tajnih informacija.

6.) **Softverski „malware"** (virusi, crvi, softverski prisluškivači, key-loggeri, trojanci, ...) - Mallory može podmetnuti različite vrste malicioznog softvera (ili „**malvera**") na Alisin kompjuter, koristeći različite metode.

7.) **Hardverski trojanci** –slično prethodnome, ali ovdje Mallory manipulira elektroničke komponente na hardverskom nivou (npr. dodavanjem mikrosklopova na silicijsku

pločicu MCU-a, koji će snimiti ili odaslati tajne informacije) koje zatim podmeće u Alisin laboratorij/radionicu.

8.) **Iskorištavanje inherentno nesigurnih fizikalnih svojstava**– ovo je slično hardverskim trojancima, ali ovdje Mallory ne petlja po Alisinoj elektronici, koja ostaje fizički netaknuta. Ako Mallory ukrade neki Alisin elektronički uređaj, Eva će pokušati izvući tajne podatke, što je moguće zbog različitih neželjenih fizikalnih efekata remanencije, inherentnih određenom tipu elektroničke tehnologije.

Neki od napada kojima se ne možemo suprotstaviti DIY pristupom su:

1.) **Bilo koji tip side-channel ili fault-injection napada protiv sigurnosnog hardvera**– napadnuti uređaj je u ovom slučaju neka vrsta *smartcard*-a (npr. kreditna kartica), sa **tamper-resistant** karakteristikama, koja čuva neku vrstu tajne (npr. privatni ključ, PIN ili tajni program) kojoj se normalno ne može pristupiti. Alice je izgubila uređaj, a Eva ga je pronašla. Eva može analizom raznih rezidualnih varijabli (npr. struje napajanja – tzv. ***„power analysis***" ili vremena potrebnog za određene operacije – tzv. „***timing attack***") otkriti tajne podatke. Ovakva analiza zahtjeva složenu matematičku/statističku obradu izmjerenih veličina. Ubacivanje neispravnih ulaznih podataka ili električnih signala izvan normalnog raspona (***„fault injection"***) može izazvati neželjenu radnju (npr. preskok naredbe za provjeru PIN-a) i opet razotkriti tajne podatke.

2.) **Sve vrste invazivnih napada** – ovdje je smart kartica opet dospjela u Evine ruke, ali ovdje će ona otvoriti čip (tzv. **dekapsulacija**[23]), da bi je onda testirala injektiranjem optičkih signala (polu-invazivni napad) ili električnih signala (invazivni napad). Tako opet može razotkriti tajne podatke.

Borba protiv ove vrste napada zahtjeva posebno projektirane sigurnosne integrirane krugove, s raznim mjerama za maskiranje rezidualnih signala i kritičnih područja memorije, fizički i električki. Moji kripto uređaji **se neće oslanjati na nikakav *tamper-proof* hardver koji štiti tajne podatke –**jednostavno zato što je razvoj i proizvodnja takvih čipova vrlo skupa i zahtjeva posebnu opremu i radne uvjete koje Alice i Bob vjerojatno nemaju. Ključevi za šifriranje će se čuvati na običnim SD karticama, papirima ili magnetofonskim trakama, a Alice i Bob će ih morati pažljivo čuvati. Sve mora biti *open-source* (hardver i softver), napravljeno s običnim komponentama za opće namjene, u skladu s prethodno definiranim DIY principima.

Kao što ćemo vidjeti, protiv mnogih napada se možemo boriti s DIY sredstvima, dok se ostali mogu učiniti neprimjenjivima, dobro definiranim projektiranjem i sigurnosnim procedurama. Sada ću detaljnije objasniti kako se možemo suprotstaviti svakoj od metoda napada, sve po DIY principima.

---

[23]**dekapsulacija –** otvaranje čipa uklanjanjem plastičnog kućišta, obično korištenjem nitratne kiseline i acetona. Cilj je otkrivanje silicijske pločice bez oštećivanja, tako da se mikrosklopovi mogu pregledati mikroskopom. Otkriveni mikrosklopovi se zatim mogu testirati ubacivanjem električnih ili optičkih signala.

Poglavlje 3 – Generatori slučajnih brojeva

3.1. Dobar RNG kao neophodna karika u lancu sigurnosti

Projektiranje dobrih kripto-sustava za Alisu i Boba moramo početi s dobrim TRNG-om. Slučajni brojevi se mogu koristiti za jednokratne šifre (OTP), za generiranje velikih prostih brojeva za RSA metodu (PGP program tako radi), za jednokratne ključeve (npr. za samo jednu vezu, odnosno sesiju – eng. *session key*) za AES metodu, za anti-TEMPEST skrembliranje monitora ili printera (miješanje vremenskog redoslijeda iscrtavanja linija na ekranu ili ispisivanja točaka na papiru) i za mnoge druge sigurnosno-kritične procese. Jednostavno ne možete ništa pouzdano šifrirati bez vrlo kvalitetnog TRNG-a. U potpoglavlju 2.2.2 smo analizirali razne metode napada na RNG koje bi mogle izvesti Eva (prisluškivanje RNG-a ili re-generiranje nizova), Mallory (petljanje po RNG-u ili ometanje) i Trudy (uplitanje u dostavu ključeva). Sada ćemo vidjeti kako se Alice i Bob mogu od toga obraniti. Oni prvo moraju naučiti testirati i ocijeniti određeni RNG, za njegovu potencijalnu primjenu u kriptografiji.

3.1.1 Definiranje zahtjeva na dobar RNG za upotrebu u kripto-sustavu

Mnogi RNG-i se mogu kupiti kao komercijalni proizvodi, ali rijetki su pouzdani za upotrebu u kriptografiji. Prvo ćemo vidjeti kako Alice može provjeriti da li je niz brojeva (dovoljno) slučajan. NIST[51] standard [16] definira niz od 15 matematičko-statističkih testova koji mogu dati dobru procjenu slučajnosti nekog niza brojeva. Ako niz brojeva ne prolazi testove, RNG je sigurno loš. Budite oprezni, jer s druge strane, ako niz brojeva prolazi testove, to još uvijek ne znači da je RNG stvarno slučajan (TRNG) i dovoljne kvalitete za upotrebu u kriptografiji!

Dobar rezultat NIST testiranja je samo početni uvjet (broj 0). Ostali su:

1.) Niz mora biti generiran stvarno slučajnim fizikalnim procesom. Svaki dobar PRNG će također proći svaki NIST test prije nego se nizovi počnu ponavljati.

2.) Sve varijable i signali moraju biti dostupni za praćenje i mjerenje. U protivnom, Alice ne može vjerovati RNG-u jer ne može provjeriti prvi uvjet. Možda ga je netko prežičio hardverskim trojancima ili je jednostavno napravljen kao Crna kutija.

3.) Projektiran tako da ga Alice može sastaviti u samogradnji, od lako dobavljivih komponenata. Specijalizirane komponente Eva može lako pratiti, pa se onda Mallory može uplesti na razne načine. Prepuštanje proizvodnje nekoj trećoj osobi znači da njoj treba apsolutno vjerovati.

51 NIST – američki institut „National Institute of Standards and Technologies“. Sličan njemačkom institutu DIN “Deutsches Institut für Normung” ili ruskom ГОСТ ”Государственный Стандарт“. Pored svih tehničkih standarda, oni također definiraju i standarde za kriptografiju.

4.) Dovoljno velika brzina izlaza, reda veličine 1 Mbit/s. Čak i brzina mjerljiva u kbit/s može biti prihvatljiva, ovisno o primjeni. Spori slučajni procesi, kao npr. bacanje igraće kocke, mogu imati dobru slučajnost, ali nisu baš praktični, s brzinom od oko 1 bit/s.

5.) RNG ne smije biti spojen s nikakvim nesigurnim elektroničkim uređajem, i naravno, ne smije biti umrežen. Ovo će spriječiti prisluškivanje i uplitanje.

6.) Instaliran u dobro oklopljenu (aluminijsku) kutiju, napajan baterijama. Ovo će spriječiti TEMPEST prisluškivanje i ometanje.

3.1.2 NIST testovi

Prema [16] je definirano sveukupno 15 testova. Detaljno i iscrpno testiranje prototipa TRNG-a u svim uvjetima rada je obavezno, da bismo utvrdili da li je prikladan za primjenu u kriptografiji.

1.) Test monobitne frekvencije

Ovo je jednostavno prebrojavanje broja nula i jedinica i usporedba. Prvo i osnovno svojstvo svakog slučajnog niza je približno jednak broj nula i jedinica.

2.) Test frekvencija unutar blokova

Isto kao i test 1, ali sada se niz od n bitova dijeli na blokove od M bitova. Prebrojavanje nula i jedinica se vrši unutar blokova, pa se zatim blokovi međusobno uspoređuju.

3.) „*Runs*“ test

Ovaj test je prebrojavanje broja „*run*“-ova u nizu od n bitova. „*Run*“ je neprekinuti niz konstantnih nula ili jedinica.

4.) Test najduljih „*run*“-ova jedinica unutar blokova

Slično testu 3, ovdje se niz od n bitova dijeli blokove od M bitova. Za svaki od blokova se prebrojava najdulji niz jedinica, čije se duljine zatim uspoređuju među blokovima.

