Kriptografija u školi

Marija Barun, Andrej Dujella i Zrinka Franušić

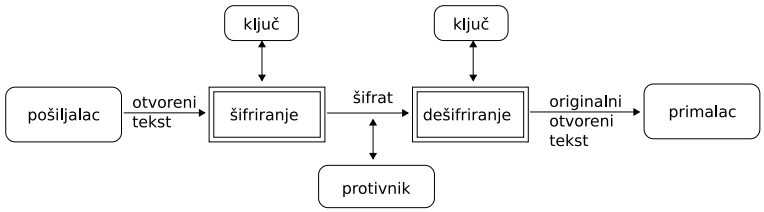
Kriptografija ima velik potencijal kojim može obogatiti nastavu matematike. Može joj dati uzbudljivost, dramatičnost, dinamičnost, a kod učenika pobuditi znatiželju i kreativnost. Upravo to tako često nedostaje u nastavi matematike u kojoj se sve servira "zdravo za gotovo". Stoga učenici nerijetko dobivaju dojam da se u matematici više ništa novoga ne može otkriti (za razliku od nekih drugih predmeta gdje im znatiželju pobuđuju otvorena pitanja poput onog "Koliko je velik Svemir?" ili "Zašto su izumrli dinosauri?"). Mnogi primjeri iz kriptografije mogu nam poslužiti da odagnamo ukorijenjene stereotipe kao npr. onaj da je svaki matematički problem rješiv pomoću prave formule ili dobrog računala. Naime, sigurnost kriptosustava leži upravo u našoj nemogućnosti da brzo i efikasno riješimo odgovarajući problem iz područja algebre, teorije brojeva ili kombinatorike. Zanimljive metode šifriranja, te posebice otkrivanje metoda za razbijanje sustava za šifriranje, omogućit će učenicima da osjete snagu i ljepotu matematike.

1 Osnovni pojmovi

Kriptografija (hrv. *tajnopis*) je znanstvena disciplina koja proučava metode za slanje poruka u oblicima čitljivim samo onima kojima su i namijenjene. Začetke kriptografije, odnosno šifriranja poruka, nalazimo kod starih Grka u 5. stoljeću prije Krista. Oni su koristili su drveni štap na kojeg bi namotali traku od pergamenta, te na nju okomito napisali poruku. Kada bi se traka odmotala, poruka na njoj postala bi nečitljiv skup znakova, a pročitati bi je mogao samo onaj koji je posjedovao štap odgovarajućeg promjera. Ta se naprava za šifriranje nazivala *skital*.

Uvedimo neke osnovne kriptografske pojmove. Cilj kriptografije je omogućiti nesmetano komuniciranje osobe A (pošiljalac) i osobe B (primalac) preko nesigurnog komunikacijskog kanala tako da treća osoba C (protivnik) ne može razumijeti njihove poruke. (U kriptografskoj literaturi su za pošiljaoca i primaoca rezervirana imena Alice i Bob, dok se protivnik najčešće zove Eva ili Oskar.) Poruku koju osoba A želi poslati osobi B nazivamo *otvoreni tekst* (engl. plaintext). Osoba A, najprije, transformira, tj. *šifrira*, otvoreni tekst koristeći se unaprijed dogovorenim *ključem* i tako dobiva *šifrat*. Zatim ga šalje nesigurnim komunikacijskim kanalom. U tom je trenutku šifrirana poruka - šifrat dostupna osobi C, no ona je ne može *dešifrirati*, jer ne posjeduje ključ. Konačno, šifrat stiže osobi B koja ga pomoću ključa *dešifrira* i dobiva otvoreni tekst.

