LABORATORIJ ZA KRIPTOGRAFIJO IN RAČUNALNIŠKO VARNOST (LKRV)

Naš laboratorij je en izmed najmlajših, saj je bil ustanovljen leta 2006, v letošnjem letu pa smo dobili tudi prostore na Jadranski 21. Vendar pa sega pobuda za vpletanje kriptografije in računalniške varnosti v življenje na FRI vsaj desetletje nazaj, ko se je današnji vodja laboratorija vrnil iz podiplomskega študija (Univerza v Waterlooju, Kanada) in podoktorskega študija (Certicom Corp., ustanovitelj in glavni kriptograf Scott Vanstone). Že tedaj smo pričel s seminarjem iz kriptografije (na IMFM) in se začeli pogovarjati o možnem sodelovanju s kolegi iz laboratorijev LRK (Vidmar), LAPS (Kodek), LALG (Vilfan). Tedanji prodekan za študijske zadeve Tomaž Mohorič pa je vključil na podiplomski študij izbirni predmet *Kriptografija in računalniška varnost*. V naslednjem letu bo ta predmet na vrsti že petič (vabljeni pa ste tudi dodiplomci!!!), prvič pa poslušajo predmet iz *Kriptografije in teorije kodiranja* tudi naši dodiplomci na interdisciplinarnem študiju računalništva in matematike. Prvi semester predava Marko Petkovšek o teoretičnih osnovah, v drugem semestru pa bo na vrsti še drugi del, kjer bomo zavili v bolj aplikativne vode z nekaterimi člani tega laboratorija:

- Aleksandar Jurišić (predavatelj),
- Matjaž Urlep in Boris Cergol (asistenta).

Omenimo še zunanje sodelavce (a vseh tako ne smemo :-):

- Enes Pašalić (doktorat Univerza v Lundu, Švedska, podoktorski študij pa na Tehnični univerzi na Danskem, pri Larsu Knudsenu),
- Jernej Barbič (doktorat na Carnegie Mellon univerzi, sedaj na podoktorskem študiju na MIT, MA, ZDA),
- Jernej Tonejc (doktorat na Univerzi v Wisconsinu - Madison, ZDA),
- Leon Matoh (en izmed avtorjev JMT protokola, ki se uporablja za mobilno plačevanje po vsej Sloveniji, a tudi več kot 10ih drugih državah).
- Arjana Žitnik (doktorat na Univerzi v Ljubljani),

Mlajši sodelavci so še

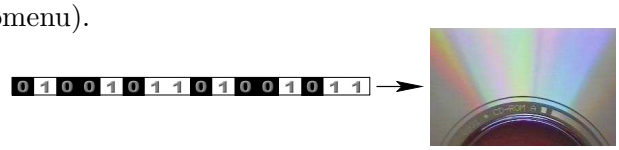
- Gregor Šega (verjetnost),
- Tadej Novak (naključna zaporedja, kode),
- Erik Schlegel (DLP na eliptičnih krivuljah).
- Matjaž Praprotnik (tekoče šifre in protokoli),
- Maruša Stanek (končni obsegi in anonimizacija) in
- Franci Močilar (analiza tveganj).

V laboratoriju pa so začeli sodelovati tudi prvi študentje: IŠRM - Peter Nose, Tadej Janež, Janoš Vidali, Lovro Šubelj, Lan Žagar in Mitja Trampuš; FRI - Rok Doltar.

Nekateri naši člani na delavnici v Plemljevi hiši na Bledu.

UVOD. Živimo v zanimivih časih, ko imamo tudi doma priložnost aktivno slediti dinamičnemu razvoju naslednjih področij:

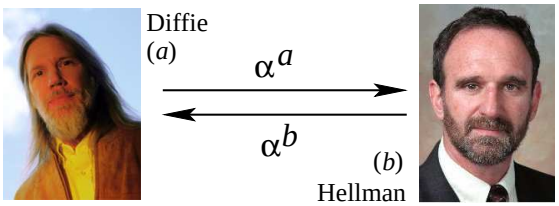
- kriptografije in računalniške varnosti (npr. kriptografija z javnimi ključi ter uporaba kriptosistemov z eliptičnimi krivuljami),
- teorije kodiranja (sestavljanje kod za odpravo napak in učinkovita implementacija),
- algebraične kombinatorike (prepletalnje algebre in diskretnih struktur, ki so v digitalni dobi pridobile na pomenu).



