Univerza v Ljubljani
Fakulteta za matematiko in fiziko
Oddelek za matematiko

Popularizacija kriptografije

Cardanova šifrirna metoda in njene priredbe

Karin Šircelj, prof. matematike
magisterij – izobraževalna smer
Projektno delo pri predmetu Kriptografija in teorija kodiranja

Povzetek

Vsak izmed nas se je, verjetno ne da bi vedel, že srečal s šifrirno metodo poimenovano po italijanskem matematiku G. Cardanu. Metoda je bila prvič uporabljena že v 16. stoletju. V osnovi je otroško enostavna, poznamo pa njene priredbe, ki so jih med drugim uporabljali visoki nemški vojaški vrhovi za šifriranje besedil med prvo in drugo svetovno vojno. V nalogi bomo predstavili osnovno Cardanovo šifrirno metodo, njeni priredbi poimenovani metoda *Turnig-grill* in *vrstično pokritje*, omenili bomo dešifriranje *Voynichovega rokopisa*, pri katerem so do večjega napredka prišli šele, ko so uporabili Cardanovo šifrirno metodo. Nalogo bomo zaključili s pripravo zgledne šolske ure pri poglavju Kombinatorika in verjetnostni račun za četrti letnik srednje tehnične gimnazije.

Ljubljana, marec – oktober 2004

Vsebina:

I. Uvod

G. Cardano, italijanski matematik rojen v 16. stoletju, se je ukvarjal z veliko področji, ne samo matematike, ampak tudi drugih znanosti. Tako se je ukvarjal tudi s takrat moderno kriptologijo in kodirnimi metodami. Bil je eden prvih, ki je šifriral besedilo tako, da je začetek sporočila šifriral s ključem, ostanek pa s samim besedilom. Vendar je bila ta njegova metoda pomanjkljivo narejena, izpopolnili so jo drugi in po njej ni znan.
Metode je leta 1550 izdal v delu knjige *De subtilitate libri XXI* in leta 1556 v *De rerum varietete libri XVII*, ki sta bili večkrat ponatisnjeni in celo prevedeni v druge jezike. Najbolj je znan po šifrirni metodi o kateri bomo govorili.
Kot zgled pomembnosti in uporabe te metode omenimo dešifriranje *Voynich-ovega rokopisa* [4]. Knjiga pisana v šifrah naj bi bila nastala nekje med leti 1470 in 1500. Leta 1912 jo je našel M. Voynich v nekem židovskem internatu blizu Rima. Kljub velikim denarnim nagradam, velikemu številu uveljavljenih kriptografov, ki so se ukvarjali z dešifriranjem, je vsebina ostala skrita vse do nedavnega, ko je G. Rugg pri odšifriranju uporabil Cardanove mreže.
Metodo pri kateri uporabljamo tako mrežo, bomo imenovali kar Cardanova šifrirna metoda. Opisna je v drugem poglavju. V tretjem in četrtem poglavju sta opisani priredbi te metode, *metoda Turnig-grill* in *vrstično pokritje*. Za vse metode je tudi izračunano število različnih mrež. V petem poglavju so omenjene težave pri posredovanju parametrov za vrstično pokritje. Bralcu je nakazana pot do rešitve in navedena ustrezna literatura. Priložena je priprava za šolski uri pri kateri predstavimo dijakom te metode. Ti pa jih uporabijo za šifriranje in dešifriranje danega besedila.
To sta naredila tudi glavna igralca naslednje zgodbice.

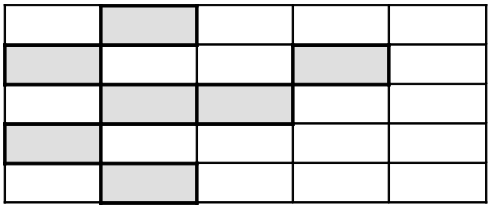
Bojan in Anita sta tipična dijaka neke slovenske srednje šole. Anita je pridna, Bojan je malce len in nekoliko zaljubljen v Anito. Med neko šolsko uro je Anita dobila sporočilo, ki ji ga je poslal Bojan. Ker se je Bojan bal, da sporočilo prestreže učitelj ali pa kateri od posrednikov (sošolcev) pri predaji, ga je napisal v šifrah. Anita je pogledala sporočilo. Pisalo je:

3IRMN3 A1DŠ3V DO2VM G1AJČ3 AOZI ALSI ČKO?

