Od Cezara do standarda DES

DRAGAN PLESKONJIĆ, dipl. ing.

Možda vam se već ukazala potreba da neke svoje datoteke odnosno njihov sadržaj sakrijete od tuđih znatiželjnih očiju ili potreba da druge sprečite da izvršavaju neke vaše programe. Možda ste nekada na disketi ili linijom za prenos podataka želeli poslati nekome poruku, program, podatke, pismo i onda se pojavila opasnost da te podatke pročita neko nepoželjan. Ako ste profesionalni programer i strahujete da bi vam neko mogao uzeti izvorni kod programa koji želite plasirati na tržište, takođe vam treba zaštita.

Problem je, može se reći, star isto kao i ljudska pismenost. Još kod starih Egipćana i Grka ukazivala se potreba da se pisani tekstovi i poruke drže u strogoj tajnosti. Vojskovođe su morale u tajnosti držati planove ratnih operacija, naučnici i pronalazači svoja otkrića, ljubavnici pisma. Danas takođe sve ove stvari dobijaju na značaju. Poruke koje izmjenjuju vlade, diplomatska predstavništva, poslovne organizacije, moraju biti zaštićene. Takođe je nužno zaštititi podatke koje filijale banaka izmjenjuju sa centrom itd. Moglo bi se nabrojati još puno situacija gde se ukazuje potreba za zaštitom.

U svim ovim situacijama poruke, podaci, programi se mogu zaštititi šifrovanjem. **Šifrovanje** je postupak pri kom se uz pomoć nekog algoritma (šifarskog sistema) tekst transformiše iz otvorenog (razumljivog) oblika u šifrovani tekst. Šifrovani tekst je nerazumljiv za sve one kojima nije namenjen. Da bi se tekst ponovo doveo u razumljivi oblik potrebno je izvršiti inverznu transformaciju, **dešifrovanje**. Šifrovanje i dešifrovanje se obavljaju uz pomoć **ključa** koji određuje postupak i koji je tajni podatak (osim kod nekih novijih metoda kod kojih postoji i javni ključ).

i vojskovođe (Cezar, Karlo Veliki, Napoleon) i mnogi drugi. Neke starije metode mogu i danas efikasno zadovoljiti skromnije potrebe, dok se za potrebe veće sigurnosti stalno stvaraju novi algoritmi sa sve boljim osobinama. To je borba između kriptografa (onih koji šifarske sisteme razvijaju) i kriptoanalitičara (onih koji te sisteme »razbijaju«), borba kojoj se kraj ne nazire.

Kod izbora algoritma za šifrovanje moramo imati u vidu stepen sigurnosti koji želimo postići, cenu koju možemo platiti (u cenu će u ovom razmatranju biti uračunato vreme pravljenja programa za šifrovanje i vreme trajanja procesa šifrovanja i dešifrovanja). U ozbiljnijim namenama moraju se uzeti u obzir obuka ljudstva, dodatni specijalizovani hardver i softver, opterećenje prenosnih puteva izazvano povećanjem količine podataka koji se prenose (linija za prenos podataka) itd.

Većinu šifarskih sistema možemo grupisati u jednu od dve grupe:
- šifre premještanja (transpozicije)
- šifre zamjene (supstitucije)
- kombinacije zamjene i premještanja.

Šifre premještanja su one kod kojih se šifrovani tekst dobija tako što se prema određenom pravilu promjeni redosled znakova (slova) otvorenog (izvornog) teksta.

Šifre zamjene su takve kod kojih se znakovi u izvornom tekstu zamjenjuju drugim znakovima, prema nekom pravilu. Ta zamjena može biti:
- prosta zamjena, isto slovo se uvek zamjenjuje istim znakom
- složena zamjena, zamjena nije ista i zavisi o ključu.

Stariji šifarski sistemi

Prapočetkom kriptografije može se smatrati staroegipatski »instrument« skital. To je u suštini jedan štap oko koga se obmota papirna traka. Poruka se piše odozgo nadole niz štap u nekoliko stupaca, a nakon toga se traka odmota sa štapa. Na traci je tada nerazumljiv niz znakova. Ključni podatak je prečnik štapa oko koga treba traku obmotati. Šifarski sistem spada u grupu šifara premještanja, jer se u suštini sastoji od istih znakova od kojih i izvorna poruka samo što su drukčije raspoređeni. Ima samo istorijski značaj.