Kriptografija javnih ključev se je začela razvijati pospešeno v zadnjih 30-ih letih (po letu 1976, ko sta Diffie in Hellman predlagala koncept kriptografije z javnimi ključi) kot pomembna disciplina, ki ni samo predmet intenzivnega raziskovanja, temveč predstavlja osnovo informacijske družbe.

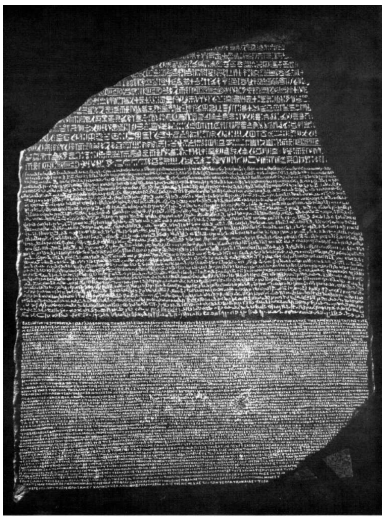
Teorija kodiranja predstavlja svojevrstno matematično zavarovanje pred muhastim svetom, v katerem živimo, saj odpravlja napake, ki jih povzročajo razne motnje in nepopolne naprave.

Algebraična kombinatorika je letos triumfirala s celotnim opisom posebne Liejeve grupe E_8 (velikost obdelave E_8 je 60GB in ga je zanimivo primerjati s projektom človeškega genoma, ki vsebuje vso genetsko informacijo celice in obsega manj kot 1GB). Del raziskav našega laboratorija pa je pripomogel k dokazu enoličnosti Pattersonovega grafa (sporadičen primitiven graf s 22.880 vozlišči in valenco 280 - pred tem je bil rekord za primitivne grafe 819 vozlišč, v splošnem pa 4096 vozlišč).



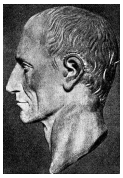
Revolucionarni DH-dogovor o ključu (oba poznata α^{ab}).

KRIPTOGRAFIJA IN RAČ. VARNOST. Gotovo ste že uganili, da je to osrednje področje LKRV-ja.



L. 1799 so v egipčanski Rosetti našli skoraj 2.000 let star kamen, na katerem so bili trije teksti: hieroglifi, pisava Egipčanov (demotic) in starogrščina. Z njim smo razvozlali hieroglife in izvedeli več o zgodovini Egipta.

Ob besedi "kriptografija" marsikdo takoj pomisli na šifriranje vojaških ukazov ali vohunskih sporočil.



Cezar ukazal napad

↓

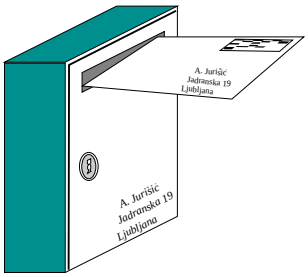
Ehbčt žnčbčo rčšćg

Res je uporaba kriptografije za namene državne varnosti dolgo časa predstavljala osnovni motiv za razvoj te vede, a ta že dolgo ni več samo v domeni vojske in tajnih služb.

Slavna šifrirna naprave II. svetovne vojne: Enigma.

Glavna naloga sodobne kriptografije sicer ostaja zavarovati vsebino sporočil pred nepooblaščenimi osebami, a danes obstaja še veliko drugih aplikacij kriptografskih metod.

Te lahko med drugim uporabimo tudi za to, da preverimo, ali je bilo sporočilo, preden je prišlo do nas, spremenjeno s strani tretje osebe, ali je oseba, ki je podpisana, res njegov pošiljatelj in ali je pošiljatelj res tista oseba, za katero se izdaja.