Seveda jo je zanimala vsebina sporočila. Vas tudi?
V pomoč pri odšifriranju naj vam bo podatek, da je besedilo šifrirano s Cardanovo šifrirno metodo, ki je opisana v naslednjem poglavju. Sestavljalci šifer običajno privzamejo, da varnost šifrirne metode ne sme biti zasnovana na njeni tajnosti, pač pa na skrivnem ključu (*Kerckhoffov princip)*. Pri odšifriranju tajnopisa ga je uporabila tudi Anita.

II. Cardanova šifrirna metoda

Cardanova šifrirna metoda je prvič omenjena okrog leta 1556. Prvi jo je objavil Girolamo Cardano v eni od svojih knjig. Šifriranje besedila - čistopisa poteka takole:
Izdelamo mrežo dimenzije *n x m*. V njej izberemo nekaj polj in jih izrežemo iz mreže.



Mrežo postavimo na papir in zaporedoma od leve proti desni vpisujemo besedilo v izrezana polja. Če je besedilo daljše kot imamo izrezanih polj, mrežo prestavimo naprej in nadaljujemo z vpisovanjem. Ko končamo z vpisovanjem besedila, mrežo umaknemo in prazen prostor med besedilom dopolnimo z naključno izbranimi črkami kot kaže slika. Tako smo šifrirali besedilo in dobili tajnopis.

K	C	L	A	R
A	T	E	R	O
T	D	A	L	L
N	P	U	R	L

A	O	U	R	Q

Kclarateroldallnpurl

Prejemnik za dešifriranje tajnopisa potrebuje enako mrežo. To postavi preko besedila in bere sporočilo v izrezanih poljih.

K	C	L	A	R
A	T	E	R	O
T	D	A	L	L
N	P	U	R	L
A	O	U	R	Q

Cardano

Metoda je zelo enostavna, vendar za daljša sporočila neprimerna in za moderen računalniški čas relativno slabe varnosti.
Že z požrešnim napadom dokaj hitro dešifriramo besedilo.
Izračunajmo koliko različnih mrež lahko sestavimo za tabelo velikosti *5 x 6*. Imamo 30 polj. Lahko si izberemo od 0 do 30 možnosti, seveda so možnosti z malo in možnosti z veliko izbranimi polji relativno nesmiselne. Ampak prištejmo tudi te. Pri računanju uporabimo obrazec za določanje števila variacij reda *r* pri *n* elementih: $V_n^r = \frac{n!}{(n-r)!}$, kjer je $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

Število polj	možnosti
0 (30)	1
1 (29)	30
2 (28)	V_{30}^{2}
⋮	⋮
13(17)	V_{30}^{13}
14(16)	V_{30}^{14}
15	V_{30}^{15}

Kar je enako
$2 \cdot \left(1 + 30 + V_{30}^{2} + \cdots + V_{30}^{15}\right)$.

Tako imamo za mrežo velikosti *n x m* natanko $2 \cdot \left(1 + nm + V_{n}^{2} + \cdots + V_{n}^{\frac{n-m}{2}}\right)$ možnosti. Pri predpostavki, da napadalec ve koliko polj je izbranih, je število enako $V_{nm}^{r} = \frac{nm!}{(nm-r)!}$.

Vrnimo se nazaj na primer. Vam je uspelo? Aniti je. Uporabila je mrežo velikosti *3 x 3* in izbrala 5 polj. Če vas zanima kaj pomenijo v tajnopisu števila med črkami, pozorno berite naprej.