5.) Test ranga binarne matrice

Slučajni bitovi se smještaju u binarne matrice definiranih dimenzija. Zatim se računaju rangovi tih matrica. Prenizak rang ukazuje na to da se neki redovi matrica mogu izraziti kao linearne kombinacije ostalih redova, što znači da niz nije slučajan.

6.) Test diskretnom Fourierovom transformacijom

Prvo se vrši FFT transformacija nad nizom od n bitova. Zatim se crta amplitudno-frekvencijski graf. Naglašeni „šiljci“ (lokalni maksimumi) u grafu ukazuju na lošu slučajnost niza.

7.) Test grupa bitova bez preklapanja

Različite predefinirane fiksne „riječi“ (grupe od tipično m=9 do 10 bitova) se prebrojavaju u nizu od n bitova.

8.) Test grupa bitova s preklapanjem

Isto kao test 7, ali ovdje se vrši pomak „prozora" od m bitova za samo jedan bit, dok se u testu 7 vrši pomak od m bitova.

9.) Maurerov univerzalni statistički test

Ovo je pokušaj sažimanja (komprimiranja) datoteke od n bitova (slično WinZip ili WinRar programima). Test ne prolazi ako je moguće smanjiti veličinu datoteke - što znači da je moguće izraziti neke dijelove fajla pomoću ostalih dijelova.

10.) Test linearne kompleksnosti

Zasniva se na posmičnom registru (*shifting register*), opet se pokušavaju napraviti linearne kombinacije među nizovima bitova, slično testu 5.

11.) Serijski test

Ovaj test se sastoji od računanja frekvencija pojavljivanja svih mogućih m-bitnih riječi u nizu od n bitova. To je u biti crtanje **histograma**.

12.) Test približne entropije

Kao i 11, ali sada se uzimaju u obzir dvije duljine riječi, od m i m+1 bitova.

13.) Test kumulativnih zbrojeva

Ovo je test slučajnih „šetnji" oko nulte točke, zasnovan na zbrojevima slučajnih brojeva, i stalno provjeravanje maksimalne devijacije od nule. Zbroj dugih nizova dobrih slučajnih brojeva u rasponu [-R,+R] mora uvijek ostati blizu nule.

14.) Test slučajnih devijacija

Test se izvršava slično kao i 13, ali sada se različiti iznosi devijacija ukupnog zbroja od nule uspoređuju po frekvencijama pojavljivanja (opet histogram).

15.) Test varijanci slučajnih devijacija

Slično testu 14, ali sada se ocjenjuju statističke varijance.

Ovi testovi su vrlo precizni i strogi (što je neophodno da bi se mogla garantirati sigurnost kripto-sustava). Na prvi pogled kompliciran, ali oni su u biti zasnovani na slijedećim, intuitivnim i lako razumljivim principima slučajnosti:

1.) Stvarno slučajni niz bitova ima podjednak broj nula i jedinica.

2.) Stvarno slučajni niz bitova ima podjednake frekvencije pojavljivanja različitih uzoraka grupa bitova (riječi od m bitova).

3.) Niti jedan dio niza bitova nema matematičke korelacije s drugim dijelovima tog cijeloga niza.

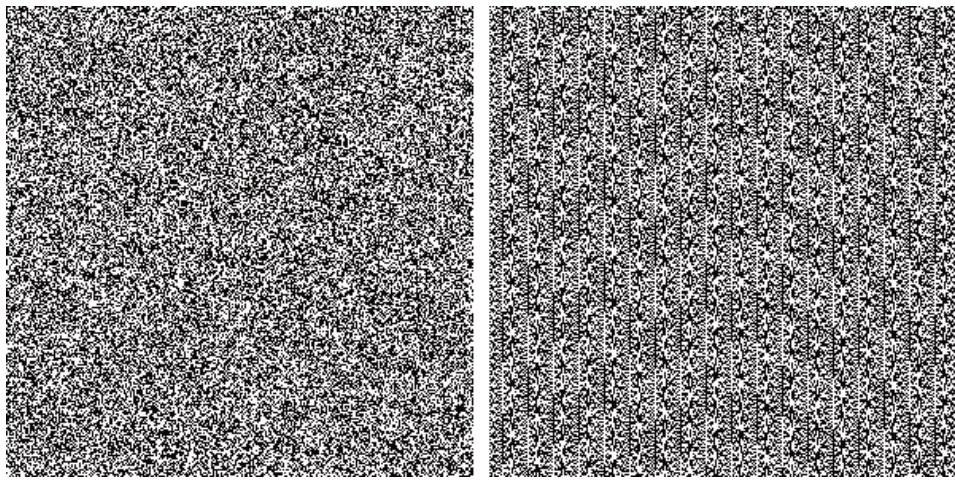
Preporučljivo je napraviti slijedeće osnovne jednostavne testove prije iscrpnog NIST testiranja, da biste dobili osnovne procjene:

1.) Generiranje histograma pomoću programa kao npr. WinHex. Prebrojavaju se sve 8-bitne riječi (od 0x00 do 0xFF, na x-osi) pa se brojevi njihovih pojavljivanja unutar fajla crtaju na y-osi. Oni moraju biti približno jednaki. Primjere možete vidjeti na [17].

2.) Pokušajte komprimirati fajl sa slučajnim brojevima, korištenjem WinZip-a ili sličnog programa. Ako je slučajnost dobra, „komprimirani" fajl mora biti veći od originala!

3.) Pokušajte simulirati Buffonov[52] problem korištenjem testiranog niza brojeva. Ako je slučajnost dobra, preciznost izračunate aproksimacije broja π se mora stalno povećavati.

4.) Generirajte bit-mapiranu sliku pomoću testiranog niza brojeva. Zatim pokušajte pronaći uzorke koji se ponavljaju. Ako su vidljivi, radi se o lošem PRNG-u.



Slika 3.1. Ljudi, kao i mnoge životinje, su dobri u brzom prepoznavanju uzoraka. TRNG i PRNG se vrlo lako razlikuju na prvi pogled.

3.1.3 Druge metode korištenja NIST testova za procjenu sigurnosti

Prije nego nastavimo s razmatranjem različitih praktičnih načina izvedbe RNG-a, pogledajmo još neke primjene testova kvalitete slučajnih brojeva. Pored ocjenjivanja kvalitete RNG-a, ovi testovi se mogu koristiti i za provjeru kvalitete mnogih drugih procesa.

1.) Izlaz svake dobre kriptografske funkcije (npr. OTP, RSA, AES, itd) mora imati dobre kvalitete slučajnog niza, da može proći NIST testove. Ako svaka riječ (uzorak) od m bitova ima **jednaku vjerojatnost** (slučajnog) pojavljivanja, onda je puno teže probiti šifru, kao što smo već vidjeli u potpoglavlju 2.2. Ibn al-Durayhim je u 14. stoljeću otkrio način kako probiti monoalfabetsku šifru jednostavno zato što arapski (kao i svi jezici) ima **raz-**

[52] Vjerojatnost da će igla duljine a pasti na jednu od dvije paralelne crte (s razmakom d) se može izračunati kao p=(2a)/(πd). To znači da se aproksimacija broja π može izračunati velikim brojem bacanja igle, ili simulacijom bacanja igle korištenjem slučajnih brojeva.

ličite vjerojatnosti pojavljivanja određenih slova i grupa slova u normalnom otvorenom tekstu. NIST testiranje izlaza kripto-uređaja (šifriranog teksta) se može koristiti kao osnovna ocjena bilo koje metode šifriranja.
2.) Slično prethodnom, NIST testiranje se može koristiti za evaluaciju kriptografskih hash funkcija i sličnih funkcija (npr. MD-5, SHA-1, SHA-2). Promjena jednog bita na ulazu hash funkcije mora izazvati nepredvidivo veliku promjenu na njenom izlazu i svaki uzorak (grupa) bitova na izlazu mora imati podjednaku vjerojatnost pojavljivanja. U protivnom bi bilo moguće barem djelomično izračunati/procijeniti ulaz hash funkcije na osnovu izlaza. Hash funkcije su ciljano napravljene s namjerom da njihova inverzija bude nemoguća (ili barem vrlo teško izvediva).

3.2. Tipovi dostupnih RNG-a i mogući problemi

Do danas je napravljeno mnogo različitih tipova RNG-a, koji koriste različite slučajne prirodne procese (ili ih simuliraju). RNG-i su izvedeni na različite načine, različitim elektroničkim sklopovima, od visoko-integriranih na jednom čipu, do izvedbi s više diskretnih komponenti na običnim štampanim pločicama. Nakon opsežne pretrage, ustanovio sam da skoro niti jedan ne ispunjava sve bitne karakteristike potrebne za upotrebu u kriptografiji (navedene u 3.1.1). Zato sam odlučio projektirati i sastaviti svoj vlastiti TRNG.