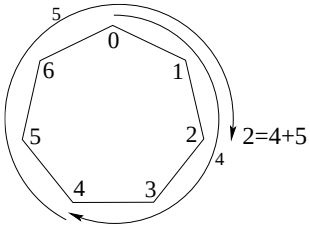


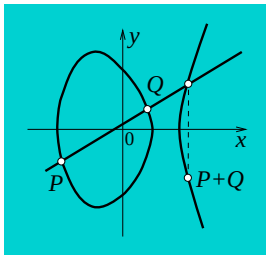
Pri konceptu kriptosistema z javnimi ključi se zgledujemo po poštnih nabiralnikih. Vsakdo, ki ve, kje je nabiralnik, lahko vanj vrže pošiljko, ne more pa je vzeti ven - to lahko stori le tisti, ki ima ključ od nabiralnika. V nasprotju z zasebno (oz. simetrično) kriptografijo ima pri javni kriptografiji vsak uporabnik **le** dva ključa: *javnega* in *zasebnega*.

Kriptografske metode so neločljivo povezane s sodobnim bančništvom, podpisovanjem in glasovanjem. Vgrajene pa so tudi v protokole, ki nam omogočajo uporabo interneta in mobilnih telefonov. Eden od izzivov, s katerimi se srečujemo v našem laboratoriju, je izgradnja novih kriptografskih protokolov.

Protokol: Vohun se je po opravljeni diverziji v sovražnem taboru vračal v grad. Ko se je v popolni temi približal vratom, je zaslišal šepetajoč glas. Kako lahko prepriča "stražarja", da pozna geslo, ne da bi ga pri tem izdal morebitnemu vsiljivcu/prisluškovalcu?

Prvi korak pri razvoju kripto protokola je izbira oziroma iskanje težko izračunljivega matematičnega problema, ki predstavlja srce protokola (npr. faktorizacija števil). Sledi praktična implementacija, ki navadno vključuje izdelavo prototipnih aplikacij na osnovi razvitih protokolov. Največjo pozornost trenutno posvečamo kriptosistemom, ki temeljijo na eliptičnih krivuljah. Ti bodo sčasoma popolnoma nadomestili znani kriptosistem RSA. Vključeni so bili tudi v Suite B, tj. seznam varnih kriptografskih algoritmov, ki jih v uporabo priporoča ameriška NSA.





V praštevilskih kolobarjih $\mathbb{Z}_p$, kjer je p praštevilo, je možno tudi deljenje z vsakim od 0 različnim elementom $a \in \mathbb{Z}_p$. Zato sodijo ti kolobarji med obsege. Končni obsegi so zanimivi tudi zato, ker računanje potenc lahko opravimo učinkovito, ne poznamo pa učinkovitih algoritmov za računanje logaritma (za razliko od realnih števil). To sta uporabila Diffie in Hellman za dogovor o ključu, kasneje pa še ElGamal za digitalni podpis.

Množica točk, ki rešijo enačbo $y^2 = x^3 + ax + b$, imenujemo **eliptična krivulja**. Točke na krivulji lahko seštevamo po "sekantnem in tangentnem" pravilu, kot to prikazuje slika. Skozi točki P in Q potegnemo premico in poiščemo tretje presečišče, ki ga nato še prezrcalimo preko osi x (v primeru podvajanja točke P pa začnemo s tangento v točki P).

V kriptografiji se nenehno bije boj med tistimi, ki želijo informacije skriti in tistimi, ki bi jih radi razkrili. Pri tem pa se morajo tako eni kot drugi ves čas prilagajati neustavljivemu naraščanju zmogljivosti računalnikov. Kriptosistem, ki se še danes zdi popolnoma varen, lahko že jutri postane popolnoma neuporaben, če nekdo odkrije luknjo v njegovi zasnovi. Seznam kriptografskih protokolov, ki jih je povozil čas, je dolg, med najbolj znanimi in še danes široko uporabljanimi sta npr. DES in WEP (ki sta ju nadomestila AES in WPA). Pri izdelavi vsakega kriptosistema je zato ključen korak preverjanje njegove zanesljivosti. Pri tem se moramo postaviti v vlogo napadalca in poskusiti s karseda raznovrstnimi sredstvi razbiti kriptosistem. V laboratoriju poleg preverjanja zanesljivosti lastnih kriptosistemov raziskujemo tudi zanesljivost drugih obstoječih kriptosistemov.