Anita je Bojanu odgovorila in ker ni hotela zaostajati za njim (spomnimo se, da je zelo pridna) je besedilo šifrirala s priredbo Cardanove šifrirne metode, ki je opisana v naslednjem poglavju. Sporočilo se je glasilo:

***I**JOJ MMU**Š** KP**N**I A**A**AT*

Vas zanima?

III. Metoda *Turnig-grill*

Metoda *Turnig-grill* je priredba Cardanove šifrirne metode. Tudi pri njej potrebujemo mrežo. Šifriranje čistopisa poteka takole.
Izdelamo kvadratno mrežo velikosti $n \times n$ in jo razdelimo na štiri enake kvadratne podmreže. Razdelitev ni nujno sestavljena iz kvadratnih podmrež, pomembno je, da je sestavljena iz štirih skladnih podmrež, ki pri vrtenju za polni kot okoli središča mreže v pozitivnem ali negativnem smislu prekrijejo celo mrežo[3].
Prvo podmrežo postavimo v levi zgornji kvadrant in za pomoč oštevilčimo njena polja zaporedoma po vrsticah s števili od 1 do $\left(\frac{n}{2}\right)^2$. Drugo oštevilčeno podmrežo postavimo tako, da je polje 1 v desnem zgornjem kotu, torej jo zavrtimo za polni kot okrog središča osnovne mreže v smeri urinega kazalca. Enako naredimo z ostalima podmrežama. Polji 1 sta tako v skrajnima spodnjima desnemu oziroma levemu polju, kot kaže slika.

1 c	2 a	3	1 n
3	4	4 a	2
2 r	4	4 o	3 d
1	3	2	1

Sedaj si v vsakem kvadrantu osnovne mreže izberemo nekaj polj, skupaj $\left(\frac{n}{2}\right)^2$, tako da si vsako število izberemo samo enkrat. Z vrtenjem okrog središča mreže za polni kot bomo pokrili ravno vsa polja mreže. S tem je mreža pripravljena.

1 c	2 a	3	1 n
3	4	4 a	2
2 r	4	4 o	3 d
1	3	2	1

Sledi šifriranje čistopisa.
Mrežo postavimo na papir in v izrezana polja vpisujemo zaporedoma od leve proti desni po vrsticah besedilo. Ko zapolnimo prazna polja mrežo zavrtimo za polni kot v smeri urinega kazalca in postopek ponovimo. To naredimo še dvakrat. Ko pridem na osnovni položaj je mreža izpolnjena.
Prejemnik mora imeti seveda enako mrežo. Za dešifriranje tajnopisa ponovi enak postopek kot je opisan zgoraj.

Metoda ima seveda nekaj pomanjkljivosti. Pošiljatelj in prejemnik morata imeti isto mrežo. Prejemnik mora poznati potrebne parametre za sestavo mreže.
Te težave so skušali rešiti na različne načine. Tako so med besedilo dopisali števke, ki so določale mesto na katerem je bilo izbrano posamezno prazno polje ali pa so črko na tem mestu zapisali odebeljeno ali kako drugače kot ostalo besedilo.
Vendar pri takem načinu sporočanja potrebnih podatkov napadalec zlahka določi *n* in s tem mrežo. Z dobrim računalnikom je ostalo dešifriranje lahko delo, zato je varnost relativno slaba.
Med I. svetovno vojno so težave s parametri rešili tako, da so uporabljali le mreže velikosti *n x n*, kjer je $n = m^2$. Mreža določene velikosti je imela svoje ime, Franc je pomenilo *n = 100* in Ana *n = 25*.

