Sjemenarstvo 16(99)6

UDK: 378.663(045)=862
Izvorni znanstveni rad

OBJEKTNI PRISTUP MODELIRANJU ANALIZE SIGURNOSNOG KRIPTOGRAFSKOG MODELA

K. ANTOLIŠ[1] i V. GRBAVAC[2]

[1]GS OS RH HVU Učilište hrvatske kopnene vojske, Zagreb

[2]Agronomski fakultet Sveučilišta u Zagrebu
Faculty of Agriculture University of Zagreb

SAŽETAK

Analiza kriptograma je problem koji sam po sebi nije trivijalan. U ovom radu, prvo ćemo se pozabaviti jednim primjerom rješavanja jednostavnog kriptograma kako bismo narečenu problematiku i poteškoće u svezi s njom i u praktičnom smislu definirali. Na taj se način detaljnije raščlanjuje cjelokupna problematika, što nas dovodi do koncipiranja osnove predloženog algoritma i pomaže pri dizajniranju jedne prilagodljive arhitekture sustavnog rješavanja problema iz faze analize kriptograma. Time je stvorena mogućnost proširenja domicilne problematike prepoznate u inicijalnom problemu dodavanjem novih funkcionalnosti i zadovoljavanjem novih zahtjeva, te njihovog rješavanja koje će se kao potreba s izrastanjem sigurnosnog sustava zasigurno pojaviti.

1. UVOD

Svjesna bića manifestiraju vrlo složen sustav ponašanja koji potječe od strane uma kroz mehanizme koje tek slabo poznajemo. Na primjer, razmislite kako rješavate problem planiranja rute kroz grad kako biste obavili niz poslova. Također promislite kako, kada hodate kroz slabo osvijetljenu sobu, prepoznajete okvire objekata i izbjegavate spoticanje. Nadalje, sjetite se kako se na zabavi koncentrirate na jedan razgovor dok oko vas mnogo ljudi istodobno govori. Niti za jednu od ovih vrsta problema nije prikladno izravno algoritamsko rješenje. Planiranje optimalne rute kroz grad poznato je kao *np-potpuni* ("np-complete") problem. Orijentiranje na mračnom terenu uključuje razumijevanje na bazi vizualnih ulaznih podataka koji su (sasvim doslovno) nejasni i nepotpuni. Identifikacija jednog govornika pokraj nekoliko desetaka izvora zahtijeva da slušatelj razluči značajne podatke od buke i zatim iz preostale kakofonije izdvoji sav neželjeni razgovor.

Ovdje ćemo se pozabaviti dizajnom jednog inteligentnog sustava koji rješava kriptograme upotrebljavajući tzv. model školske ploče ("blackboard model"), i to na način koji odgovara načinu na koji bi čovjek riješio taj problem. Kao što ćemo vidjeti, upotreba objektno-orijentiranog razvoja pokazati će se vrlo prikladnom.

2. DEFINIRANJE OKVIRA PROBLEMA

Kako je bilo naznačeno u narečenom opisu, baviti ćemo se problemom analize kriptograma, odnosno procesom transformacije šifriranog u obični tekst, ili dešifriranjem. U svojoj najopćenitoj formi, dešifriranje kriptograma jedan je nezgodan problem koji prkosi čak i najsofisticiranijim tehnikama. Na primjer, DES ("data encryption standard" – standard šifriranja podataka, odnosno algoritam šifriranja s povjerljivim ključem koji koristi višestruku primjenu supstitucije i premještanja slova) čini se osiguranim od bilo kakvih matematičkih manjkavosti i kao takav je otporan na bilo kakve trenutno poznate napade. Srećom, naš je problem puno jednostavniji, pošto smo se ograničili na jednostruku supstituciju slova.

Kao dio naše analize, prođimo kroz jedan scenarij rješavanja jednostavnog kriptograma. Utrošite nekoliko narednih minuta na rješavanje sljedećeg problema, te kako napredujete, zabilježite što ste sve pokušali (bez čitanja unaprijed!):

CZLSGBAK MS ADR CZBMB ASM P CLBFSJP

Kao pomoć, navesti ćemo da znak *M* predstavlja obično slovo *Ć*.