TEORIJA KODIRANJA

je matematična veja, ki nam ponuja rešitev problema, kako zapisati podatke, da bomo tudi potem, ko jih bomo prenesli preko nezanesljivega kanala, še vedno lahko razbrali izvorno sporočilo. Brez teorije kodiranja bi bilo nemogoče razbrati vsebino šibkih signalov, ki jih pošiljajo vesoljske sonde, oddaljene več miljard kilometrov. Teorije kodiranja ne gre mešati s kriptografijo. Cilj kriptografije je otežiti branje sporočil (nepooblaščenim osebam), bistvo teorije kodiranja pa je ravno nasprotno - olajšati branje podatkov.

Teorija kodiranja se ne ukvarja le s tem, v kakšni obliki poslati podatke, da bodo ti v čim manj okrnjeni obliki prispeli na cilj, ampak tudi z odpravljanjem napak v zapisu podatkov. Teorija kodiranja nam na primer omogoči, da lahko brez kakršnihkoli motenj poslušamo Mozartovo ali Madonnino zgoščenko, četudi nam jo je spraskala mačka. Posledica uspešne uporabe teorije kodiranja je bilo med drugim tudi to, da so drastično padle cene pomnilnika. Včasih je bilo treba izdelati pomnilnik, ki je vseboval le minimalno število napak, sedaj pa imamo na voljo orodja, ki avtomatično iščejo in odpravljajo napake v pomnilniku.

Algoritmi za odpravljanje napak pa niso koristni le pri zapisovanju in pošiljanju podatkov, ampak tudi pri samem delovanju računalnikov. Dokler so bili računalniki in programi, ki so jih izvajali, dovolj enostavni, so bile tehnične napake precej očitne in hitro opazne (če je npr. odpovedala vakuumska žarnica). Razvoj strojne opreme nam je prinesel vezja, katerih elementi merijo komaj nekaj nanometrov. V tako zapletenih sistemih so algoritmi za avtomatsko odpravljanje napak edino možno sredstvo za zagotavljanje maksimalne zanesljivosti delovanja naprave.

ALGEBRAIČNA KOMBINATORIKA.

V laboratoriju se ukvarjamu tudi z različnimi področji, ki predstavljajo teoretično osnovo za teorijo kodiranja in kriptografijo. Med njimi posebno pozornost namenjamo algebraični kombinatoriki. Eden osnovnih ciljev te matematične discipline je klasifikacija objektov (običajno grafov) z določenimi lastnostmi. To lahko primerjamo z iskanjem vseh planetov v našem osončju ali pa z iskanjem vseh kemijskih elementov. Predstavljajmo si, da bi se dalo izračunati, da nam manjka še en planet oziroma element, nato pa bi začeli iskati nove načine, da bi ga odkrili. Sedaj pa pomislimo, da bi z našim iskanjem prišli do povsem novega matematičnega objekta s številnimi lepimi lastnostmi. Lahko bi se npr. izkazalo, da je povezan s teorijo kodiranja ali pa končnimi geometrijami, ki jih uporabljamo kot osnovne gradnike pri shemah za deljenje skrivnosti.

Še eno bolj teoretično področje, s katerim se srečujemo v našem laboratoriju je statistično načrtovanje oziroma teorija načrtovanja eksperimentov. Izsledki te teorije so široko uporabni v različnih disciplinah, kjer je potrebno pri znanstvenem delu izvajati eksperimente. Z uporabo učinkovitih načrtov, lahko raziskovalec optimizira izvajanje eksperimenta in s tem zmanjša stroške ter porabljeni čas in energijo.

Superračunalnik Cray XMP-24 je predelani XMP-22 - prvi komercialni superračunalnik, v uporabi od 1983 do 1993, za svoje čase najhitrejši: 420 milijonov operacij na sekundo.