Sledeći značajan metod je takozvani **Cezarov sistem**. Pripisuje se rimskom imperatoru Juliju Cezaru. Šifrovanje se izvodi tako što se ispišu sva slova alfabeta, a zatim se ispod njih ispišu takođe sva slova, ali počevši od nekog proizvoljnog slova. Kada se dođe do zadnjeg slova, onda se prelazi na početak. Ključni podatak je slovo od koga počinje donji alfabet.

Primer:

Prvo definišemo zamjenu:

```
A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž
D Đ E F G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć
```

Neka je otvoreni tekst: MIKRORAČUNAR.

Šifrovano to je: SNPVTVDFBŠDV.

Napomena: Dvostruki simboli DŽ, LJ i NJ posmatraju se kao dva odvojena slova.

Može se odabrati bilo koji redosled slova u donjem alfabetu. Obično se uzima neka reč ili fraza kao ključ, i ona se ispiše od neke pozicije (pošto se prethodno izbace ista slova), a zatim se ispišu ostala slova alfabeta kao kod prethodnog primera.

Primer:

Neka je ključ reč TAJNOVITOST što postaje TAJNOVIS kad se izbace slova koja se ponavljaju:

```
A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž
R Š U Z Ž T A J N O V I S B C Č Ć D Đ E F G H K L M P
```

Otvoreni tekst KOMPJUTER postaje BDČĐSKHJE.

Može se uzeti i numerički ključ. Npr. neka je ključ niz cifara: 1203542.

Otvoreni tekst KRIPTOGRAFSKE METODE.

Ključ 1203542120354 212035.

Šifrirani tekst LŠIŠAŠISCFUPI OFVOFJ.

Objašnjenje: Ako npr. određenoj slovu otvorenog teksta odgovara c fra 2, tada se ono menja slovo koje je po abecedi drugo iza to slova. Tako je u gornjem primer slovo G zamenjeno slovom I koje drugo iza slova G po abecedi itd.

Vižnerov metod. Kod ovog met da ključ se sastoji od d simbola (= 1,2...). Ako se slovima alfabet daju numeričke vrednosti A=0, B= itd., tada se ključ piše ispod poruk i sabiraju se pojedinačno simboli poruke i ključa modulo 30 (broj sim bola u alfabetu poruka). Tako je fo mula za svaki šifarski simbol:

e = m + k (mod 30).

Ukoliko ključ ima samo jeda simbol, Vižnerov metod prela u već opisani Cezarov metod. Jeda specijalni slučaj Vižnerovog metod je i takozvani Beaufort sistem. Ko

```
A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž
B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž A
C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž A B
Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž A B C
Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž A B C Č
D Đ E F G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć
Đ E F G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć D
E F G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ
F G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E
G H I J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F
H I J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G
I J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H
J K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I
K L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J
L M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K
M N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L
N O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M
O P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N
P R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O
R S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P
S Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R
Š T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R S
T U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R S Š
U V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R S Š T
V Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U
Z Ž A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V
Ž A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z
A B C Č Ć D Đ E F G H I J K L M N O P R S Š T U V Z Ž
```

Njega je formula za svaki šifarsk simbol:

e = k − m (mod 30)

e = m − k (mod 30).

Šifrovanje se izvodi na sledeć način:

1. Formira se tabela
2. Odabere se ključ – neka to u ovom primeru bude reč KLJUČ.

otvoreni tekst → šifrovanje → šifrovani tekst → dešifrovanje → otvoreni tekst

Znači, da bismo svoj tekst zaštitili, potrebno je odabrati odgovarajući algoritam šifrovanja i ključ. Ključ je tajni podatak koji će znati samo oni koji imaju pravo uvida u podatke (poruku, program), dok algoritam može biti poznat svima. Za neke namene dobro je držati u tajnosti i algoritam jer se time postiže veća sigurnost. Ako onaj ko želi doći do tajnih podataka sazna oba podatka (algoritam i ključ), podaci će biti otkriveni. Znači, zahteva se poseban dogovor između zainteresovanih oko rukovanja ključem, tj. njegovog čuvanja u tajnosti.