3.2.1 Pseudo-slučajni generatori (PRNG)

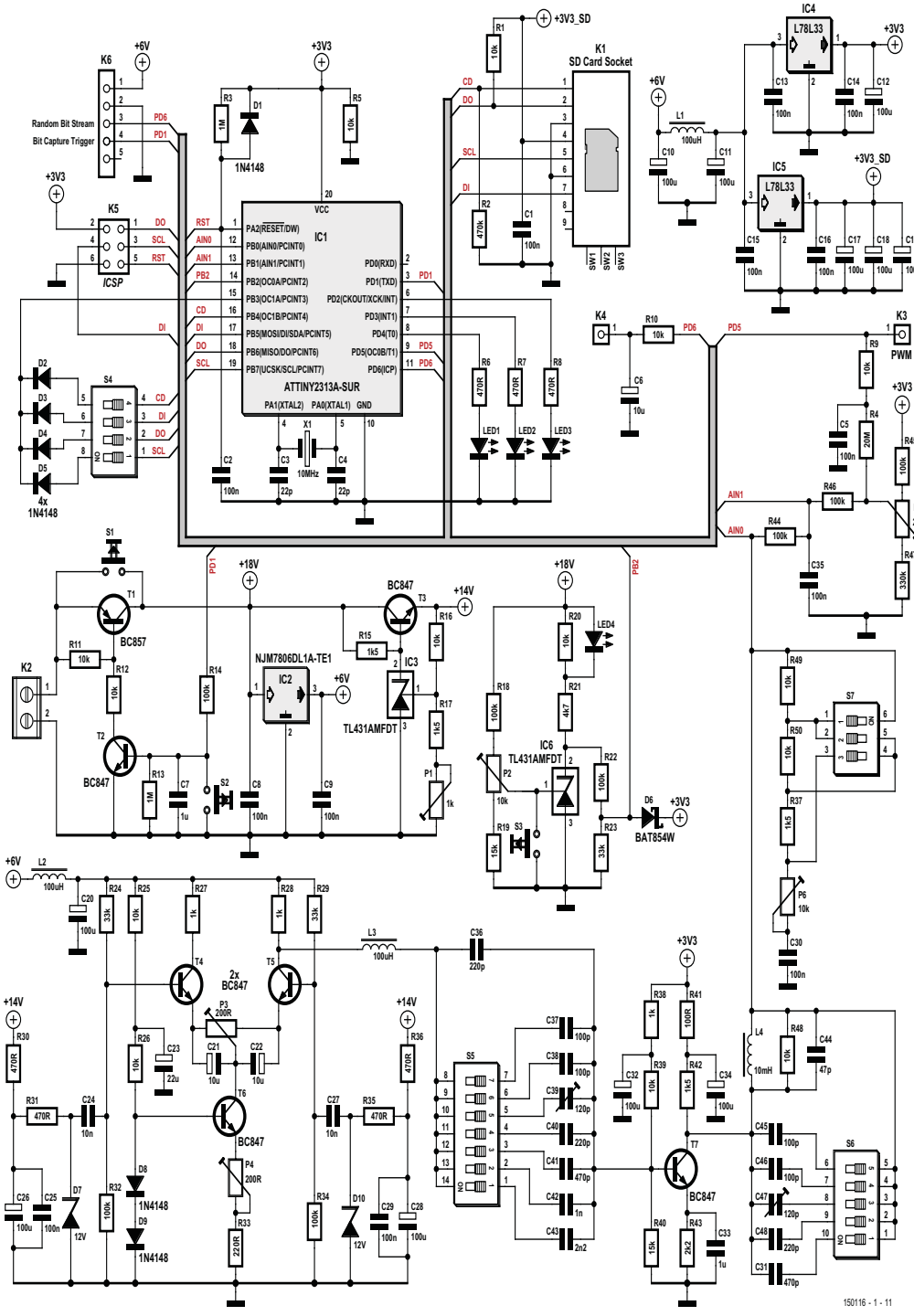
Iako nisu stvarno slučajni, oni se ipak mogu koristiti u kripto-sustavima, naravno uz određena stroga ograničenja. Najjednostavniji tip PRNG-a je tzv. **linearno-kongruencijski generator**, iz 1948. godine [7]. Definiran je jednostavnom rekurzivnom formulom:

$$x_{i+1} = (ax_i + c) \bmod m$$

Svaki slijedeći pseudo-slučajni ne-negativni cijeli broj x_{i+1} se računa na osnovu prethodnog broja x_i. Funkcija „mod" je ostatak cjelobrojnog dijeljenja nakon što se izraz u zagradama podijeli sa m. Broj m se zove „modul". Dijeljenje sa m daje ostatak u rasponu od [0,m-1] (granice uključene), što znači da će svi pseudo-slučajni brojevi x_i ostati u tom rasponu. Početna vrijednost x_0 se naziva *seed* (prevodi se kao „sjeme" ili „ključ"). S pažljivo izabranim brojevima a i m, PRNG će generirati m različitih vrijednosti prije nego se niz počne ponavljati. Na primjer, ako je m=24, a=6, c=5 i x_0=1, niz će postati 1, 11, 23, 23, 23… Nakon samo tri različite vrijednosti (iz raspona [0,23] – što su 24 moguće vrijednosti), niz će „zapeti" na 23 i ostati tamo.

Da bi PRNG radio dobro, m mora biti **prost broj**. Nadalje, broj a mora biti tzv. **primitivni korijen** broja m (detaljno objašnjeno u [7]). Broj c može biti bilo koja vrijednost različita od nule, zato što ako je c=0 i x_i=0, niz će zapeti na x_k=0, čak i ako su a i m pravilno izabrani.

Ovaj PRNG će generirati niz s dobrim karakteristikama slučajnosti (proći će NIST testove). Niz će se početi ponavljati nakon m koraka. NIST testovi će onda pokazati de-



Slika 3.2. –Elektronička shema Elektorovog TRNG-a

Poglavlje 4 – Kriptografija na papiru, u računalima i u realnosti

Specifikacije i zahtjevi za dobar kriptografski uređaj se prvo moraju precizno definirati. Kao što smo već vidjeli, mnogi sigurnosni sustavi u prošlosti su zatajili i bili razbijeni, jednostavno zato što prijetnje nisu bile pravilno prepoznate. Napadači često nisu **probijali** zaštite, nego su ih jednostavno **zaobilazili**. To je velika razlika. Nećete učiniti ništa korisno ako **krivi problem** riješite **na dobar način** – ta varijanta je još gora nego obrnuta, kod koje ste barem pravilno prepoznali pravi problem. Nešto slično se dogodilo s Maginotovom linijom na početku 2.sv.rata – dobro projektirana za statično rovovsko ratovanje 1.sv.rata, pokazala se slabom protiv modernog, mobilnog *Blitzkriega*. Prva dva poglavlja, a posebno potpoglavlje 1.2.2 obrađuju mnogo takvih primjera.

4.1. Zašto kripto-sustavi padaju?

U 2. poglavlju smo razmotrili razne metode probijanja kripto-sustava. Postoje naravno, i mnogi drugačiji napadi, od kojih su neki još uvijek nepoznati i vrhunskim stručnjacima, što znači da ih tek treba otkriti. Čak i ako je matematika kriptografije **savršena**, elektronički uređaji na kojima se kriptografija izvodi u realnosti **nisu ni približno savršeni**, a ljudi koji rukuju tim uređajima i osjetljivim tajnama su **redovito daleko od savršenih**. Prvo ćemo razmotriti još nekoliko povijesnih primjera (anegdota s početka ovog poglavlja, navodno istinit događaj, je jedan on njih).

4.1.1 Glasovita ENIGMA

Znamo dobro da je (nakon velikih napora u Bletchley Parku) ipak pala, tako što je enkripcija probijena. Električni hardver Enigme je bio kvalitetno izveden, a njemačko osoblje koje je njima rukovalo je bilo dobro osposobljeno i disciplinirano. Čak i nakon što su saveznici uspjeli zarobiti potpuno ispravne Enigme, i dalje nisu mogli brzo probijati šifre. Ovo dokazuje da je Enigma bila projektirana, izvedena i sastavljena u skladu sa svim pravilima – kada su algoritmi postali poznati protivnicima, bitne tajne – tj. kriptografski ključevi (postavke rotora) su i dalje ostale tajne, tako da su njemačke komunikacije i dalje bile sigurne. Ovo je jedan od osnovnih principa dobre kriptografije.

Nadalje, kritične operacije šifriranja/dešifriranja poruka Enigmom i odašiljanja/prijema šifriranog teksta radio-telegrafom su bile **fizički razdvojene**, što je bitno za sigurnost (što smo spomenuli već nekoliko puta, u prethodnim poglavljima). Enigma je radila na jako niskim frekvencijama, tako da nije bilo opasnosti od TEMPEST napada, pogotovo unutar čelične podmornice okružene slanom vodom. Eva (odnosno cijeli tim u Bletchley Parku, s vrhunskim poljskim kriptolozima i Alanom Turingom) nije mogla efikasno probiti šifre (sve do 1943). Mallory je mogla nešto učiniti podmetanjem poznatog otvorenog teksta (tzv. „***chosen-plaintext attack***"), dok Trudy nije mogla biti neke koristi, pogotovo u podmornici. Ovdje bi bilo bitno primijetiti da niti jedna od metoda napada iz 2. poglavlja, namijenjena za digitalne elektroničke sustave, nije upotrebljiva protiv Enigme, zbog očiglednih razloga.

nuklearne bombe) i poslati ih u SSSR, što im je omogućilo da brzo nadoknade svoj početni zaostatak u utrci u nuklearnom naoružavanju.