Kriptosustave možemo podijeliti na one s *tajnim* i one s *javnim* ključem. Kriptosustavi s tajnim ključem koriste najčešće isti ključ za šifriranje i dešifriranje poruka (ili se ključ za dešifriranje može lako odgonetnuti poznavanjem ključa za šifriranje i obratno). Sva njihova sigurnost leži upravo u tajnosti ključa. U literaturi ove sustave još nalazimo pod imenom *simetrični* ili *konvencionalni* kriptosustavi. Kod kriptosustava s javnim ključem, odnosno *asimetričnih* kriptosustava, je nemoguće, u nekom razumnom vremenu, odrediti



Slika 1: Shema klasične kriptografije

ključ za dešifriranje (usprkos tome što je ključ za šifriranje poznat). Dok su simetrični kriptosustavi poznati još od davnina (koristili su ih stari Grci i Rimljani), prva ideja o uporabi asimetričnih kriptosustava pojavila se tek u drugoj polovici 20. stoljeća.

2 Primjeri

U ovom dijelu opisat ćemo neke jednostavne kriptosustave koji mogu poslužiti za popularizaciju matematike u školama i drugdje. Oni su namijenjeni i razumljivi i onima koji nemaju visoku matematičku naobrazbu, prvenstveno učenicima osnovnih i srednjih škola, ali i odraslima. Grana kriptografije koja razvija takve sustave naziva se *Kid Krypto* (prema Fellows i Koblitz, vidi [8, 6]).

2.1 Primjer (Cezarova šifra)**.**

Opisat ćemo način šifriranja koji potječe od rimskog vojskovođe Julija Cezara koji je na taj način komunicirao sa svojim prijateljima. Sastoji se u tome da se svako slovo poruke (tj. otvorenog teksta) zamijeni slovom koje se nalazi n mjesta dalje u alfabetu. Pretpostavimo da želimo šifrirati tekst "LAV". Koristit ćemo se engleskim alfabetom od 26 slova, a slova Č, Ć, Đ, Dž, Lj, Nj, Š, Ž, zamijenit ćemo redom slovima C, C, DJ, DZ, LJ, NJ, S, Z. Ako je na primjer $n = 5$, onda šifrat glasi "QFA". Općenito, šifriranje i dešifriranje ovom šifrom može se opisati ovim funkcijama:

$$e_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad e_n(x) = (x + n) \bmod 26,$$

$$d_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad d_n(y) = (y - n) \bmod 26,$$

pri čemu je $0 \leq n \leq 25$, a svakom smo slovu abecede jednoznačno pridružili njegov redni broj počevši od 0, prema korespodenciji:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Sa $a \bmod 26$ označavamo ostatak pri dijeljenju broja a s 26. Umjesto zbrajanja u prstenu $\mathbb{Z}_{26}$, učenici mogu koristiti krug ("kolo") načinjen od kartona pri čijem su rubu ispisana redom sva slova abecede.

Sada ćemo nešto reći o dekriptiranju šifrata (tj. određivanju šifrata bez poznavanja ključa) dobivenog Cezarovom šifrom. Jedna od metoda dekriptiranja jest primjena "grube

sile", odnosno ispitivanje svih mogućih ključeva redom sve dok ne dobijemo neki smisleni tekst. Ova je metoda opravdana jer je broj ključeva mali (tj. upravo onoliki koliko je i slova - 26). Na primjer, neka šifrat glasi "XENRSTMW". Tada dobivamo sljedeće:

$$\begin{array}{cccccccccc} \mathrm{X} & \mathrm{E} & \mathrm{N} & \mathrm{R} & \mathrm{S} & \mathrm{T} & \mathrm{M} & \mathrm{W} & \text{za} & n=0, \\ \mathrm{W} & \mathrm{D} & \mathrm{M} & \mathrm{Q} & \mathrm{R} & \mathrm{S} & \mathrm{L} & \mathrm{V} & \text{za} & n=1, \\ \mathrm{V} & \mathrm{C} & \mathrm{L} & \mathrm{P} & \mathrm{Q} & \mathrm{R} & \mathrm{K} & \mathrm{V} & \text{za} & n=2, \\ \mathrm{U} & \mathrm{B} & \mathrm{K} & \mathrm{O} & \mathrm{P} & \mathrm{Q} & \mathrm{J} & \mathrm{T} & \text{za} & n=3, \\ \mathrm{T} & \mathrm{A} & \mathrm{J} & \mathrm{N} & \mathrm{O} & \mathrm{P} & \mathrm{I} & \mathrm{S} & \text{za} & n=4. \end{array}$$