Postoje brojni razrađeni algoritmi šifrovanja. Njihov razvoj je tekao od davnih vremena i u njemu su učestvovali veliki naučnici (npr. Leone Batista Alberti, Vižner (Vigenère), Turing, Rivest, Šamir, Adleman)

```
n;(G/.;i=?&2370:"e7i9.;376g13:I==2/.;i<?&A3716.&023<a/3i376)7i2<+.
n<<m6C3<;C0;/50m6e8.+;0/n96ž&'<81m77A=0o3&B*g:0?58=.csn6:a0ž>.Ba18
>+6a5ž27.%&:2gž6eA9(?5&<<26#4ž,0yaC507&e.A.3e7i.31=i2-.92sm&355,ž,
 .n8:<#*<3(0*e76(A&2/=0K,.n0,;*/7wg"a4A76C*qn<=6a8Ci6;*e989649750m4
&;8g17&=;<-+&i4.<9Ci0m"3/50A*C92gH,4:8=./e;*;2.&B2E8*e2>/&aD2gž64<
2g=00CD(C"17i+.a5=<;6(3Ci*6-/n467*e8.g6a)/7(ža:n<92%.I=<="%<3,a)/i
6/&?0.+2a870<?/4A=g=0)/=(8"s=2?*B36g=*8;*sm4D.E./8B?6m/.8.gž"2=i:A
&0:8g:0,CvD;08Bi.<..:*57"eH7(;+&zi=2>e8.gž5;=;090e7i12%&<i7?0':.4š
*žugG/&<3,m.4..g10B7i<m3:9.g</.6i2<+.;*g;*/3i5..*<3,;0s*AB.182=<a/
3i:A0,/i+.a83i56a0ž*37&;7i0m748<2<74J.sm14:2tA*C/;0m/.n*35&27G(?*e
<2:Ba:A=9B?&D*36a)/i:2a5=C(/";3i5.60=62<+&n<,m1736(m(7L46:a3/C0C"e
p49619=564*//ku3405,:a/3i12n)<8:A";/7m,&98gž"8B*=65.n96?60Ci2<+:nF
,m4&;8g<71/DD2/.>;0:"1/,g:0B7i+.a5ž8E65&n2g?"?C6,4ž+(m4*n;(ž11/6:.
-&n2A:&ACi6;*-n467*eA>gA3&5*36a?/+,G#*276H>:n961"9/4(m*e=705a0=30m
4:n=<m#*H+,1/4A=gB(7=)(C"r:2um;/4(m/4D*g4&33;(0*//i2?*5B83<(&n>=2,
e8.g6;3=?(m149>B.n;/5(m%&n99</&J.gH*+ž>g80//i:2a33i)6a2=03.a5ž8=.-
 .B2um;34)6a83ug:&AC=0:me<*B9"e<.2.a4I=9<62<*g4-&D*g80/=3g/*e>;6C"1
/>:=&1/w
```

3. Napiše se otvoreni tekst i ispod njega ključ.

Neka je otvoreni tekst:

OVU PORUKU TREBA PRENETI HITNO I U TAJNOSTI.
KLJ UČKLJU ČKLJU ČKLJUČK LJUČK L J UČKLJUČK.

Prvo slovo otvorenog teksta je O, dok je prvo slovo ključa K. U tablici, u preseku kolone O i vrste K nalazi se slovo Č i to je prvo slovo šifrata. Nastavljajući ovaj postupak šifruje se cela poruka. U ovom slučaju šifrovana poruka glasi:

ČIF LSDHZR ZDŠKU ŠDŠBČZV VUPRČ Z F PČZČCNZ.

Dešifrovanje je jednostavno:

Ispiše se šifrovani tekst i ispod njega ključ, pronađe vrsta u kojoj se nalazi slovo ključa, u toj vrsti se pronađe slovo šifrata i na vrhu (ili dnu) te kolone je slovo otvorenog teksta.

Autošifrovanje. Ukoliko se želi izbeći glavni nedostatak ovog metoda – konačna dužina ključa – to se efikasno postiže takozvanim autošifrovanjem. Autošifrovanje se izvodi na sledeći način: ispiše se otvoreni tekst, a ispod njega prvo se ispiše ključ pa se onda ponavlja sam otvoreni tekst. Nakon toga se izvrši šifrovanje. Loša strana je ta što nehotična greška u šifrovanju može daljnji tekst učiniti potpuno nerazumljivim.