Generiranje velike količine dobrih slučajnih brojeva, za svakog ruskog agenta u SAD-u, je 1940-ih bio veliki problem. Elektronička računala su još uvijek bila u povojima, nedovoljno razvijena i nepouzdana. Tehnički resursi potrebni za generiranje i kopiranje slučajnih nizova su stoga bili jako ograničeni. Sve potrebne radnje – generiranje, dupliciranje i dostava/distribucija jednokratnih ključeva su bile vrlo teško izvedive tehnologijom dostupnom 1940-ih godina. Vidjet ćete kako sam ja riješio svaki od ovih problema (za moj TRNG sada već znate), ali za to mi je trebala barem tehnologija na nivou sredine 1970-ih godina.

Postoji jedna dobra vježba koju bi svaki razvojni inženjer trebao povremeno provoditi. Nakon što ste uspješno riješili neki problem, zapitajte se kako bi naši **kolege iz prošlosti** riješili isti taj problem? Vratite se malo u 1970-e, 1950-e… Mnoge probleme je moguće riješiti i puno starijom tehnologijom, a vi toga vjerojatno niste svjesni. Sjećate li se serijala „Povratak u budućnost"? Epizoda u razdoblju Divljeg Zapada je odličan primjer – **kako postići brzinu veću od 140 km/h s tehnologijom 1880-ih** - jer je DeLorean ostao bez benzina? Jedna (vrlo opasna metoda) je forsiranje standardne lokomotive (pogonjene klipnim parnim strojem) iz tog doba preko svih tehničkih sigurnosnih granica, zajedno sa željezničkim tračnicama. Mnoge današnje europske željezničke pruge su nesigurne za brzine veće od 100 km/h. Iako su (50-ak godina kasnije) napravljene parne lokomotive koje su sigurno mogle postići i brzine veće od 200 km/h, standardni modeli iz tog vremena su imali grube oblike i stoga jako loša aerodinamička svojstva – inženjerima je trebalo dosta vremena da prihvate prirodno efikasne oblike (kao npr. tijela ptice), pogotovo kod projektiranja kopnenih vozila. Čak i ako bi, i kotao i ložište, izdržali ekstremna naprezanja materijala zbog previsokog tlaka i temperature (veća brzina zahtjeva veći tlak pare u kotlu, zajedno s većim izlaznim protokom pare, za što je potrebna mnogo veća temperatura u ložištu), vjerojatno bi prevelike aerodinamičke sile (otpor i uzgon, oba rastu s **kvadratom brzine**) i vibracije polomile lokomotivu ili je jednostavno izbacile iz tračnica. Ručno upravljanje strojem s vanjskim izgaranjem (tada i nije bila dostupna neka automatizacija, možda centrifugalni regulatori brzine i sigurnosni tlačni ventili, koji bi svi u ovom slučaju morali biti blokirani) u ovako ekstremnim uvjetima je jako teško. Možda bi Marty i Doc postigli bolje rezultate s improviziranim raketnim pogonom, s krutim gorivom na bazi crnog baruta s „bogatom" smjesom, s više ugljena, a manje salitre, koji tako ne bi eksplodirao nego samo brzo izgorio? Mogli bi recimo, sklepati improviziranu rafineriju – ionako bi trebali izdestilirati samo nekoliko litara benzina (sirova nafta je tad već bila dostupna). DeLoreanov motor mora izdržati samo nekoliko minuta rada s lošim „*moonshine*[59]" benzinom, nakon toga se može i raspasti. Takva havarija je puno manje opasna za vozače nego eksplozija parnog kotla ili DIY raketnog motora. Možete li smisliti neku drugu metodu?

---

59 Riječ iz američkog slenga, stvorena u razdoblju prohibicije. Odnosi se na ilegalna, tajno proizvedena alkoholna pića, noću pod „svjetlošću mjesečine", u kućnim destilerijama.

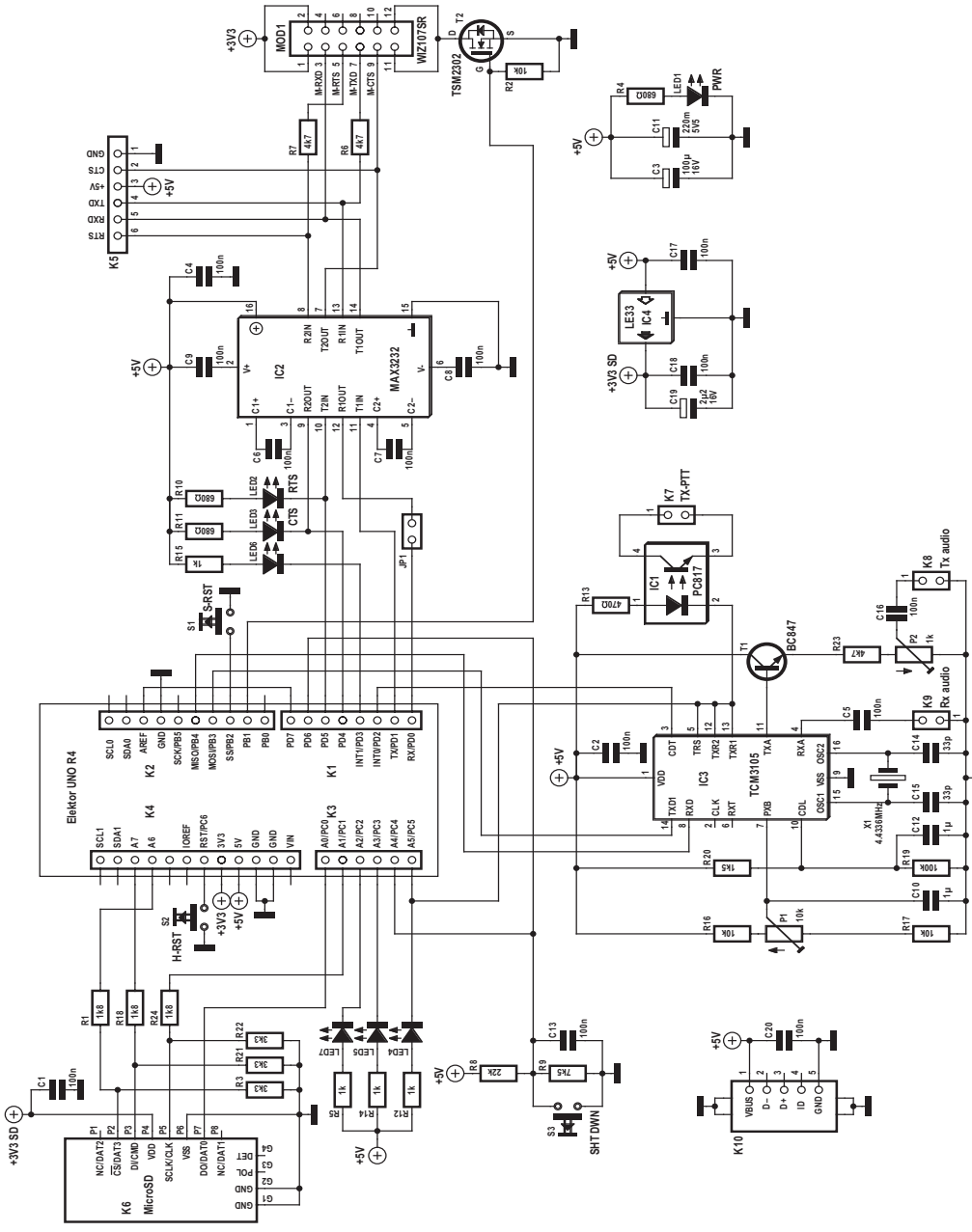
U to vrijeme (početak 1990-ih), sve navedene izjave su bile rutinski etiketirane i odbačene kao „teorije zavjere“.

4.4. Elektorov OTP Crypto Shield

Vidjeli smo kako kriptografski sustavi često lako padaju. Oni mogu pasti na praktički beskonačno mnogo načina. Čak i ako su matematika, tehnologija, implementacija i sigurnosne procedure savršene, ljudi koji koriste sustav će uvijek pronaći novi, često originalan i genijalan način da sve upropaste. Vidjeli ste i da su neki sustavi bili namjerno napravljeni tako da ih se lako probije!

Ovaj uređaj sam napravio u suradnji s Elektorom nakon što sam uzeo u obzir sve probleme koje smo do sada (u ovoj knjizi) razmotrili. Ovaj Crypto Shield je napravljen kao dodatak na Elektorov **UNO R4** (poboljšani sustav sličan Arduinu, koji koristi ATmega328PB, „B“ model s **dva** hardverska SPI porta i **dva** UART porta). UNO R4 možda neće biti lako nabaviti, ali isti Shield će raditi i sa običnim ATmega328, s malo različitim MCU firmverom (drugi UART port je „bitbangiran[76]“). Sklop koristi Vernamov OTP kao jedinu potencijalno neprobojnu šifru. Na slici 4.1. je prikazana shema sklopa „Shield-a“ . Ako Elektorov UNO R4 nije dostupan (na slici 4.2), zamjenski sklop s ATmega328P se može sastaviti prema shemi na slici 4.3. Slijedite web poveznicu [25] projekta, za moj članak objavljen u Elektoru i sve detaljne opise potrebne za izradu sklopova, zajedno s Labs stranicom i videosnimkama s demonstracijom rada uređaja.