Poglejmo koliko možnosti je za različne izbore praznih polj, kaj lahko naredimo z požrešnim napadom.
Izberemo mrežo *n x n*, kjer je n sodo število.
Razdelimo jo na štiri podmreže velikosti $\left(\frac{n}{2}\right)\times\left(\frac{n}{2}\right)$. Na mreži izberemo $\left(\frac{n}{2}\right)\cdot\left(\frac{n}{2}\right)$ polj.
Vsako polje lahko izberemo samo v eni od podmrež, torej imamo $4^{\left(\frac{n}{2}\right)^2}$ možnosti. Ker podmrežo vrtimo za kot 90°, možnosti, ki jih lahko z vrtenjem za polni kot prevedem eno na drugo, štejem samo enkrat. Torej imamo $4^{\left(\frac{n}{2}\right)^2} : 4 = 4^{\left(\frac{n}{2}\right)^2 - 1}$ možnosti.
Za *n = 8* imamo $4^{15} = 2^{30}$ možnosti.
Če je *n* liho število je teh možnosti $4^{\left(\frac{n}{2}\right)^2 - \frac{1}{4}}$.
Možnosti štejemo podobno kot zgoraj, le da središčnega polja ne uporabljamo. Vanj vpišemo poljuben znak in ga ne spreminjamo.
Za *n = 7* imamo $4^{12} = 2^{26}$ možnosti.

Vrnimo se k naši zgodbi.
Bojan, vešč mladi kriptolog (sicer len, ampak brihten), je takoj dešifriral sporočilo. Uporabil je mrežo velikosti 4 x 4. Seveda se ni pustil premagati pri odkrivanju novega, pa še odgovoriti je želel na Anitino sporočilo, zato ji je odgovor poslal šifriran z linear grid metodo. Tu je njegov odgovor.

AOOI EPKS DPUK NSUO TCVU RIAS NOMJ OTKI

IV. Vrstično pokritje

Oglejmo si priredbo Cardanove šifrirne metode imenovano *linear grid*. Mi jo bomo imenovali *vrstično pokritje*. Mrežo namreč sestavljamo po vrsticah, ki so medsebojno odvisne.
Izberemo si *m* predalov z *n* elementi in jih položim v vrsto kot kaže slika.

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

Posamezna polja označimo s števili od 1 do *n* (kot pomoč pri izbiri praznih polj). Vsako število od 1 do *n* si izberemo v enem od predalov. Izbrati moramo vsa števila.
V naslednjem koraku šifriranja postavimo zadnji predal na prvo mesto in tako nadaljujemo glede na velikost besedila (število črk v besedilu). Ko bomo sestavili *m* vrstic, bomo zaradi omejitve pri izbiri praznih polj, pokrili vsa polja v mreži velikosti *m x n*.

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4

Preštejmo koliko možnosti imamo.
Vsako izmed *n* praznih polj lahko izberemo v enem od m predalov, torej imamo m^n možnosti. Ker predale prestavljamo *m*-krat izločim možnosti, ki se pri prestavljanju prevedejo ena na drugo, tako imamo $m^n : m = m^{n-1}$ možnosti.
Vidimo, da je varnost za majhne *n* in *m* še vedno relativno slaba, za velike *n* in *m* pa imamo že relativno dobro varnost.

Kaj pa pošiljanje podatkov o mreži? To težavo rešimo s permutacijami.
Vrstično pokritje lahko predstavimo s permutaciajmi in tako namesto potrebnih parametrov prejemniku pošljemo ustrezno permutacijo. Za dešifriranje mora izračunati njeno inverzno permutacijo.

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
C	A	R	D	A	N	O	G	I	R	O	L	A	M	O	K

2	7	9	16	4	6	11	13	1	8	10	15	3	4	12	14
A	O	I	K	D	N	O	A	C	G	R	O	R	A	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Dobimo naslednjo permutacijo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 7 & 9 & 16 & 4 & 6 & 11 & 13 & 1 & 8 & 10 & 15 & 3 & 4 & 12 & 14 \end{pmatrix}.$$

In zaključek naše zgodbe?
Ko je Anita dešifrirala dobljeno sporočilo z uporabo zgornje permutacije, je Bojan dobil…, Anita pa…
Kaj, boste izvedeli, če boste dešifrirali sporočila.

V. Ponujena rešitev »pomanjkljivosti« opisanih metod: Diffie-Hellmanova metoda

Ogledali si bomo še kako lahko izboljšamo nekatere pomanjkljivosti pri pošiljanju potrebnih podatkov.
Podatki, ki jih potrebujeta pošiljatelj in prejemnik za uspešno komunikacijo:

- katero metodo bosta uporabljala (Kerckhoffov princip***)***,
- velikost mreže in število izbranih polj,
- čas spremembe parametrov (če bosta seveda spreminjala parametre),
- način spremembe parametrov.