Krenuti sada s napornim istraživanjem prilično je nerazborito. Pod pretpostavkom da abeceda u običnom teksta obuhvaća 30 velikih štampanih slova, slijedi da postoji ukupno 30! (oko 2.65×10^{32}) mogućih kombinacija. Iz tog razloga moramo pokušati nešto drugo osim upotrebe gole sile. Alternativna tehnika je napraviti jednu pretpostavku na temelju našeg poznavanja rečenica, riječi i slova, te zatim nastaviti linijom te pretpostavke do njenih logičkih zaključaka. Kada u jednom trenutku više nećemo moći napredovati, odabrati ćemo sljedeću obećavajuću pretpostavku koja se veže na prethodnu, i tako dalje, sve dok nas svaka uzastopna pretpostavka vodi bliže rješenju. Ako uvidimo da smo zaglavili, ili ako smo donijeli zaključak koji je u suprotnosti s nekim od prethodnih zaključaka, moramo se vratiti i promijeniti neku od ranijih pretpostavki.

Evo našeg rješenja, s prikazom rezultata svakog koraka:

1. U skladu s navedenom pomoći, možemo direktno zamijeniti *M* sa slovom *Ć*.

CZLSGBAK ĆS ADR CZBĆB ASĆ P CLBFSJP

2. Druga je riječ kratka i počinje s *Ć*, tako da je to najvjerojatnije pomoćni glagol *ĆE*.

CZLEGBAK ĆE ADR CZBĆB AEĆ P CLBFEJP

3. Iz gramatike znamo da negdje iza tog glagola mora doći još jedan glagol i to u infinitivu. Čini se da je vjerojatno u pitanju četvrta riječ.

CZLEGIAK ĆE ADR CZIĆI AEĆ P CLIFEJP

4. Šesta riječ je jednoslovna. Pošto smo *E* i *I* već upotrijebili, ostaju nam *O*, *U* i *A*. Pretpostavimo da je to *O*.

CZLEGIAK ĆE ADR CZIĆI AEĆ O CLIFEJO

5. Četvrta je riječ obrasca *??IĆI*. Potraga za mogućim kombinacijama polučuje *OTIĆI*, *OBIĆI* i *STIĆI*. Pošto smo *O* već iskoristili, preostaje nam samo *STIĆI*.

STLEGIAK ĆE ADR STIĆI AEĆ O SLIFEJO

6. Posljednja riječ je obrasca *S?I?E?O*. Potraga za rješenjima daje *SVIREPO*, *SMIRENO* i *SVILENO*. Niti jedna od tih riječi nema smisla u rečenici, tako da nam zaključujemo da smo ranije donijeli neku krivu pretpostavku. Čini se da je problem u šestoj riječi, pa tako ovog puta pokušajmo s *U*.

CZLEGIAK ĆE ADR CZIĆI AEĆ U CLIFEJU

7. Sada pada u vodu i nemogućnost da četvrta riječ započinje s *O*. Pretpostavimo stoga da je četvrta riječ *OTIĆI*.

OTLEGIAK ĆE ADR OTIĆI AEĆ U OLIFEJU

8. Potraga za riječima koje odgovaraju obrascu *O?I?E?U* otkriva riječ *ODIJELU*. No to bi značilo da prva riječ započinje s *OTD* što nema smisla, jer između *T* i *D* mora doći bar jedan samoglasnik. Stoga zaključujemo da četvrta riječ ne može sadržavati *O*, pa nam opet preostaje samo *STIĆI*.

STLEGIAK ĆE ADR STIĆI AEĆ U SLIFEJU

9. Sada smo dobili *S?I?E?U*. Poznavanje gramatike nam nalaže da to mora biti imenica, te s isključivanjem već iskorištenih slova dobivamo *SLIJEDU*, *SRIJEDU*, *SMIRENJU*, *SNIJEGU* i *SPIKERU*. Razabiremo da uvrštavanje jedino riječi *SRIJEDU* ima smisla.