Na drugi način, dekriptirati se može pomoću *frekvencijske analize* slova. Za ovu metodu korisno je znati kojim je jezikom tekst pisan, jer se frekvencije slova u različitim jezicima razlikuju. Otkrivanje frekvencije slova može biti i jedna zanimljiva nastavna aktivnost. Analiziranjem manjih tekstualnih odlomaka na različitim jezicima učenici se mogu osobno uvjeriti da su najfrekventnija slova hrvatskog jezika redom A, I, O, E, N, engleskog jezika E, T, A, O, I, njemačkog E, N, I, R, S, itd. Na primjer, ako šifrat glasi

"REYJREYNPEOJPWEQONHENXQZLE",

onda pronađemo najfrekventnije slovo u šifratu. To je slovo E koje se pojavljuje 6 puta. Ukoliko pretpostavimo da je to slovo A, dobit ćemo sljedeći otvoreni tekst (s umetnutim razmacima)

MATEMATIKA JE KRALJICA I SLUGA.

2.2 Primjer (Vigenéreova šifra)**.**

Ovaj način šifriranja vrlo je sličan Cezarovom. U ovom slučaju ključ je sačinjen od bloka slova, odnosno kraće riječi. Ako smo za ključ uzeli riječ "ZEC" koja se sastoji od 25., 4. i 2. slova u alfabetu, onda ćemo prvo slovo otvorenog teksta pomaknuti za 25 mjesta dalje, drugo za 4 mjesta, treće za 2, četvrto ponovo za 25, peto za 4, itd.

Za dekriptiranje poruke potrebno je najprije pretpostaviti, odnosno pogoditi, koliko je duga ključna riječ. Ukoliko je ključ blok od 3 slova, onda načinimo frekvencijsku analizu svakog trećeg slova u šifratu. Ovdje se nameću neka zanimljiva pitanja. Što se dešava ako je pretpostavka o duljini ključne riječi bila pogrešna? Koliko bi šifrat trebao biti dug da bi ga imalo smisla analizirati? Koliko bi trebala biti dugačka ključna riječ pa da šifriranje bude sigurnije? (Očito što dulja! Potpuno siguran sustav je onaj s "beskonačno" dugačkim ključem.)

2.3 Primjer (Tajni protokol)**.**

Ovo je simpatična aktivnost koja se može provesti i kod učenika nižih razreda, no i svugdje gdje je potrebno brzo i diskretno provesti neku "numeričku" anketu.

Zamislimo da nastavnik želi saznati prosječan broj sati koje učenik troši na učenje i pisanje zadaće svakog tjedna. Postoji opravdana bojazan da učenici ne bi bili potpuno iskreni ukoliko taj podatak trebaju iznijeti javno (bolji učenici mogli bi svoju "brojku" umanjiti, a oni lošiji uvećati). Stoga nastavnik može primijeniti sljedeću proceduru koja će sačuvati pravo na privatnost svakog učenika. Protokol započinje Adam koji izabire "tajni" cijeli broj n. Neka je $n = -215$. "Tajni" broj n Adam uvećava za broj sati koji provodi u učenju, npr. za 5, $n_A = n + 5 = -210$. Zatim, Adam šapne broj n_A sljedećoj učenici

Branki. Branka na školske obveze utroši tjedno 7 sati, pa je $n_B = n_A + 7 = -203$. Broj n_B Branka došapne Cvijeti. Cvijeta uvećava n_B za "svoj" broj 4, tj. $n_C = n_B + 4 = -199$, te ga prošaputa Davoru. Protokol se nastavlja redom do posljednjeg učenika Zlatka kojem je prišapnut broj n_V njegovog predhodnika Vlatka. Nakon uvećavanja broja n_V, $n_Z = n_V + 6$, Zlatko tu informaciju proslijeđuje Adamu. Adam od konačnog zbroja n_Z odbija "tajni" broj n. Pretpostavimo da je $n_Z = -100$. Sada Adam svima može priopćiti da je ukupan broj sati koji njegov razred utroši na izvršavanju školskih obveza jednak $n_Z - n = 115$. Budući da ovaj razred broji 22 učenika, prosječna vrijednost iznosi 5.2 sata.