Te podatke lahko izmenjata na različne načine. Nekaj smo jih že omenili v prejšnjih poglavjih. Vendar pa obstajata dve večji težavi. Če napadalec ugotovi trenutni ključ, potem lahko določi vse potrebne podatke za dešifriranje. Težava je tudi v tem, da izbor velikosti predalov in števila izbranih polj pri vrstičnem pokritju ni naključen, ampak je odvisen od velikosti besedila. Izbor polj pa je odvisen od zaporedja izbiranja.
Ti težavi lahko rešimo, če parametre pošljemo na drugačen način. Tega se pred letom 1967 ni dalo. Zakaj? Ker pri tem načinu uporabimo Diffi-Hellmanovo metodo, ki je bila odkrita šele leta 1976. O metodi lahko več preberete v [2] (prvi članek o tej metodi) in v skoraj vsakem učbeniku kriptografije. Rešitev problema je predstavljena v [1].

VI. Zaključek

V nalogi smo spoznali Cardanovo šifrirno metodo in njene priredbe. Za vsako metodo smo izračunali število možnih izbir mrež pri dani velikosti. Opisali smo nekaj težav in njihovih rešitev. Ob zgodbici o Bojanu in Aniti smo pokazali primer uporabe opisane metode. (Ste pomislili na »plonkanje«? Sicer je to goljufija, ampak tudi s pisanjem »plonkca« se veliko naučimo.)

Za vedoželjne računalnikarje postavljamo izziv. Izdelajte program, ki bo šifriral in dešifriral besedila z opisanimi metodami.

Za vedoželjne zgodovinarje pa še to. Šifrirna metoda izgleda na prvi pogled zelo nepomembna, vendar je v preteklosti služila tudi za ohranjanje nemških vojaških skrivnosti v I. in II. svetovni vojni. Veliko pove dejstvo, da so jo uporabljali vrhovi nemške vojske. Po izkušnjah z mehaničnim načinom šifriranja v vojnah predpostavljamo, da bi morala tudi za to metodo obstajati šifrirna mašina, o čemer nismo našli nobenih podatkov, zato je nadaljnje iskanje še nedokončano delo.

Postavljene cilje smo dosegli, če je napisano spodbudilo bralca k samostojnemu brskanju, pregledovanju in uporabi literature in metod na področju kriptografije in teorije kodiranja.

VII. Zgledna šolska ura

SPROTNA PRIPRAVA
na vzgojno-izobraževalno delo

Ime in priimek učitelja: Karin Šircelj, prof. matematike
Srednja šola za elektrotehniko in računalništvo Ljubljana *STROKOVNA GIMNAZIJA* *Program: Tehniška gimnazija*
Razred: G4 *Ura:* *Datum:*
Učna tema: ***Verjetnostni račun in statistika***
Učna enota: Vaje – kombinatorika in verjetnostni račun
Vzgojno-izobraževalni cilji: Dijakom vzbuditi zanimanje za Kriptologijo in teorijo kodiranja. Najprej predstaviti staro, enostavno šifrirno metodo, jo uporabiti na enostavnemu primeru. Nato zbuditi zanimanje za nadaljnje delo – predstavitev priredb, uporaba modernih tehnologij (računalnik) namesto papirja in svinčnika. Spodbuditi dijake k nadaljnjemu, samostojnemu raziskovanju. Predstaviti osnove šifriranja in dešifriranja, v pogovoru naglasiti pomen varnosti pri komuniciranju.
Učna oblika: frontalna, delo v skupinah
Učna metoda: razlaga, vodeni razgovor, reševanje nalog
Učna sredstva in pripomočki: zvezek, delovni listi, papir, prosojnice, flomastri
Opombe: Za izvedbo potrebujemo dve šolski uri.