STREGIAK ĆE ADR STIĆI AEĆ U SRIJEDU

10. Peta riječ u ovim okolnostima može biti jedino *VEĆ*.

STREGIVK ĆE VDR STIĆI VEĆ U SRIJEDU

11. Treća riječ je troslovna i prvo joj je slovo *V*. To je najvjerojatnije *VAM*.

STREGIVK ĆE VAM STIĆI VEĆ U SRIJEDU

12. Preostala riječ sada može biti samo *STRELJIVO* ili *STRELJIVA*. *A* je već iskorišteno, tako da konačno rješenje glasi:

STRELJIVO ĆE VAM STIĆI VEĆ U SRIJEDU

I tako smo došli do rješenja. Možemo dati sljedeća tri zapažanja glede navedenog procesa rješavanja problema:

- Koristili smo mnoge različite izvore znanja, kao što su znanja gramatike, pravopisa i samoglasnika.
- Zabilježili smo naše pretpostavke na jednom središnjem mjestu i primijenili naše izvore znanja na ove pretpostavke kako bismo donijeli odgovarajuće zaključke.
- Rasuđivali smo na oportunistički način. U nekim smo slučajevima zaključivali od općih prema posebnim pravilima (na primjer, ako riječ ima dva slova i počinje s Ć, onda je to vjerojatno *ĆE*), a u drugim slučajevima od posebnih prema općim (*S?I?E?U* bi moglo biti više riječi, no kao imenica koja ima smisla jednio *SRIJEDU* zadovoljava našu hipotezu).

Ovo što smo opisali je pristup rješavanju problema nazvan model školske ploče. Model školske ploče prvi je objavio Newell 1962. godine, a kasnije je objedinjen od strane Reddy-ja i Ermana u projekte Hearsay i Hearsay II, od kojih se obadva bave problemom prepoznavanja govora. Model školske ploče ispostavio se korisnim u ovom području i taj je sustav ubrzo bio uspješno primjenjen i u drugim poljima, uključujući interpretaciju signala, modeliranje trodimenzionalnih molekularnih struktura, razumijevanje slika i planiranje. Sustavi na bazi školske ploče pokazali su se osobito vrijednim pažnje u svezi s predstavljanjem deklarativnog znanja, te su prostorno i vremenski učinkoviti u usporedbi s alternativnim pristupima.

Sustav školske ploče zadovoljava našu ranije razmatranu definiciju sustava. Stoga možemo kodificirati njegovu arhitekturu u smislu skupa razreda i mehanizama koji opisuju način na koji objekti iz tih razreda surađuju.

3. ZAHTJEVI ANALIZE KRIPTOGRAMA

Kriptografija "obuhvaća metode za pravljenje podataka nerazumljivim neovlaštenim stranama". Koristeći kriptografske algoritme, poruke (običan tekst) mogu se pretvoriti u kriptograme (šifrirani tekst) i obratno.

Jedna od najosnovnijih vrsta kriptografskih algoritama, u uporabi od vremena starih Rimljana, zove se *supstitucijsko šifriranje*. S ovim šifriranjemm, svako je slovo iz obične abecede dovedeno u vezu s nekim drugim slovom. Na primjer, mogli bismo zamijeniti svako slovo sa sebi narednim slovom: *A* postaje *B*, *B* postaje *C*, *Ž* radi krug i postaje *A*, i tako dalje. Na taj način, običan tekst

CLOS je primjer objektno orijentiranog programskog jezika

može biti šifriran u kriptogram

DMPT kf rsjnkfs pckflunjp psjkfnjujsbnjph rsphsbnšlph kfžjlb

Supstitucija slova je najčešće rađena na preskoke. Na primjer, *A* postaje *G*, *B* postaje *J*, i tako dalje. Kao primjer, promotrite sljedeći kriptogram:

ZBSNHK TA PA CKMDKSN LF LFSBAJN

Pomoć: ovdje šifrirano slovo *B* predstavlja obično slovo *R*.

Uvelike je pojednostavljujuća pretpostavka smatrati da je korišteno samo supstitucijsko šifriranje pri kodiranju poruke. Usprkos tome, dešifriranje nastalog kriptograma nije algoritamski trivijalan zadatak. Dešifriranje ponekad zahtijeva pokušaje i pogreške, pri čemu radimo pretpostavke o pojedinoj supstituciji a zatim procijenjujemo njihove implikacije. Na primjer, možemo započeti s jednoslovnim i dvoslovnim riječima u kriptogramu i postaviti hipotezu da one stoje umjesto uobičajenih riječi kao što su *i* i *a*, ili *ja*, *mi*, *se*, *li*, *da*, i *na*. Supstituirajući ostale slučajeve pojavljivanja ovih šifriranih slova, možemo primijetiti mogućnosti za dešifriranje drugih riječi. Na primjer, ako postoji riječ od tri slova koja započinje s *t*, ta bi riječ lako mogla biti *tri*, *taj*, ili *tog*.