[76] **bitbanging** – emuliranje određenog komunikacijskog protokola (npr. UART, SPI, I^2C… kada nema odgovarajućeg hardverskog elektroničkog sklopa) direktnim očitavanjem/prebacivanjem ulaznih/izlaznih bitova korištenjem CPU/MCU softvera, ne hardvera.



Slika 4.1. Shema Elektorovog OTP Crypto Shielda

Poglavlje 5 – Još nekoliko jednostavnih i jeftinih, ali vrlo sigurnih uređaja

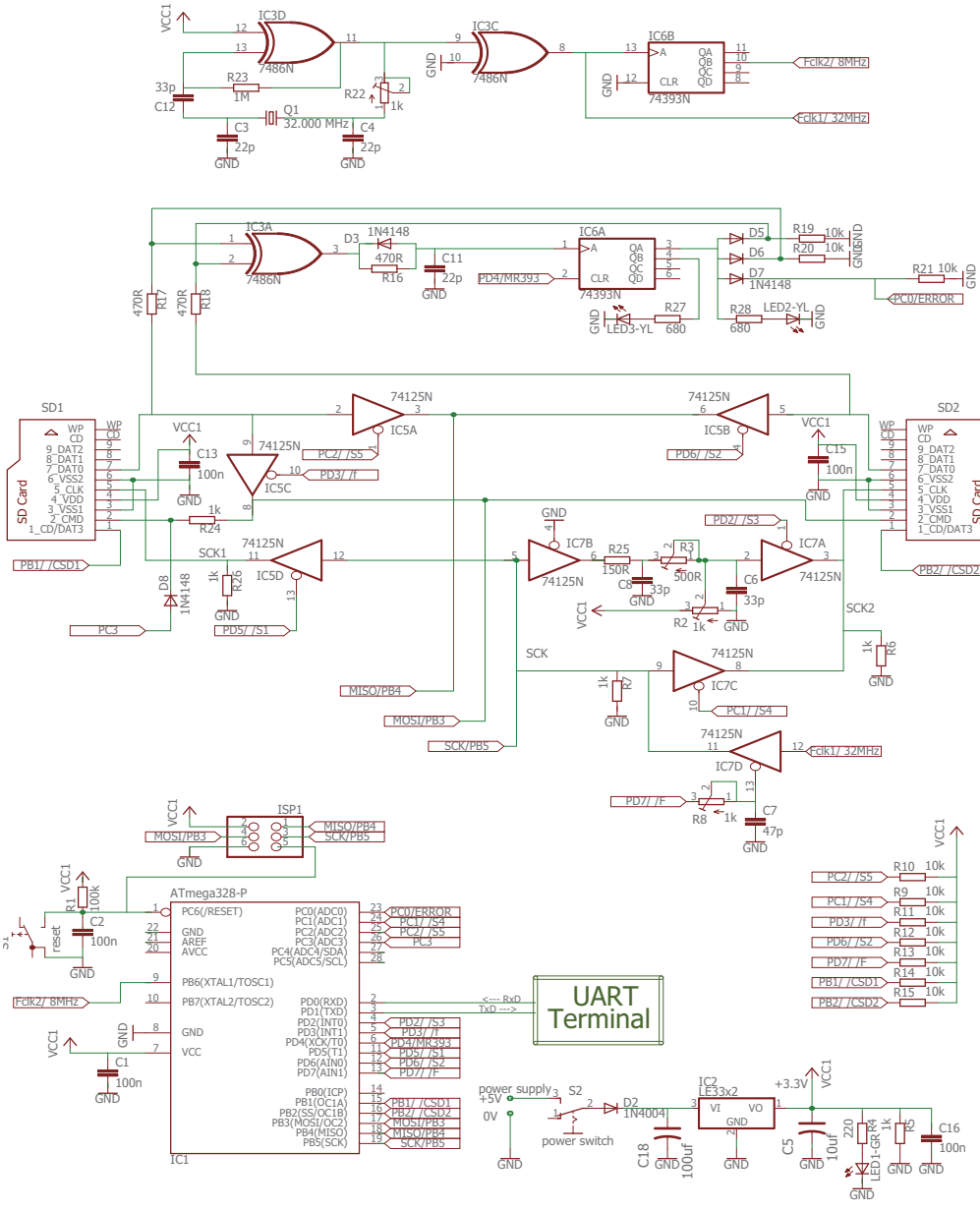
Većina ovih korisnih „alatki“ je u vrijeme pisanja engleskog originala ove knjige već bila razvijena do razine potpuno testiranih prototipova sastavljenih na perforiranim pločicama. Magnezijeva „analogna memorija“ i MyNOR računalo (1-bitno računalo bez integriranog CPU-a) su sada već sastavljeni na profesionalnim štampanim pločicama i objavljeni u Elektoru (PCB Gerber datoteke i sve ostalo), a sve ostale imamo u skorom planu. Bit će potrebna još manja podešavanja MCU firmvera, što vrijedi i za uređaje iz 4. poglavlja – oni se isto uvijek mogu dodatno poboljšavati, barem na nivou softvera.

5.1. Uređaj za kopiranje SD kartica

SD kartice inherentno skrivaju mnoge sigurnosne „zamke“ (kao što smo pokazali u 1.3, i ponovno dokazivali, na više načina). S druge strane, teško ih je potpuno odbaciti zbog njihove rasprostranjenosti i lake dobavljivosti, malih dimenzija, niske cijene, velikog kapaciteta memorije i jednostavnosti spajanja preko dobro poznatih fizičkih sučelja i komunikacijskih protokola. Ako te sigurnosne zamke možemo nekako zaobići, uz precizno i strogo definirane procedure sigurnog rukovanja (eng. *OpSec*), one će se opet moći koristiti u sigurnim kripto-sustavima, naravno uz određena ograničenja.

Elektor TRNG, OTP Crypto Shield, i TEB kutijica koriste SD kartice. Ovaj uređaj za kopiranje će omogućiti slijedeće:

1. S obzirom na to da može pristupiti svakom pojedinom sektoru SD kartice (512 bajtova), on može pouzdano i sigurno kopirati fajl s jedne SD kartice na drugu, bez nekontroliranog curenja podataka između dvije SD kartice, ali i prema bilo kojem drugom čipu ili nesigurnom uređaju. Obično PC računalo može kopirati SD kartice, ali Alice ne može kontrolirati pristup svakom pojedinom sektoru, tako da će neki podaci uvijek neprimjetno „procuriti“ prema PC-u, ali i iz njega!
2. Moguće je sigurno kopirati fajlove s OTP ključevima (nizovi slučajnih brojeva koje je generirao TRNG) za Alisu i Boba. Uređaj može isto tako kopirati datoteke između **čistih** i **prljavih** SD kartica (objašnjeno u 2.6.5) i osigurati da čista SD kartica **ostane čista**, dok će se **prljave** kartice moći koristiti za razmjenu podataka sa bilo kojim nesigurnim sustavom.
3. Može otvarati i uređivati tekstualne datoteke, za pripremu poruka za offline šifriranje korištenjem OTP Crypto Shielda. Moguće su i ostale osnovne operacije na fajlovima u FAT32 formatu, kao što su brisanje, mijenjanje naziva, formatiranje SD kartica i ostalo.



Slika 5.1. Shema uređaja za sigurno kopiranje SD kartica

4 DMA[82] mod za brzo kopiranje omogućava da se niz bitova (više sektora odjednom u nizu) sa SD1 prebaci direktno na SD2 (kroz IC5C), bez da uopće prolazi kroz IC1 MCU, brzinom koja je prevelika (32 MHz) da bi IC1 mogao „uhvatiti" i pročitati te podatke na svom SPI portu (ako je u njemu podmetnut trojanac).
5 Kloniranje cijele SD1 na SD2 je također moguće, kopiranjem po sektorima, bez obzira na formatiranje kartica i datoteka (ne moraju nužno biti formatirane na FAT32 sistem).
6 Provjera ispravnog kopiranja se također izvršava u DMA modu preko IC3A, čiji XOR izlaz će otići u visoko stanje (H), ako se dva različita bita pojave na njegovim ulazima. Bistabil IC6A će to zapamtiti i o tome obavijestiti MCU.

IC3C i IC3D se koriste za generiranje signala takta od 32 MHz, kojega IC6B dijeli s 4, da bi generirao CLK takt od 8 MHz za MCU. Mikrokontroler može komunicirati sa SD1 ili sa SD2 u „sporom" SPI modu (SCK do 4 MHz), a zatim preusmjerava SPI signale u „brzi" SPI DMA mod (SCK na 32 MHz), koji prebacuje više sektora datoteka u nizu s SD1 na SD2. IC5 i IC7 služe za preusmjeravanje signala, čime upravlja MCU. Sklop oko IC7A i IC7B stvara kašnjenje SCK takta za jedan period od 32 MHz, da se izlaz SD1 sinkronizira s ulazom SD2 u modu DMA kopiranja. Pogledajte Labs stranicu projekta na [27] za sve detalje.

Iako hardverski trojanci podmetnuti unutar IC1 MCU-a ovdje ne mogu učiniti mnogo štete (uređaj za kopiranje, kao i TRNG, obično ostaje unutar Alisine ili Bobove sigurne kuće/tajnog skloništa i teško može pasti u ruke treće osobe) kao na OTP Crypto Shieldu ili na TEB kutijici, cijeli sklop za kopiranje se može modificirati da radi sa Z80 umjesto s ATmega328P. Procesor Z80 je sporiji (CLK na 4 MHz- Qc na IC6B), ali DMA prijenos će opet ostati na 32 MHz.