TEKOČI PROJEKTI

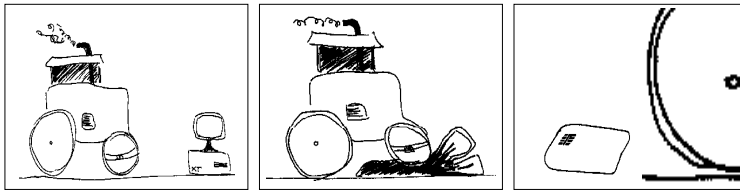
Certifikatna agencija z ECC za potrebe MORS-a

Cilj projekta je izgradnja delujočega modela certifikatne agencije, zasnovane na lastni implementaciji kriptosistema z eliptičnimi krivuljami, ki bo odgovarjala najvišjim zahtevam varnosti in bo služila kot alternativa trenutno dostopnim komercialnim rešitvam. Medtem ko osnovo za algoritem RSA predstavlja dejstvo, da je računsko zahtevno poiskati delitelje velikih števil, pa kriptosistemi z eliptičnimi krivuljami temeljijo na t.i. problemu diskretnega logaritma na eliptični krivulji. Glavna prednost kriptosistemov z eliptičnimi krivuljami je ta, da lahko za zagotavljanje enakovrednega nivoja varnosti uporabljamo krajše ključe kot pri RSA, kar omogoča hitrejše izvajanje kriptografskih algoritmov. V okviru projekta testiramo certifikatno agencijo @friCA, ki izdaja varnostne certifikate študentom in zaposlenim na FRI.

Kriptosistemi z eliptičnimi krivuljami nad praštevilskimi obsegi in pametne kartice za potrebe MO/SV

Pri tem projektu podrobneje preučujemo postopke kriptografije z eliptičnimi krivuljami nad obsegi velike praštevilske karakteristike, ki so pisani na kožo software rešitvam.

Eliptična kriptografija je zaradi hitrega izvajanja algoritmov posebej primerna za implementacijo na napravah, kjer smo močno omejeni z računsko zmogljivostjo. Eden od naših ciljev je implementirati navedeni kriptosistem na pametnih karticah.



Od osebnega računalnika pa do pametne kartice.

Anonimizacija podatkovnih baz

Z eksponentno rastjo zbiranja raznovrstnih občutljivih osebnih podatkov se je pojavila potreba po zaščiti identitete posameznika. Vsekakor pa to želimo narediti na tak način, da ohranimo uporabno vrednost zbirk podatkov. Radi bi npr. dosegli, da bodo raziskovalci, ki bodo preučevali pogostost rakavih obolenj, lahko uporabljali podatkovno bazo in prišli do potrebnih demografskih informacij, nikakor pa ne bodo mogli določiti identitete posameznega rakavega bolnika. Analiziramo tudi možne napade na anonimizirane baze in iščemo varnostne nadgradnje.

SODELOVANJE IN POVEZAVE.

Laboratorij sodeluje z Inštitutom za matematiko, fiziko in mehaniko ter programsko skupino prof. Dragana Marušiča, vzdržuje pa tudi stike s sledečimi ustanovami v tujini:

- University of Waterloo, Kanada
- University of Ottawa, Kanada
- Memorial University of Newfoundland, Kanada
- Certicom Corp., Mississauga, Kanada
- University of Wisconsin, ZDA
- Worcester Polytechnic Institute, ZDA
- Telecom-Italia, Italija
- Tilburg University, Nizozemska
- POSTECH, J. Koreja
- Osaka Kyoiku University, Japonska
- Tohoku University, Japonska

VABILO. Tisti, ki vas zanima kriptografija, računalniška varnost ali katero od drugih področij, s katerimi se ukvarjamo v laboratoriju, ste vabljeni, da nas obiščete.

Ponujamo mentorstvo pri diplomskih nalogah in magisterijih, lahko pa se nam tudi pridružite pri delu na kakšnem od naših projektov.