Također možemo iskoristiti i naše poznavanje pravopisa i gramatike kako bismo pokušali riješiti supstitucijsku šifru. Na primjer, pojavljivanje dvostrukog slova vjerojatno predstavlja niz *jj*, uobičajen kod formiranja superlativa nekih pridjeva. Na sličan način, mogli bismo pokušati proširiti riječ koja završava sa slovom *i* sufiksom *iti* ili *ati*. Na najvišoj razini apstrakcije, mogli bismo pretpostaviti da je vjerojatnija pojava slijeda riječi *da se* nego slijeda *da ju*. Također, mogli bismo pretpostaviti da struktura rečenice tipično uključuje po jednu imenicu i glagol. Stoga, ako smo u našoj analizi identificirali glagol, ali ne i vršioca radnje, mogli bismo početi tražiti pridjeve i imenice.

Ponekad se moramo i vratiti unatrag. Na primjer, mogli smo pretpostaviti da je određena dvoslovna riječ bila *se*, ali ako supstitucija slova *s* uzrokuje kontradikcije ili bezizlazne situacije kod drugih riječi, onda bismo mogli pokušati s riječju *bi* ili *ja*, i uz to poništiti ostale pretpostavke bazirane na ovoj ranijoj supstituciji.

Ovo nas vodi k zahtjevu za naš problem: osmisliti jedan sustav, koji prevodi kriptogram natrag u svoj prvobitni sadržaj, pod pretpostavkom da se koristila samo jednostavno supstitucijsko šifriranje.

4. ARHITEKTURA SUSTAVA ŠKOLSKE PLOČE

Englemore i Morgan pojašnjavaju model školske ploče analogijom na problem grupe ljudi koja rješava slagalicu ("jigsaw puzzle")[14]:

> Zamislite prostoriju s velikom školskom pločom i grupom ljudi oko nje od kojih je svatko u posjedu više dijelova slagalice. Započinjemo time da dragovoljci stavljaju na ploču (pretpostavimo da je ljepljiva) svoje dijelove koji "najviše obećavaju". Svaki član grupe gleda u svoje dijelove i provjerava da li se bilo koji od njih podudara s dijelovima koji se već nalaze na ploči. Oni s odgovarajućim dijelovima dolaze do ploče i ažuriraju nastajuće rješenje. Novi dodaci uzrokuju situaciju da neki drugi dijelovi sada nalaze svoje mjesto, pa tako ostali ljudi dolaze do ploče te ih postavljaju. Nije važno da li je pojedina osoba u posjedu više dijelova od neke druge. Cijela se slagalica može riješiti u potpunoj tišini, odnosno ne postoji potreba za direktnom komunikacijom unutar grupe. Svaka se osoba sama pokreće, prepoznajući kada njeni dijelovi mogu doprinijeti ukupnom rješenju. Ne postoji apriorno određeni redoslijed kojim ljudi dolaze do ploče. Do kooperativnog ponašanja dolazi uslijed stanja u kojem se nalazi rješenje na ploči. Ako se promatra izvođenje zadatka, do rješenja se dolazi dodavanjem (po jednog dijela u svakom trenutku) i na oportunistički način (kako se pojavljuje mogućnost za postavljanje još jednog dijela). Nasuprot tome je, na primjer, način da sustavno krenemo od gornjeg lijevog kuta i isprobavamo svaki dio.