Kombinovani Vižnerov sistem. To je Vižnerov sistem sa višestrukim ključevima, formula za njega je:

e = m + k + l + ... + s (mod 30)

Ovo su bili najtipičniji primeri šifarskih sistema korišćenih do pojave računara. Ostali sistemi su uglavnom varijacije ovih sistema.

Ilustracija šifrovanja

Dajemo primer jednostavnog programa koji bi korisno mogao poslužiti za šifrovanje. Napisan je u Turbo Pascalu. (Primer br. 1.)

Sledi primer otvorenog i šifrovanog teksta. Ključ je bila reč **ENIGMA**. Korišten je priloženi program.

Otvoreni tekst je bio sledeći:

U raznim vremenima i raznim društvenim uređenjima bilo je ljudi koji su učestvovali u jednoj posebnoj vrsti »rata mozgova«. Tom krugu ljudi pripadali su spartanski borci, Julije Cezar i Karlo Veliki, engleski osobenjaci i matematički geniji. U osnovi, svi su oni koristili samo dva oružja: maštu i analitički školovan matematički duh. Svi su oni pokušavali da postignu cilj koji je i danas u središtu pažnje: da obezbede sigurnost podataka. Otkrićem pisma, Čovečanstvo nije samo steklo mogućnost gomilanja znanja, već je stvorilo i jedan problem. Jer, znanje može doći u ruke onih kojima nije namenjeno. Razumljivo je stoga da se ni kraljevi i vojskovođe, političari ni alhemičari nisu ustručavali da se pozabave naukom koja se prema grčkom naziva »kriptologija«.Problem je jednostavan: kako sastaviti poruku koju će samo ovlašćeni primalac moći da pročita i razume? Borba se rasplamsala između onih koji su tragali za bezbednošću podataka i onih koji su tu bezbednost ugrožavali. Svaka nova generacija kriptologa uvek je iznova pokušavala da pronađe šifru koja se ne bi mogla provaliti. Uvek bi se, međutim, našla neka oštroumna glava kojoj bi provala uspela.

Šifrovani tekst dobijen za navedeni otvoreni tekst prikazuje primer br. 2.

Savremeni šifarski sistemi

Ranije opisani šifarski sistemi su kreirani i korišteni u vreme prije pojave računara. Njihova primena u računarstvu je moguća, ali je ograničena uglavnom na jeftinu kratkotrajnu zaštitu podataka. Ove metode mogu zadovoljiti mnoge potrebe pogotovu kad se štite podaci za koje ne postoji prevelik interes od nekoga ko bi želio do njih doći. Stariji šifarski sistemi se mogu upotrebiti i tamo gde se zahteva kratkotrajna zaštita podataka. Njihov nedostatak je u činjenici da svaki jezik ima karakteristiku da se pojedina slova ili skupine slova češće pojavljuju od drugih. To svojstvo se, s obzirom na konačnu dužinu ključa, prenosi i u šifrovani tekst. Ako se pođe od te činjenice i statističkih tablica svojstava pojedinih slova može se značajno olakšati kriptoanaliza (tj. razbijanje) šifrata. Pojava računara je još više, zbog mogućnosti brze obrade, oslabila ove metode. Zbog svega navedenog se usavršavaju nove metode prilagođene današnjem razvoju računarstva. Veliki teoretski značaj ima sistem čiji je koncept postavio američki naučnik **Vernam**: otvoreni tekst (poruka, podaci) se prikaže u binarnom obliku, zatim se generira ključ u binarnom obliku i obavi se sabiranje po modulu 2.

Primer:

Poruka: 1 0 1 0 1 1 0 1 0 1 0 0 0 1
Ključ: 1 1 0 0 0 0 1 1 0 1 0 1 1 1
Šifrat: 0 1 1 0 1 1 1 0 0 0 0 1 1 0

Dešifriranje je jednostavno. Iz šifrata se otvoreni tekst dobija tako što se saberu šifrat i ključ, takođe po modulu 2.

Za generisanje ključa se koriste generatori pseudoslučajnih nizova. Za njih je bitno da daju što dužu sekvencu brojeva, tj. da imaju što veći period nakon koga će se generisana sekvenca ponoviti, kako bi se onemogućilo da se neke osobine prirodnog jezika prenesu na šifrat i sprečilo razbijanje šifre. Kod ovog sistema je aktuelan problem distribucija ključa i sinhronizacija šifrovanja i dešifrovanja. Vernamov sistem predstavlja uglavnom koncept. Praktične realizacije su mnogo složenije i obavljaju se po dosta zamršenim algoritmima.