Nekaj naslovov že opravljenih

diplomskih nalog:

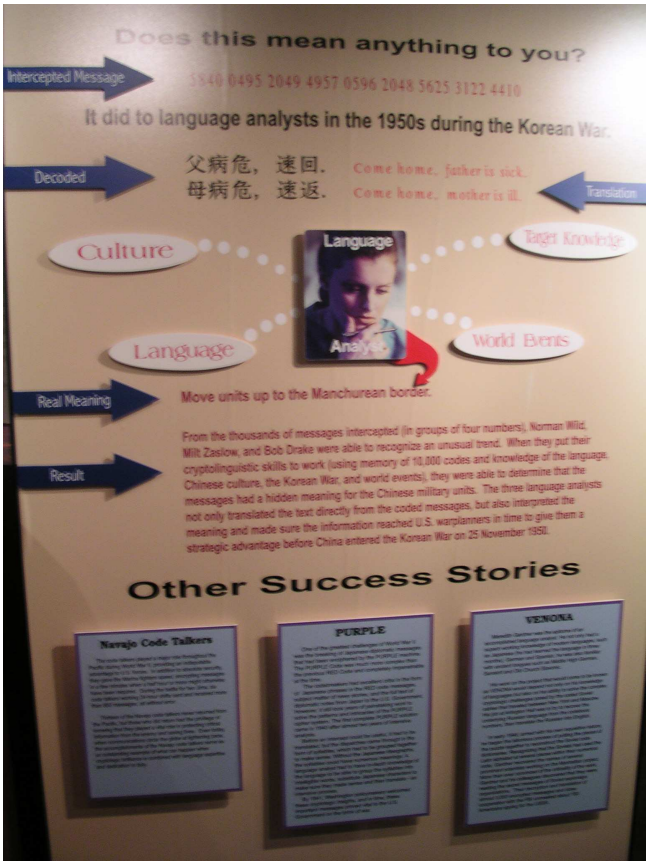
- Schoofov algoritem,
- Pseudo naključna zaporedja v kriptografiji,
- RSA kriptosistem,
- Digitalna poštna znamka,
- Kriptoanaliza urno kontroliranega pomičnega registra,
- Digitalni denar,
- Deljenje skrivnosti,
- Učinkovite implementacije v $\mathbb{Z}_p$,
- Baze binarnih končnih obsegov,
- Normalne baze nizke kompleksnosti,
- Konvolucijske kode,
- Razdaljno-regularni grafi in posplošeni četverokotniki,
- Weilovo parjanje v shemah za šifriranje,
- Čebiševe baze in odprtost na napade s stranskim kanalom,
- Zasebna življenja javnih ključev,
- Sferični t-načrti,

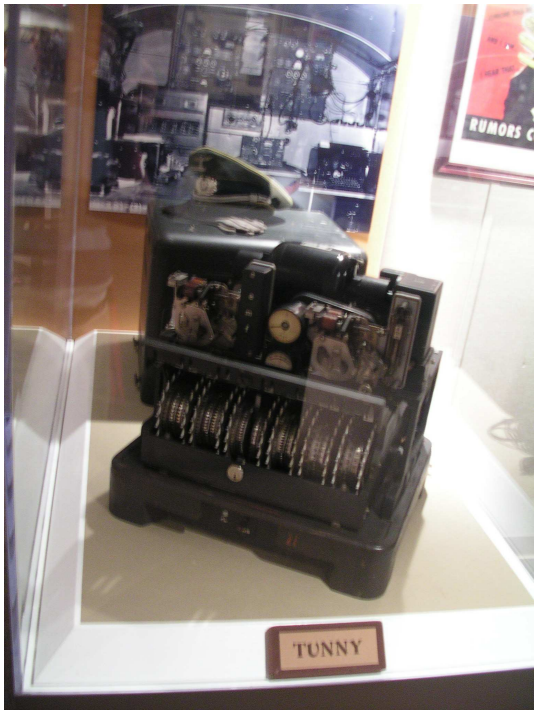
magisterijev in doktoratov:

- Varno poslovanje med različnimi varnostnimi okolji (FRI),
- Analiza bodočih oblik napadov na sistemsko in aplikacijsko infrastrukturo (FRI),
- Celovit sistem za varno izmenjavo podatkov (FE),
- Razdaljno-regularni grafi majhnega diametra (mag.), 1-homogeni grafi brez trikotnikov (doktorska disertacija) (FMF),
- Uporaba Berlekamp-Masseyevega algoritma v kriptografiji in teoriji kodiranja (FMF),
- Pollardova rho-metoda in diskretni logaritem (FMF).