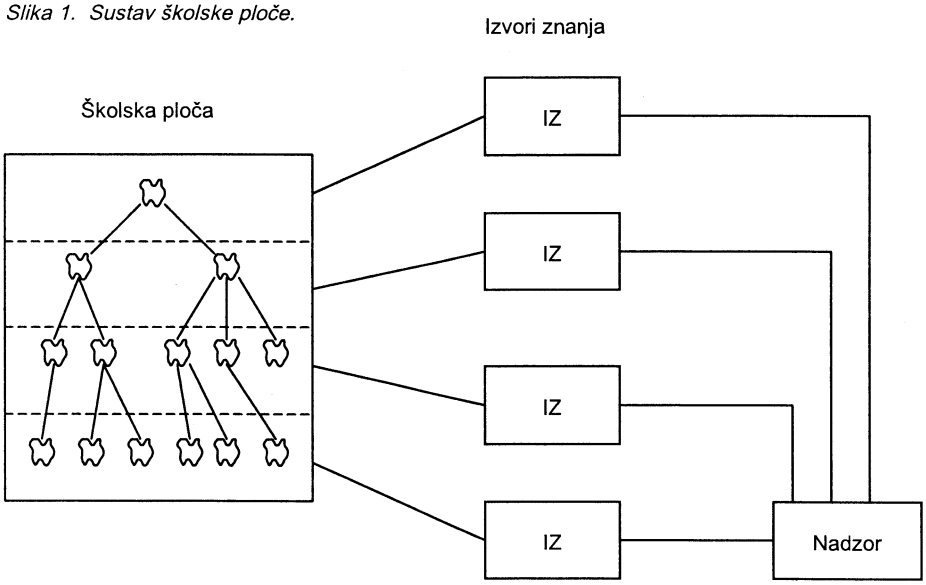
Kao što slika 1. nalaže, sustav školske ploče sastoji se od tri elementa: školske ploče, višestrukih izvora znanja, i upravljača koji povezuje i posreduje između spomenutih izvora znanja. Primijetite kako sljedeći opis odgovara principima objektnog modela. Shodno Nii-ju, "svrha školske ploče jest da sadržava računske podatke i podatke o stanju rješenja pribavljenih od strane izvora znanja i potrebnih tim istim izvorima znanja. Školska se ploča sastoji od objekata iz prostora rješenja. Objekti na ploči hijerarhijski su organizirani u razine analize. Objekti i njihova svojstva definiraju vokabular prostora rješenja".

Kao što Eaglemore i Morgan pojašnjavaju, "Područje znanja potrebnog za rješavanje problema je podijeljeno u izvore znanja koji se drže razdvojenim i

neovisnim. Cilj svakog izvora znanja je ponuditi informaciju koja će voditi ka rješenju problema. Izvor znanja uzima skup trenutnih informacija s ploče i ažurira ga shodno svojem specijaliziranom znanju. Izvori znanja predstavljeni su kao procedure, skupovi pravila ili logičkih tvrdnji".

Izvori znanja, ili kraće IZ-i, obuhvaćaju specifično područje. U sustavima prepoznavanja govora, izvori znanja mogli bi uključiti entitete koji su sposobni zaključivati o fonemima, riječima i rečenicama. U sustavima prepoznavanja slika, izvori znanja bi uključili entitete koji poznaju jednostavne elemente slika, kao što su rubovi i područja slične građe, kao i elemente viših razina koji predstavljaju interesantne objekte s raznih krajolika, kao na primjer kuće, ceste, polja, automobile, ljude ili neprijateljska vozila i vojni aspekt opreme.

Slika 1. Sustav školske ploče.



Općenito govoreći, izvori se znanja podudaraju s hijerarhijskom strukturom objekata na školskoj ploči. Nadalje, svaki izvor znanja koristi objekte jedne razine kao svoj ulaz, a zatim kreira i/ili modificira objekte druge razine kao svoj izlaz. Na primjer, u sustavu prepoznavanja govora, izvor znanja koji objedinjava znanje o riječima mogao bi promotriti niz fonema (niža razina svojstava) kako bi formirao novu riječ (viša razina). Alternativno, izvor znanja koji sadrži znanje o strukturi rečenica, mogao bi hipotetizirati potrebu za jednim glagolom (visoka razina), i filtriranjem liste mogućih riječi (niža rizina) ovaj bi izvor znanja provjerio tu hipotezu.

Ova dva pristupa zaključivanju predstavljaju povezivanje unaprijed i povezivanje unatrag. Povezivanje unaprijed uključuje zaključivanje od specifičnih do opće tvrdnje, a povezivanje unatrag započinje s hipotezom, a zatim pokušava provjeriti tu hipotezu pomoću postojećih tvrdnji. Upravo zato kažemo da je kontrola u modelu školske ploče oportunistička. Ovisno o okolnostima, neki izvor znanja izabran za aktivaciju koristi povezivanje ili unaprijed ili unatrag.