Pitanje koje se može postaviti učenicima jest kako mogu "razbiti" tajnost ovog protokola. To je moguće ukoliko npr. Adam i Cvijeta surađuju. Njih dvoje tada mogu zajedno otkriti koliko se zadaćama tjedno bavi njihova kolegica Branka. Zaista, Cvijeti je poznat broj n_B, pa uz Adamovu pomoć može odrediti da je to broj $n_B - n_A = -203 - (-210) = 7$.

2.4 Primjer (RSA)**.**

RSA kriptosustav je prvi kriptosustav s javnim ključem. Osmislili su ga Ron Rivest, Adi Shamir i Len Adleman 1977. godine i do danas je jedan od najrasprostranjenijih kriptosustava s javnim ključem. Njegova sigurnost je zasnovana na teškoći faktorizacije velikih prirodnih brojeva. Opišimo, najprije, originalni RSA kriptosustav. Odabir parametara za ovaj sustav vrši u sljedećih nekoliko koraka:

- Izabiremo dva velika (barem 100 znamenaka) prosta broja p i q slične veličine, no ne preblizu jedan drugome.
- Računamo $n = pq$.
- Odabiremo broj e koji je relativno prost s brojem $(p-1)(q-1)$. Često se ovaj broj bira slučajnim odabirom i potom se provjeri zadani uvjet.
- Pomoću Euklidovog algoritma izračuna se broj d takav da je

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Vrijednosti n i e su javne, odnosno (n, e) predstavlja *javni ključ*, dok je (p, q, d) *tajni ključ*. Pretpostavimo da otvoreni tekst predstavljen numeričkom vrijednošću x za koju vrijedi da je $0 \leq x < n$. Šifriranje poruke x vrši se pomoću funkcije

$$e_K(x) = x^e \bmod n,$$

a dešifriranje pomoću

$$d_K(y) = y^d \bmod n.$$

Funkcije e_K i d_K su međusobno inverzne, no dokaz nije sasvim jednostavan, već uključuje poznavanje Eulerovog teorema (vidi npr. [3]) koji povlači da za svaki cijeli broj x koji je relativno prost s pq, broj $x^{(p-1)(q-1)}$ daje ostatak 1 pri dijeljenju sa pq. Napomenimo da je funkciji e_K vrlo teško odrediti inverz ukoliko nam nije poznata faktorizacije broja $n = pq$, pa se klasičan napad na ovaj kriptosustav sastoji upravo od traženja faktorizacije broja n. Inače, dosad nije pokazano je li određivanje poruke x iz poznavanja šifrata $x^e \bmod n$ ekvivalentno faktorizaciji od n.

2.5 Primjer ("Dječji" RSA)**.**

Opisat ćemo sada pojednostavljeni ("dječji") RSA kriptosustav koji je primjeren učenicima srednjih škola. Preduvjet je da su učenici upoznati s osnovama teorije kongruencija, te da znaju prikazati prirodan broj u različitim bazama. Najprije, Alice izabire cijele brojeve a, b, a', b' i postavlja sljedeće vrijednosti:

$$\begin{aligned} M &= ab - 1, \\ e &= a'M + a, \\ d &= b'M + b, \\ n &= (ed-1)/M = a'b'M + ab' + a'b + 1. \end{aligned}$$

Njen javni ključ je (n, e), a tajni d. Definirajmo sljedeće funkcije

$$\begin{aligned} e_{ALICE}(x) &= ex \bmod n, \\ d_{ALICE}(y) &= dy \bmod n, \end{aligned}$$

gdje je x prirodan broj koji predstavlja poruku, tj. otvoreni tekst. Funkcije e_{ALICE} i d_{ALICE} su međusobno inverzne. Zaista, neka je $0 \leq x < n$. Tada je

$$\begin{aligned} d_{ALICE}(e_{ALICE}(x)) &\equiv dex \equiv (b'M + b)(a'M + a)x \equiv (a'b'M^2 + ab'M + a'bM + ab)x \\ &\equiv (Mn + 1)x \equiv x (\bmod\, n) = x. \end{aligned}$$

Nadalje, Bob odabire cijele brojeve a_1, b_1, a_1', b_1', te, na isti način kao i Alice, generira brojeve e_1, d_1, n_1. Analogno su definirane funkcije $e_{BOB}(x) = e_1 x \bmod n_1$ i $d_{BOB}(y) = e_1 y \bmod n_1$. Bobov javni ključ je (n_1, e_1), a tajni d_1.