Obisk NSA muzeja.

Koliko jezikov je v rabi danes?





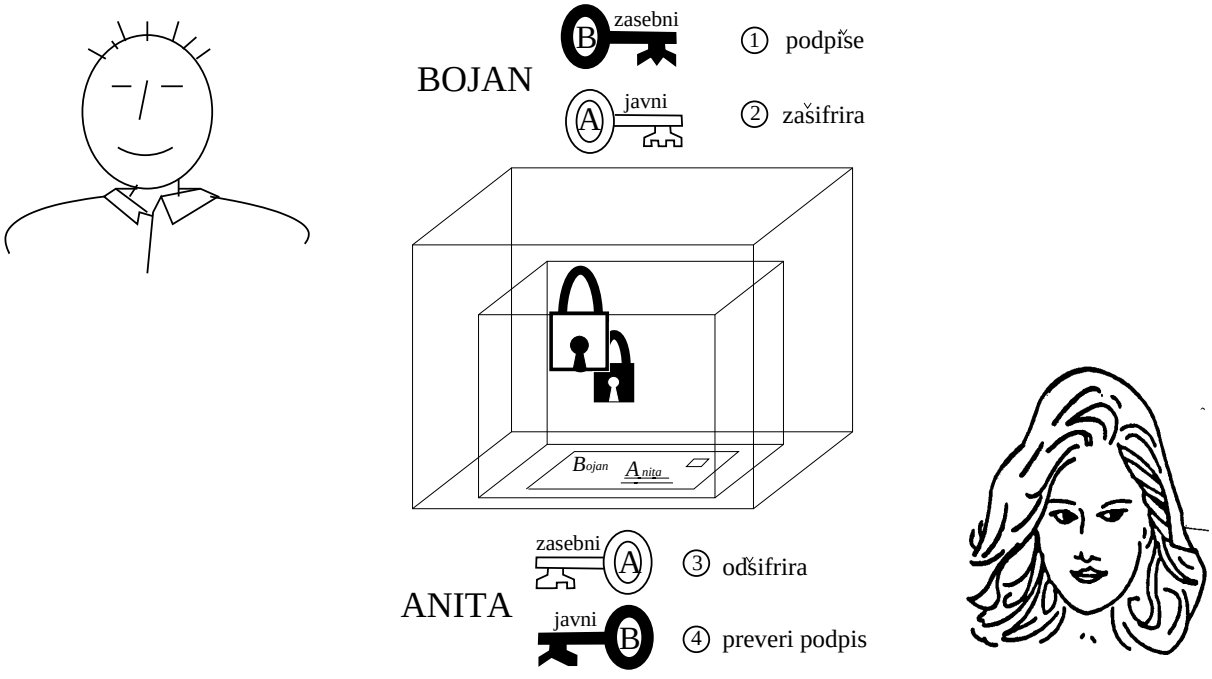
Šifrirna naprava za komunikacijo med nemškim vrhovnim poveljstvom in SS četami (članek “Fish and I” opisuje, kako je matematik W. Tutte razbil to šifro).

Kljub temu, da so sporočilo o napadu razbili pravočasno, pa so Američani doživeli polom.

Kriptoanaliza pa je obrodila sadove v nadaljevanju vojne.

Purple - šifrirna naprava, ki so jo v II. svetovni vojni uporabljali Japonci.

Slednja fotografija pa kaže kako blizu smo tudi z LRA skupino naše fakultete.



Bojanovo ljubezensko pismo prispe varno v Anitine roke.