Izvori znanja obično utjelovljuju dva elementa, a to su prvotne okolnosti i aktivnosti. Prvotne okolnosti izvora znanja predstavljaju stanje na školskoj ploči za koje je taj izvor znanja zainteresiran. Na primjer, prvotna okolnost za neki izvor znanja u sustavu raspoznavanja slika mogla bi biti prepoznavanje relativno linearnog područja elemenata slike (moguće prikazujući cestu). Iniciranje prvotne okolnosti uzrokuje da izvor znanja usredotoči svoju pažnju na taj dio školske ploče i zatim krene u akciju obradom svojih pravila ili proceduralnog znanja.

U takvim okolnostima, konzultiranje mišljenja nije potrebno, što znači da kada pojedini izvor znanja smatra da može ponuditi nešto interesantno, on o tome izvješćuje upravljača školske ploče. Figurativno govoreći, to je kao kada bi svaki izvor znanja podigao svoju ruku kako bi pokazao da može nešto korisno napraviti, a upravljač poziva onoga koji se čini da najviše obećava.

5. ANALIZA IZVORA ZNANJA

Vratimo se sada na naš specifični problem, i razmislimo o izvorima znanja koji bi mogli doprinijeti rješenju. Kao što je i tipično za većinu aplikacija s osmišljenim znanjem, najbolja strategija je sjesti kraj jednog stručnjaka u tom području i zabilježiti interesantne metode kojima se on služi kako bi riješio probleme iz svoje domene. U svezi našeg trenutnog problema, to bi moglo značiti da pokušamo riješiti nekoliko kriptograma i da zabilježimo naše razmišljanje tokom samog postupka rješavanja.

Naša analiza pokazuje da je trinaest izvora znanja od važnosti, i oni su navedeni skupa sa znanjima koja utjelovljuju u sljedećoj listi:

- Uobičajeni prefiksi — Uobičajeni početni dijelovi riječi, kao što su *pod*, *anti* ili *pred*.
- Uobičajeni sufiksi — Uobičajeni završeci riječi, kao što su *lac*, *telj*, *ar*, *inja* ili *stvo*.
- Suglasnici — Slova koja nisu samoglasnici.
- Direktna supstitucija — Pomoći navedene kao dio problema.
- Dvostruka slova — Uobičajena dvostruka slova, kao što je *jj*.
- Učestalost slova — Vjerojatnost pojavljivanja svakog slova.

• Važeći nizovi	Važeće i nevažeće kombinacije slova, kao što su *st* i *nd*.
• Podudaranje obrazaca	Riječi koje odgovaraju određenom obrascu slova.
• Struktura rečenice	Gramatika, uključujući značenja raznih fraza.
• Kratke riječi	Moguća rješenja za riječi duljine od jednog do četiri slova.
• Riješeno	Da li problem jest ili nije riješen, ili ako daljnji napredak nije moguć.
• Samoglasnici	Slova koja nisu suglasnici.
Struktura riječi	Položaj samoglasnika i uobičajena struktura imenica, glagola, pridjeva, zamjenica, priloga, prijedloga, veznika i tako dalje.

Ove izvore znanja možemo također urediti u jednu hijerarhiju. Konkretno, neki izvori znanja djeluju na osnovi rečenica, drugi na osnovi riječi, a treći na osnovi grupe susjednih slova, dok izvori znanja najniže razine djeluju na osnovi zasebnih slova. I zaista, ova hijerarhija odražava objekte koji bi se mogli pojaviti na ploči: rečenice, riječi, nizovi slova i pojedinačna slova.

6. ZAKLJUČAK

Iako je naš objektno orijentirani pristup analizi inauguriran u ovom radu uključivao i izvođenje brojnih pokušaja i promašaja, kao i promatranje proceduralnih postupaka stručnjaka iz ove problemske domene, na kraju je ipak ostvaren uspjeh. U radu je na adekvatan način formulirana jedna polazna osnova na čijim se temeljima može pristupiti dizajniranju jednog učinkovitog objektno orijentiranog sustava rješavanja kriptograma. Vidljivo je odvajanje funkcija označenih kao potrebitih za rješavanje kriptograma u zasebne cjeline, što temeljno čini našu analizu objektno orijentiranom. Brojne su prednosti takvog pristupa, što se lako može iščitati iz same činjenice da je moguće relativno jednostavno prilagoditi listu pobrojanih ključnih elemenata i svojstava našeg sustava nekom novom kriteriju ili dodatnim zahtjevima bez da bitnije utječemo na bilo koji od već formiranih čimbenika našeg modela u razvoju. Izvedba bi u takvom slučaju najvjerojatnije obuhvaćala adaptaciju pojedinog izvora znanja i njegovih pravila novonastaloj situaciji ili pak dodavanje novog izvora znanja sa specifičnim znanjima neophodnim za zadovoljavanje pridodanog uvjeta. Sve narečeno govori o važnosti strukturiranja u radu prezentiranog objektno orijentiranog pristupa modeliranju analize sigurnosnog kriptografskog modela.