ZGRADBA UČNE URE IN		***ZADOLŽITVE***
1. ura	*UČITELJ*	*DIJAK*
Uvajanje, motivacija *20 minut*	Pove nekaj osnovnih dejstev o Kriptologiji in teoriji šifriranja. Naveže se na članke [5], [6]. Opiše Cardanovo šifrirno metodo. Na tablo zapiše Bojanovo sporočilo in jih spodbudi k odšifriranju.	Sodelujejo v pogovoru. Predstavijo svoje izkušnje povezane s šifriranjem podatkov. Skušajo dešifrirati sporočilo.
Vsebina učne enote *15 minut*	Razdeli dijake v 4 skupine. Skupinam, da navodila. Pomaga in da dodatna pojasnila drugima dvema skupinama.	Tri skupine sestavijo mrežo in šifrirajo besedilo. Vsaka skupina sestavi mrežo za eno od predstavljenih metod (glede na znanje). Dve skupini dobita delovne liste na katerih sta opisani priredbi (turnig-grill, vrstično pokritje). Mreže narišejo na prosojnice. Četrta skupina, v kateri so dijaki z boljšim znanjem računalništva, napiše program, ki bo pri danima *m* in *n* sestavil mrežo in šifriral dano besedilo.
Utrjevanje, ponavljanje *10 minut*	Usmerja predstavitve in jih dopolnjuje, če je potrebno. Razdeli šifrirana Anitin in Bojanov odgovor.	Predstavnika druge in tretje skupine opišeta turig-grillovo metodo in vrstično pokritje in ju predstavita na primerih, ki so ju izdelali v skupini. Doma skušajo dešifrirati dobljeni besedili.
Opombe	Vprašanje: ali bo dovolj časa?	

ZGRADBA UČNE URE IN		***ZADOLŽITVE***
2. ura	*UČITELJ*	*DIJAK*
Uvajanje, motivacija *15 minut*	Na kratko obnovi vsebino in potek prejšnje šolske ure.	Poslušajo. Predstavnik četrte skupine opiše potek dela v računalniški skupini in demonstrira izdelani program na dobljeni domači nalogi.
Vsebina učne enote *20 minut*	Predstavi vprašanja na katera bodo skušali najti odgovor: - Izračunaj koliko je vseh možnosti za sestavo mreže pri izbrani velikosti za Cardanovo šifrirno metodo? - Koliko je teh možnosti za metodo turnig-grill? - Izračunaj kolikšna je verjetnost, da napadalec uspe v prvem poskusu. - Kolikšna je verjetnost, da napadalcu uspe v prvem poskusu, če pozna število praznih polj v mreži? - Kaj pa, če pozna polovico praznih polj?	Zapišejo vprašanja in iščejo odgovore. (Dijaki lahko seveda postavijo vprašanja, ki so se njim postavila ob spoznavanju metod.)
Utrjevanje, ponavljanje *10 minut*	Preverja odgovore in jih dopolnjuje, če je potrebno. Usmeri dijake k nadaljnjemu raziskovanju na področju kriptografije in teorije kodiranja.	Dijaki odgovarjajo na postavljena vprašanja in utemeljijo svoje odgovore.
Opombe	Vprašanje: ali so vprašanja pretežka?	

VIII. Literatura

1. S. Fratini, An Encryption Algorithm using a Variation of the Turning-Grille Method, Mathematics Magazine, Vol. 75, No. 5, str. 389-396.
2. W. Diffie, M. E. Hellman, New Directions in Cryptography, Transactions of Information Theory, vol. IT-22, str. 29 – 40.
3. internet http://educ.queensu.ca/~fmc/may2004/cardano.html
4. G. Rugg, The Mystery of the Voynich Manuscript, Scientific American, Vol. 291, No. 1, str. 78-83.
5. J. Zupan, Nekaj o kriptografskih metodah, Obzornik mat. fiz. 25 (1978) 4, str. 129–136.
6. S. Kuharić, Povjest kriptografije (http://fly.srk.fer.hr/~peloquin/OPCENITO/seminar.htm)