Pretpostavimo da Alice želi Bobu poslati poruku x. Šifriranje Alice vrši tako što redom računa vrijednosti

$$\begin{aligned} y &= d_{ALICE}(x), \\ z &= e_{BOB}(y), \end{aligned}$$

te Bobu šalje poruku y. Primivši ju, Bob ju dešifrira na sljedeći način:

$$e_{ALICE}(d_{BOB}(z)) = e_{ALICE}(d_{BOB}(e_{BOB}(y))) = e_{ALICE}(y) = x.$$

Konkretno, pretpostavimo da Alice želi Bobu poslati poruku "ALICE". Najprije ovu poruku treba pretvoriti u numeričku vrijednost. Kako ne bismo dobili prevelike brojeve, pretvaranje ćemo vršiti po blokovima veličine 3 slova. Ukoliko poruka nije višekratnik broja 3, onda je nadopunimo s jednim ili dva prazna mjesta. Pretvaranje vršimo u bazi 27: slovu A pridružujemo broj 1, slovu B broj 2, ..., slovu Z broj 26. Praznom mjestu pridružujemo vrijednost 0. (Ukoliko bismo koristili korespodenciju iz Primjera 2.1 imali bismo problema sa šifriranjem poruka koje počinju slovom A!). U našem slučaju šifriramo najprije poruku "ALI", a zatim "CE". Dakle,

$$x = (\mathrm{ALI})_{27} = (1 \cdot 27^2 + 12 \cdot 27 + 9)_{10} = (1062)_{10}.$$

Pretpostavimo da je Alice odabrala sljedeće vrijednosti: $a = 15$, $b = 12$, $a' = 10$, $b' = 11$, te dobila da je $M = 179$, $e = 1805$, $d = 1981$, $n = 19976$. U javni direktorij Alice je stavila

$(19976, 1805)$. Na isti način, Bob je odabrao brojeve $a_1 = 10$, $b_1 = 8$, $a_1' = 15$, $b_1' = 13$, te izračunao da je njegov javni ključ $(15656, 1195)$, a tajni 1035. (Ovdje treba pripaziti da je $x < n$ i $x < n'$. Koji je najmanji takav n?). Sada Alice najprije koristi svoj tajni ključ 1981 i računa

$$y = 1981x \bmod 19976 = 6342,$$

a zatim, iskoristivši Bobov javni ključ, dobiva

$$z = 1195y \bmod 15656 = 1186.$$

Bob prima šifrat 1186, te ga dešifrira tako što najprije koristi svoj tajni ključ, a onda uporabi Alicein javni ključ, odnosno računa

$$1035 \cdot 1186 \bmod 15656 = 6342 = y,$$
$$1805 \cdot 6342 \bmod 19976 = 1062 = x.$$

Ovaj kriptosustav može se razbiti pronalaženjem prirodnog broja d takvog da je $de \equiv 1 \pmod{n}$ (čak ne nužno onog d kojeg Alice koristi kao svoj tajni ključ). To je moguće efikasno napraviti pomoću Euklidovog algoritma (vidi [3]), no taj algoritam vjerojatno nije poznat onima kojima je ovaj sustav namijenjen. Otvoreno je pitanje može li se ovaj sustav razbiti bez primjene neke verzije Euklidovog algoritma. Ovaj primjer možda može poslužiti kao dodatna motivacija za uvođenje Euklidovog algoritma u nastavu matematike ili informatike.