OBJECT-ORIENTED APPROACH TO CRYPTOGRAPHIC SECURITY MODEL ANALYSIS MODELING

SUMMARY

Cryptanalysis is a problem that is not trivial by itself. In this work, we will first tackle an example of a simple cryptogram in order to practically define the described problem-domain along with its difficulties. Thus the overall problem-domain gets to be analysed, which leads us to the conception of the suggested algorithm basis and helps us with the design of an elastic systematic problem-solving architecture from the analysis phase. By that means a possibility of extending the problem-domain, recognized in the initial problem, is being offered through adding of new functionalities and meeting of new requirements, as well as their solving, which will inevitably arise as a need with the security system development.

7. LITERATURA - REFERENCES

1. Adam Blum, "Neural Networks in C++", John Wiley & Sons, New York 1992.
2. Andrzej Lasota, Michael C. MacKey : Chaos, Fractals, and Noise : Stochastic Aspects of Dynamics (Applied Mathematical Sciences, Vol 97) / Published 1994.
3. Antoliš K. et al : Razvitak infosustava i umjetne inteligencije u prometnoj medicini, 6. međunarodno znanstveno savjetovanje "Tehnika i logistika prometa, Opatija, 1998.
4. Arthur M. Langer : The Art of Analysis / Published 1997.
   Coad, P. Yourdon E.: Object-oriented analysis, Prentice Hall, Englewood Cliffs, N.J., 1990.
5. Craig Larman : Applying Uml and Patterns / An Introduction to Object-Oriented Analysis and Design / Published 1997.
6. D. Mišljenović, I. Maršić, "Umjetna inteligencija", Školska knjiga Zagreb 1991.
7. David R. C. Hill : Object-Oriented Analysis and Simulation Modeling / Published 1996.
8. Derek Coleman, et al : Object-Oriented Development : The Fusion Method (Prentice-Hall Object-Oriented Series) / Published 1994.
9. Edward Yourdon, Carl A. Argila: Case Studies in Object-Oriented Analysis and Design (Yourdon Press Computing Series) / Published 1996.
10. Grbavac V. et al : The concept of info function model in complex organisational system, Informatologija, 1998.
11. Grbavac V. et al : Ekspertni sustavi u funkciji razvoja prometa, IESP '96. Ljubljana, 1996.
12. Hugh Beyer, Karen Holtzblatt: Contextual Design: A Customer-Centered Approach to Systems Designs / Published 1997.
13. Jeffrey A. Hoffer, et al: Modern Systems Analysis and Design / Published 1996.
14. Kumpati S. Narendra, Kannan Parthasarathy, "Identification and Control of Dynamical Systems Using Neural Networks", IEEE Transactions on Neural networks, VOL. 1. No. 1. March 1990.
15. Kim Walden, Jean-Marc Nerson: Seamless Object-Oriented Software Architecture : Analysis and Design of Reliable Systems (The Object-Oriented) / Published 1995.

16. Methods Jeffrey L. Whitten, et al : Systems Analysis and Design / Published 1997.
17. Peter Coad, Edward Yourdon : Object Oriented Design (Yourdon Press Computing Series) / Published 1991.
18. Richard A. Layton : Principles of Analytical System Dynamics (Mechanical Engineering Series) / Published 1998.
19. Robert B. Angus et al: Planning Performing and Controlling Projects: Principles and Applications / Published 1997.
20. Ronald J. Norman: Object-Oriented Systems Analysis and Design (Prentice Hall Series in Information Management) / Published 1996.

Adresa autora – Authors' address:
Dr. sc. Krunoslav Antoliš
GS OS RH HVU Učilište hrvatske kopnene vojske
HR - 1000 Zagreb
Prof. dr. sc.Vitomir Grbavac
Agronomski fakultet Sveučilišta u Zagrebu
Svetošimunska 25
HR - 1000 Zagreb

Primljeno – Received:
20. 11. 1999.