Danas su veoma poznata dva algoritma. Prvi je DES (Data Encryption Standard), federalni standard za šifrovanje podataka u SAD. Podaci se šifruju po blokovima od po 64 bita, pri čemu se koristi 64-bitni ključ. Šifrovanje bloka se obavlja u 16 iteracija prema dosta složenom algoritmu. U prodaji su čipovi i (sporije) softverske realizacije koji šifruju po DES-u.

Drugi algoritam, RSA (Rivest-Shamir-Adleman), pripada grupi sistema sa javnim ključevima (public key systems). Ovaj teoretski novi koncept rešava dosta osetljiv problem upravljanja ključevima (key management). Bazira se na dosad efikasno nerešenom problemu brze faktorizacije velikih (recimo 100-cifrenih) brojeva. Algoritam nudi veliku sigurnost, ali je njegova realizacija dosta složena, a šifrovanje i dešifrovanje su dosta spori. Šifrovanje se može ubrzati korištenjem dosta skupog hardvera koji obavlja operacije sa velikim brojevima.

Dva navedena algoritma su dosta opisana u literaturi i već postoje njihove brojne modifikacije i različite izvedbe. Postoje brojni drugi algoritmi i stalno se kreiraju novi. Ide se za tim da se nađe algoritam koji će nuditi što veću sigurnost, a biti što jednostavniji i pogodniji za primenu i imati što nižu cenu. Ovi zahtevi su uglavnom oprečni. Apsolutna sigurnost ne postoji i zato se teži da joj se što više približi.

Zainteresovani se mogu obratiti autoru članka radi pomoći u rešavanju problema zaštite ili dobijanja programa za šifrovanje po navedenim algoritmima ili algoritmima prema posebnim zahtevima.

```
Program Sifrovanje;
Var  ottext, siftext : text;
filename1, filename2 : string[14];
i, j, odgovor, code  : integer;
kljuc : string[100];
znak  : char;
Begin
ClrScr;
writeln('Zadaj kljuc ( ključ je niz znakova ) :');
readln(kljuc);
writeln('Da li želiš šifrovanje (1) ili dešifrovanje (2)?');
readln(odgovor);

If odgovor = 1 then   (****** S I F R O V A NJ E ******)
Begin
writeln('Na kojoj datoteci se nalazi otvoreni tekst?');
readln(filename1);
assign(ottext,filename1);
reset(ottext);
writeln('Na koju datoteku treba ispisati šifrovani tekst?');
readln(filename2);
assign(siftext,filename2);
rewrite(siftext);
j := 1;

(****** čitanje otvorenog teksta iz datoteke ******)
(****** šifrovanje i ispis******)

While not eof(ottext) do
begin
 While not eoln(ottext) do
 begin
  read(ottext,znak);
  code := ord(znak) + ord(copy(kljuc,j,1));
  write(siftext,chr(code));WRITE(CHR(CODE));
  j := j+1;
  if j > length(kljuc) then j := 1;
 end;
 readln(ottext);
 writeln(siftext);WRITELN;
end
End
Else (****** D E Š I F R O V A NJ E ******)
Begin
 writeln('Na kojoj datoteci se nalazi šifrovani tekst?');
 readln(filename2);
 assign(siftext,filename2);
 reset(siftext);
 writeln('Na koju datoteku treba ispisati dešifrovani tekst?');
 readln(filename1);
 assign(ottext,filename1);
 rewrite(ottext);
 j := 1;
 (****** čitanje šifrovanog teksta iz datoteke ******)
 (******    dešifrovanje i ispis******)
 While not eof(siftext) do
 begin
  While not eoln(siftext) do
  begin
   read(siftext,znak);
   code := ord(znak) - ord(copy(kljuc,j,1));
   write(ottext,chr(code));    WRITE(CHR(CODE));
   j := j+1;
   if j > length(kljuc) then j := 1;
  end;
  readln(siftext);
  writeln(ottext);WRITELN;
 end;
End;
close(ottext);close(siftext);
End.
```

Primer br. 1