S nekoliko dodatnih komponenti, cijeli sklop se može nadograditi **brojačem pulsova** na SPI signalnim vodovima, tako da se rezultati brojenja mogu usporediti s referentnim **zlatnim** ATM328P **čipom**. Ako je izbrojen veći broj pulsova, to je indikacija moguće aktivnosti hardverskog trojanca. Potrebno je poslati još dodatnih pulsova na SPI da bi dodatni podaci „iscurili" prema SD karticama.

Postoji još jedna, relativno komplicirana procedura poboljšanja sigurnosti SD kartice, a to je preprogramiranje njenog internog MCU-a koji upravlja LBA adresiranjem i ujednačavanjem trošenja sektora (*wear-levelling*) među fizičkim memorijskim lokacijama, odnosno fizičkim sektorima SD kartica. Cilj bi bio izbjegavanje nekontroliranog i opasnog *write amplificationa* (objašnjeno u 1.3).

---

82 DMA: **D**irect **M**emory **A**ccess, odnosno direktan pristup memorijama. Način prijenosa podataka od jedne memorije (ili I/O jedinice) prema drugoj direktno, bez prolaska podataka kroz registre i interne podatkovne sabirnice CPU-a. Osim što radi puno brže, također i smanjuje opterećenje CPU-a, ali zahtjeva dodatne sklopove. Uređaj za kopiranje SD kartica je napravljen da iskoristi sve prednosti DMA prijenosa.

5.2. Uređaj za kopiranje između SD kartice i audio kazete

Magnetske trake su bolje od SD kartica po svim sigurnosnim aspektima. Ovo smo već analizirali u potpoglavlju 1.3. Posebne varijante sistema digitalnih magnetskih traka, koji mogu snimati digitalne signale direktno na traku, su dosta skupe. Alice i Bob će ih teško moći nabaviti, a takvi uređaji često sadrže dodatne digitalne sklopove kojima neće moći vjerovati (slično kao i novijim modelima VCR-a – objašnjeno u 1.3). Pored toga, postoji mnogo različitih formata digitalnih magnetskih traka, a svatko tko ih kupuje u današnje vrijeme će lako privući Evinu pažnju.

Obične analogne audio kazete su i dalje rasprostranjene i lako dobavljive. Jednostavni analogni kazetofoni ne mogu sadržavati dodatne sklopove ili trojance. Zato je najbolje rješenje za Alisu i Boba napraviti ovaj uređaj, koji će pretvoriti digitalne signale u analogne audio pulzacije, koje se mogu snimati na standardnu audio kazetu brzinom od 1200 bps. Nadalje, ovaj uređaj će raditi s **bilo kojim običnim analognim kazetofonom bez modifikacija** (elektroničkih ili mehaničkih) **na samom kazetofonu**. U razdoblju 1980-ih, Sinclair ZX Spectrum je bio napravljen da radi s običnim standardnim kazetofonima, dok je Commodore 64 koristio svoj posebno projektirani kazetofon (koji je opet radio sa standardnim audio kazetama).

Traka standardne **kompaktne audio kazete** se kreće brzinom od 4.75 cm/s i postiže koristan frekventni raspon do 12 kHz (najkvalitetniji kazetofoni, s vrhunskim analognim korektivnim filterima i vrlo preciznim sklopovima za stabilizaciju brzine trake, su 1980-ih na običnim audio kazetama postizali gornju graničnu frekvenciju do 20 kHz, kao npr. japanski Nakamichi).

Za ovaj sklop, dovoljan je raspon frekvencija od 180 Hz do 3000 Hz. On zato može raditi i s diktafonskom **mikrokazetom** na 2.4 cm/s, čak i na 1.2 cm/s. Gornja granična audio frekvencija raste približno proporcionalno s brzinom trake. Sada bi se trebali podsjetiti da su standardni modemi za stare analogne telefonske linije bili napravljeni za brzine do 28 kbps (mogli su postići do 56 kbps s digitalnom kompresijom u realnom vremenu), a frekvencijski raspon analognih telefonskih linija i sklopova je otprilike isti (do 3000-4000 Hz). Zašto ovo sada spominjem? Prisjetimo se jednog od osnovnih principa projektiranja pouzdanih sigurnosnih kripto sustava – **nikako ne forsirati dostupnu tehnologiju do krajnjih granica!** Knjiga [28] objašnjava praktički sve bitne detalje magnetofonske tehnologije, dok [29] pokriva mnoge druge „zastarjele“ tehnologije.

Neizbježne fluktuacije brzine trake, pod nazivima „**zavijanje**“ (eng. *wow*, spore varijacije, do 5 Hz, posljedica elastičnosti, tromosti i tolerancija dimenzija mehaničkih sklopova) i „**cviljenje**“ (eng. *flutter*, brze varijacije, do 100 Hz, uzrokovane uglavnom vibracijama) su glavni problemi kod pohrane digitalnih podataka na magnetskim trakama. One uzrokuju varijacije frekvencije tonova, što je veliki problem za FSK modulaciju, a također i varijacije amplitude (manji problem). One su u biti još veći problem kod hi-fi muzičkih uređaja, jer uho osjetljivog audiofila može primijetiti i varijacije brzine od samo 0.5%. Najkvalitetniji (vrlo skupi) magnetofoni imaju varijacije brzine manje od

Poglavlje 6 – Praktični dio

Demonstrirat ćemo nekoliko praktičnih napada. Vrijeme je da prethodno razrađenu teoriju isprobamo u praksi. Koristit ćemo jako jednostavan i jeftin hardver. Možete i sami jednostavno ponoviti ove eksperimente. Prvo ćemo izvesti dva TEMPEST napada (osnove TEMPEST-a smo objasnili u 2.4.1). Nakon toga slijede dva napada preljevom međuspremnika (*buffer-overflow*, potpoglavlje 2.3.1) na Z80 računalo (standardni Von Neumannov CISC CPU). Za kraj ćemo demonstrirati dva napada na standardnu SRAM memoriju zasnovana na efektima remanencije digitalnih memorija (objašnjeno u 2.6). Ako ste pažljivo pročitali i shvatili teoriju, vjerojatno ćete smisliti i vlastite varijante, ili metode da unaprijedite ili automatizirate slijedeće procedure.

6.1. Primjeri TEMPEST napada

U većini slučajeva, Eva mora početi s nekakvim „izviđanjem", odnosno obavještajnim radom (eng. *intelligence work*). Ona prvo mora prikupiti tehničke informacije o Alisinom hardveru kojeg pokušava napasti. Čak i ako Alice radi za dobro financiranu troslovnu organizaciju, ona vjerojatno koristi običnu tipkovnicu, monitor, računalo, printer ili mikrovalnu pećnicu. Vrlo je vjerojatno da barem jedan od tih uređaja ima nekoliko slabih točaka, kroz koje TEMPEST signali mogu „procuriti".

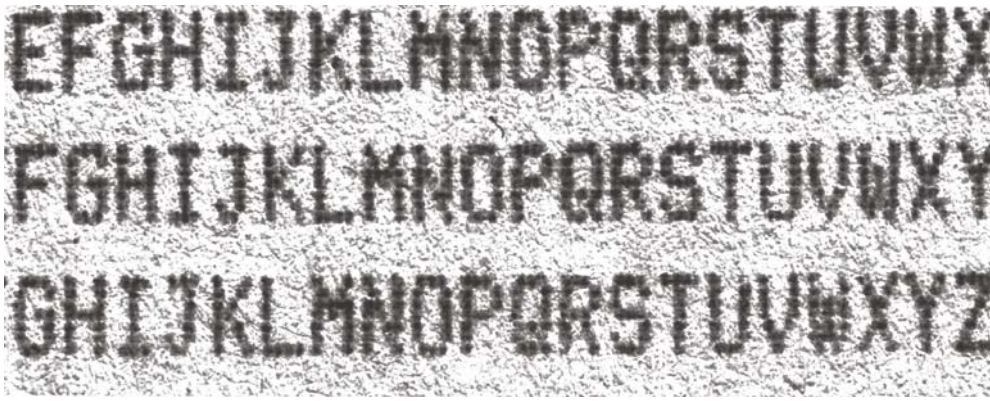
Nakon što sazna tip i model Alisinog printera (npr. od „čistačice" Trudy), nabavit će isti takav printer i analizirati ga, odnosno pronaći njegove potencijalne slabe točke. Pokušat će izmjeriti rezidualna zračenja, elektromagnetska i akustička. Zatim mora prepoznati koje dijelove frekvencijskog spektra ima smisla prisluškivati. Onda će izmjeriti frekvencijske raspone oko središnjih frekvencija (odnosno frekvencija vala nosača – eng. *carrier frequencies*) i pokušati prepoznati koja je vrsta rezidualne modulacije prisutna (npr. AM ili FM, ali najčešće se radi o određenoj kombinaciji različitih modulacija). Sada Eva može sastaviti prislušni uređaj, npr. usmjerenu antenu, niskošumno pretpojačalo, RF prijemnik s odgovarajućim demodulatorom, osciloskop, itd. S obzirom na to da su primljeni signali redovito jako slabi, ona će morati podesiti svoje analogne filtere na najmanje frekvencijske raspone, da bi što više smanjila šumove. Demodulirani signal će vjerojatno trebati dodatno obraditi raznim naprednim digitalnim filterima (kao što je npr. **dekonvolucijski filter** korišten u 2.4.1), da bi konačno na izlazu dobila korisne signale.

Počet ćemo s TEMPEST napadom na matrični printer.

6.1.1. TEMPEST napad na matrični printer

Matrični printeri su jako loši sa stajališta sigurnosti. Iako *daisy-wheel* printeri stvaraju puno jaču akustičku buku, zvukovi koji nastaju udarcem čekića u različite pisaće šipke (*typebars*) se međusobno tek neznatno razlikuju. Zato je TEMPEST napad na matrični printer relativno jednostavan – ukupni broj pinova (iglica) udarenih istovremeno je približno proporcionalan amplitudi audio signala (buke).

Matrični printeri imaju više vertikalno postavljenih iglica u nizu (obično između 7 i 24) u glavi pisača, koja se kreće horizontalno. 24-pinski tipovi su bili vrhunac tehnologije na nivou kućnih računala sredinom 1980-ih. U ovoj demonstraciji sam koristio Samsung Bixolon SRP-275, 9-pinski printer sa standardnom namotanom papirnom trakom širokom 76 mm. Eva može kupiti isti takav printer na eBay-u i za početak će napraviti nekoliko testova. Prvo će odskenirati štampana slova da bi provjerila raspored točkica u matrici (sl.6.1).



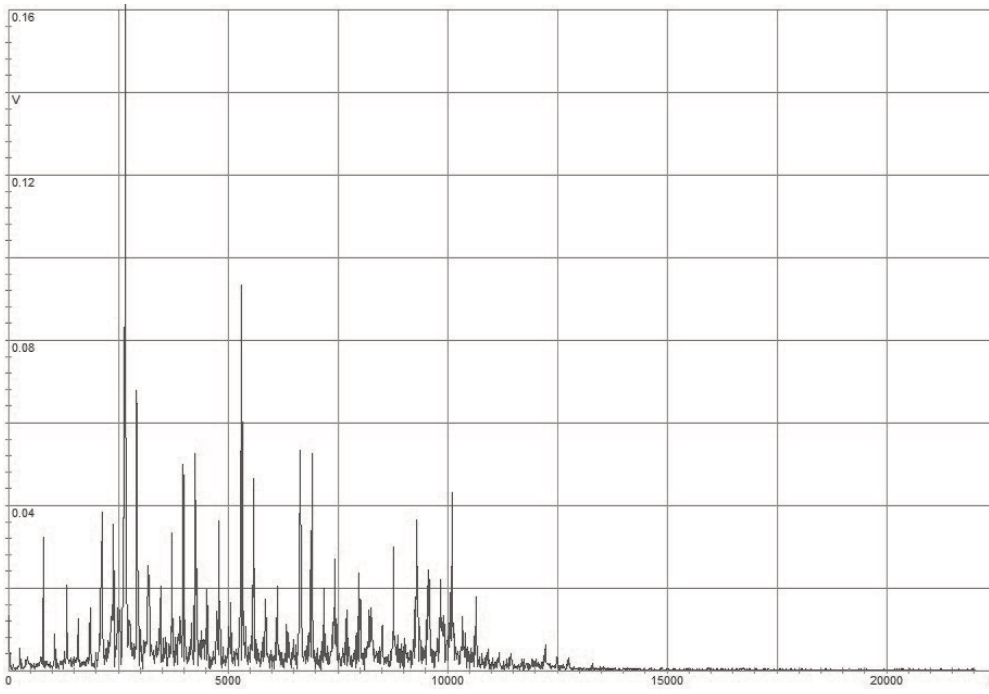
Slika 6.1. Ispisana slova na SRP-275, skenirana i digitalno obrađena

Kao što vidite, sva standardna velika engleska ASCII slova mogu stati u matricu od 7x5 točaka. Kada glava pisača putuje slijeva nadesno, ispisujući npr. slovo "P", prvo udara 7 pinova, zatim 2, opet ista ta 2 i konačno opet 2 (sada različita) pina. Na taj način, mjerenjem amplitude zvučnih pulzacija, slovo „P" se može kodirati kao 7-2-2-2. Po istoj toj logici, slovo „I" se kodira kao 2-7-2, slovo „L" kao 7-1-1-1, „H" kao 7-1-1-7, a „W" kao 6-2-4-2-6. Izmjerit ćemo akustičke signale-uzorke tih slova i usporediti ih.

Slijedeći korak je mjerenje frekvencijskog spektra rezidualnog zračenja uređaja – ovdje je to frekvencijski spektar akustičkih impulsa. Počet ćemo od frekvencija koje ljudsko uho može registrirati. Na sl.6.2. možete vidjeti spektar signala na mikrofonskom ulazu PC računala, iz standardnog mikrofona. Odmah uočavamo naglašeni šiljak na 2650 Hz, i krećemo od toga. Ta frekvencija odgovara broju horizontalnih točaka u sekundi koje SRP-275 može ispisati.

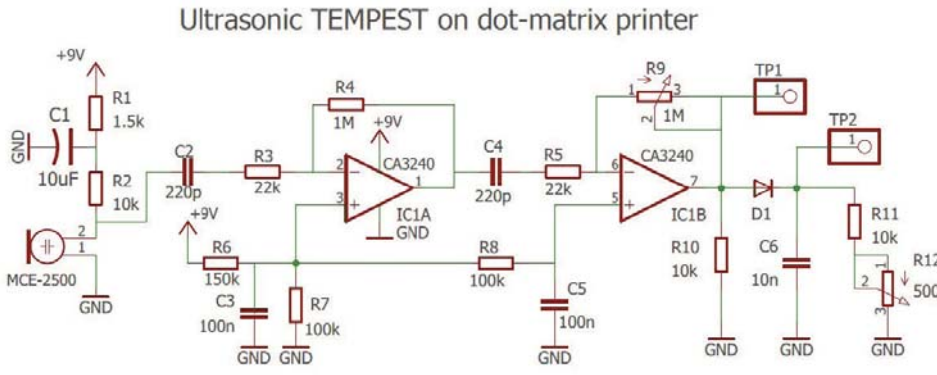
Ne vidimo ništa iznad 10 kHz, ali to je zbog filtriranja u mikrofonskom pretpojačalu, kao i u samom mikrofonu. Raspon do 4 kHz je dovoljan za ljudski glas. Spektralne komponente zvuka se mogu očekivati i duboko unutar ultrazvučnog (iznad 20 kHz) područja jer su pinovi u glavi pisača vrlo kratki. Nadalje, analiziranje zvučnih pulzacija na 2650 Hz je kompliciranо, jer istitravanje (eng. *ring-out*) zvučnog pulsa jedne vertikale pinova na toj frekvenciji traje predugo – unutar tog vremena glava pisača može ispisati još najmanje 10 horizontalnih točaka. Zato će prislušni uređaj morati biti podešen na više ultrazvučne harmoničke članove (iznad 30 kHz) koji se istitravaju puno brže. Susjedni

(horizontalni) akustički impulsi se moraju razdvojiti da bi bilo moguće prepoznati pojedini akustički uzorak u vremenskom području (npr. 2-7-2 za slovo „I“).



Slika 6.2. Spektar zvuka printera SRP-275 u čujnom rasponu

Ultrazvučni TEMPEST prijemnik je prikazan na slici 6.3. Jednostavno dvostupanjsko pojačalo na ulazu ima *electret* mikrofon MCE-2500, s ultrazvučnim rasponom do 100 kHz. Kondenzatori C2 i C4 definiraju donju graničnu frekvenciju na 30 kHz, što filtrira niske čujne frekvencije, čije istitravanje traje predugo.



6.3. Shema ultrazvučnog mikrofonskog pojačala

Poglavlje 7 – Dodatne ideje

Postoje još mnoge ideje za razvoj jeftinih, jednostavnih uređaja, korisnih Alisi i Bobu, koje još nisam počeo ozbiljno razvijati. Ovo posljednje poglavlje je cijelo posvećeno tome. Dobre ideje (kao ni razvoj prototipova) danas više ne donose neku zaradu, tako da ću ih sada podijeliti s vama. Ako mislite da možete pronaći način da neke od njih komercijalizirate, molim vas da učinite najbolje što možete!

7.1. SIGSALY-2 *„Reloaded"*

Originalna SIGSALY je stvorena za vrijeme 2.sv.rata. Bio je to sustav kriptiranja ljudskog glasa, zasnovan na jednokratnoj šifri (OTP). Koristio je kompliciranu kombinaciju analogne i digitalne (!) elektronike, s **gramofonskim pločama** (sada bi bio dobar trenutak da ponovo pogledate knjigu [29]), na kojima su bili pohranjeni OTP ključevi snimljeni u obliku bijelog šuma. Cijeli sistem je bio izrazito kompleksan, težio oko 50 tona, i koštao oko 1 milion USD (što bi bilo oko 15 miliona u današnjim novcima).

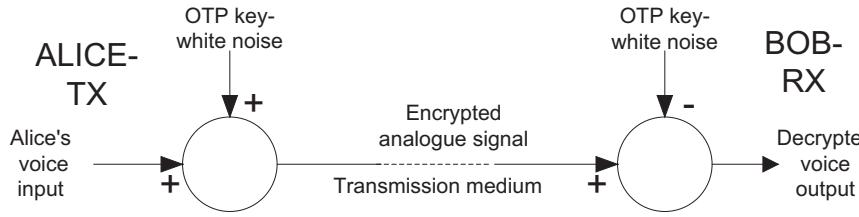
Dok sam razmišljao o načinu kako realizirati kvazarni OTP sustav (potpoglavlje 4.4.1), došao sam na ideju da upotrijebim **analogne** sklopove za OTP šifriranje i dešifriranje. Zato sam uzeo originalnu SIGSALY kao početnu točku jer je ona koristila **analogni medij** (gramofonske ploče) za pohranu OTP ključeva, a isto tako i mnogo analognih elektroničkih sklopova za obradu signala i kriptografske operacije. Korištenjem moderne analogne i digitalne elektronike, SIGSALY-2 će koštati oko 200 EUR u dijelovima – Alice i Bob si to mogu priuštiti!

Glavna ideja je upotrijebiti **analogno zbrajanje** (jednostavan sklop za zbrajanje s jednim operacijskim pojačalom) analognog signala glasa i bijelog šuma (odnosno niza slučajnih brojeva na izlazu iz SD kartice) za kriptiranje Alisinog glasa. Nakon prijema, Bob će koristiti **analogno oduzimanje**, odnosno oduzeti će snimljeni (na svojoj SD kartici) bijeli šum od primljenog kriptiranog glasa da bi dobio otvoreni, razumljivi Alisin glas. Amplituda OTP-bijelog šuma mora biti oko 10x veća od amplitude signala Alisinog glasa, da bi njezin glas postao sigurno nerazumljiv (kod omjera 1/1, Eva će još moći razumjeti Alisin zašumljeni glas bez puno napora).

Zašto ovakav pristup? Obrada analognog signala nije jako zahtjevna – i dobri stari Z80 to može. **Glavni razlog**, međutim, je taj što ovaj sustav može biti napravljen da radi s kvazarnim OTP-om (ili sa sličnim sustavima, kod kojih nije potrebno da se Alice i Bob fizički nalaze da bi razmjenjivali OTP ključeve!). Sjećate li se glavnog problema, analiziranog u 4.4.1? Alice i Bob mogu uhvatiti isti signal s istog kvazara ili satelita (da bi generirali OTP ključeve), ali vjerojatno amplitude neće biti jednake, a uvijek će biti prisutno i neko kašnjenje (reda veličine 20-40 ms, ako se oboje nalaze na planeti Zemlji, što možemo razumno pretpostaviti). Čak i ako se razlika u amplitudi i vremensko kašnjenje mogu savršeno kompenzirati, ta dva signala opet neće biti 100% jednaki. Razlog tome su uvijek prisutne male razlike među parametrima analognih filtera u Alisinom i Bobovom radio prijemniku, ali i različite putanje radio signala kroz atmosferu. Korištenje OTP en-

kripcije u uobičajenom „digitalnom“ modu (kao u potpoglavlju 4.4, OTP Crypto Shield) zahtjeva 100% identične OTP ključeve (za Alisu i Boba), precizno sinkronizirane, što nije problem kod digitalnog kopiranja OTP ključeva s Alisine na Bobovu SD karticu.

Kompenzacija razlike u amplitudi Alisinog i Bobovog OTP ključa kod SIGSALY-2 je relativno jednostavna, a kompenzacija vremenskog kašnjenja je malo složenija. Ovo je slično traženju izgubljenog pokazivača položaja ključa kod OTP Crypto Shielda. Poslije ćemo vidjeti da će to ovdje raditi puno brže, s analognim sklopovima u SIGSALY-2. Čak i ako Alisin i Bobov OTP ključ (nakon kompenzacije na Bobovom prijemniku) nisu 100% identični, **to će se manifestirati samo kao slabiji šum** nakon dešifriranja na Bobovom prijemniku, ali Alisin glas će još uvijek biti dovoljno razumljiv! Sustav će raditi dobro i ako Alice odašilje FSK modemski signal umjesto svog glasa, jer nema digitalne kompresije glasa. Idemo korak po korak, sastavit ćemo Matlab simulaciju, koja je meni radila sasvim dobro.

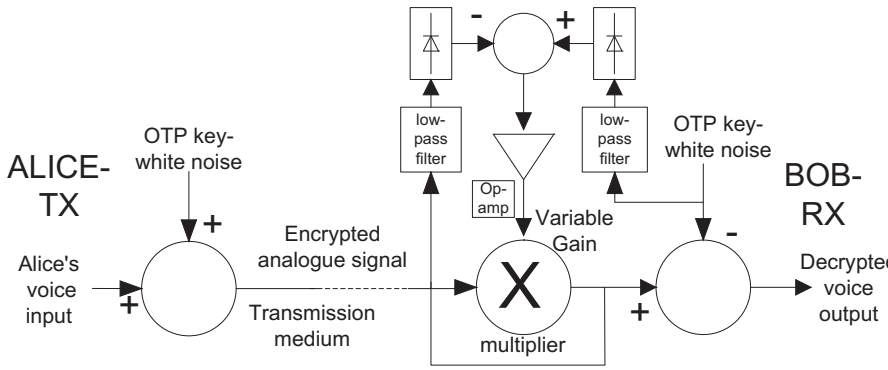


Slika 7.1. Osnovni princip analognog OTP kriptiranja glasa

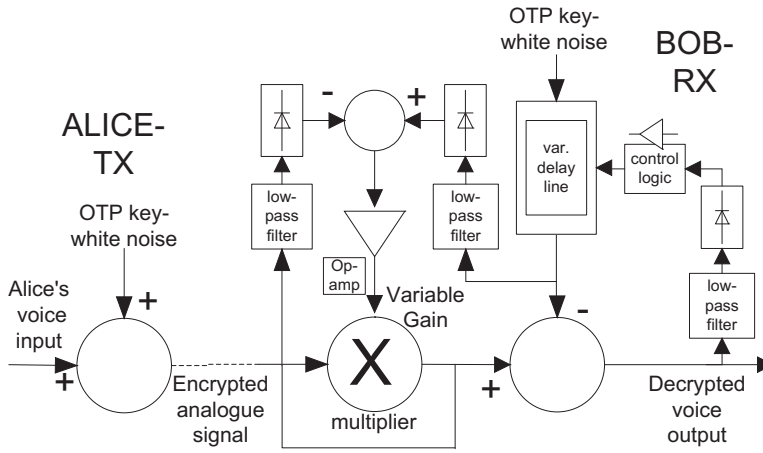
Slika 7.1 pokazuje osnovni princip. Morat ćemo se pozabaviti s više problema. Prvi je moguća razlika u amplitudi između Alisinog i Bobovog OTP ključa–šuma. Ovo se jednostavno rješava. Kako je amplituda OTP ključa-šuma na Alisinom odašiljaču najmanje 10x veća od amplitude glasa na ulazu, to znači da je dovoljno da ARP (eng. AGC, može biti potpuno analogni sklop, nešto kao PI regulator) na Bobovom prijemniku mijenja faktor pojačanja primljenog šifriranog signala, da bi izjednačio njegovu amplitudu s amplitudom OTP ključa-šuma. Ako se dva izmjenična signala zbrajaju, njihova efektivna vrijednost se računa kao

$$U^2_{šifrirano} = U^2_{šum} + U^2_{glas}$$

što znači da će rezultat biti 10.05 V, za šum na 10 V i glas na 1 V. Ova razlika od 0.05 V se može zanemariti u usporedbi s otvorenim/razumljivim glasom amplitude 1 V. Dakle, ako se amplitude primljenog šifriranog signala i OTP šuma na Bobovoj strani izjednače, to je dovoljno dobro da se može nastaviti s kompenzacijom vremenskog kašnjenja.



Slika 7.2. ARP sklop za izjednačavanje amplitude primljenog signala i OTP šuma



Slika 7.3. Promjenjiva linija za kašnjenje – FIFO buffer na izlazu SD kartice i njegova upravljačka logika

Da bismo kompenzirali vremensko kašnjenje, ubacili smo promjenjivu liniju za kašnjenje (mrtvo vrijeme) poslije izlaza OTP ključa-šuma na Bobovom prijemniku. To može biti FIFO buffer na izlazu SD kartice (koja sadrži OTP ključ-šum), prije pretvorbe u analogni signal. Dok vrijeme kašnjenja nije dobro podešeno, amplituda dešifriranog izlaza je vrlo visoka, iznad 10 V (ako su šifrirani ulaz i OTP ključ-šum izjednačeni na 10 V), kao što smo već objasnili. Kada je vrijeme kašnjenja dobro podešeno, izlazna amplituda će pasti na cca. 1 V, što je amplituda Alisinog glasa na njenom ulazu, jer se sada kriptirani analogni signal amplitude 10 V oduzima od dobro sinkroniziranog OTP šuma iste amplitude, tako da ostaje samo Alisin glas, plus mali dodatni nekompenzirani šum. Amplituda ispravljenog i filtriranog izlaza dešifriranog glasa je ulaz za upravljačku logiku za upravljanje promjenjivim kašnjenjem FIFO buffera – iznos mrtvog vremena se mijenja dok se dobro ne