Pokažimo kako se pomoću Euklidovog algoritma može pronaći tajni ključ d. Primijenimo Euklidov algoritam na brojeve $n = 19976$ i $e = 1805$ (koji su javni):

$$\begin{aligned} 19976 &= 1805 \cdot 11 + 121 \\ 1805 &= 121 \cdot 14 + 111 \\ 121 &= 111 \cdot 1 + 10 \\ 111 &= 10 \cdot 11 + 1 \\ 10 &= 1 \cdot 10 \end{aligned}$$

Krenuvši od pretposljednjeg retka prema gore redom imamo:

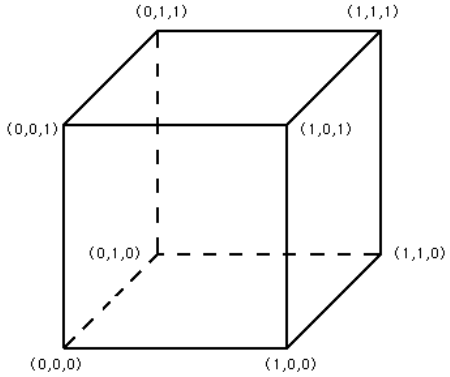
$$\begin{aligned} 1 &= 111 - 10 \cdot 11 = 111 - (121 - 111 \cdot 1) \cdot 11 = 111 \cdot 12 - 121 \cdot 11 \\ &= (1805 - 121 \cdot 14) \cdot 12 - 121 \cdot 11 = 1805 \cdot 12 - 121 \cdot 179 \\ &= 1805 \cdot 12 - (19976 - 1805 \cdot 11) \cdot 179 = 1805 \cdot 1981 - 19976 \cdot 179, \end{aligned}$$

pri čemu smo u svakom drugom koraku izvršili sređivanje izraza. Vidimo da $d = 1981$ zadovoljava uvjet $de \equiv 1 \pmod{n}$

2.6 Primjer (Savršen kôd)**.**

Kriptosustav koji ćemo ovdje opisati spada u kriptosustave s javnim ključem, a primjeren je učenicima srednjih škola. Za početak će nam biti potrebni neki pojmovi iz teorije grafova.

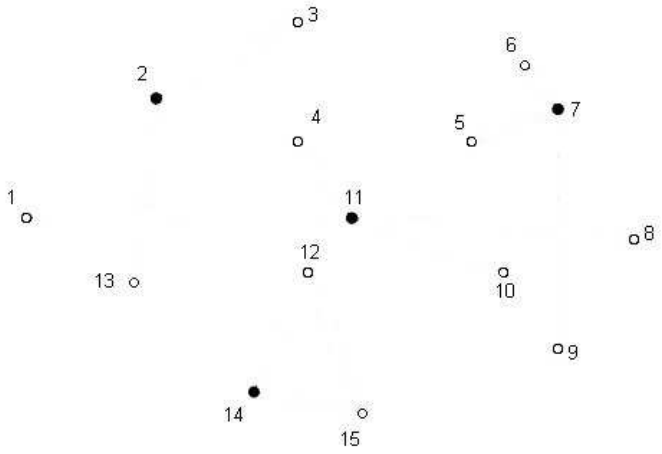
Graf je skup točaka koje nazivamo *vrhovi*, od kojih su neki povezani crtama koje zovemo *bridovi*. *Susjedstvo* danog vrha sastoji se od samog tog vrha, te svih vrhova koji su s njime povezani bridom. *Savršen kôd* u grafu je podskup skupa vrhova sa svojstvom da je svaki vrh grafa u susjedstvu jednog i samo jednog vrha iz tog podskupa. Graf ne mora nužno posjedovati savršen kôd, no grafovi o kojima će ovdje biti riječ imat će jedan ili više savršenih kodova. Za ilustraciju, zamislimo graf kocke koji se sastoji od 8 vrhova i 12 bridova. Svaki par nasuprotnih vrhova predstavlja savršen kôd (npr. vrhovi s koordinatama $(0,0,0)$ i $(1,1,1)$).



Slika 2: Kocka - savršeni kôd $\{(0,0,0),(1,1,1)\}$

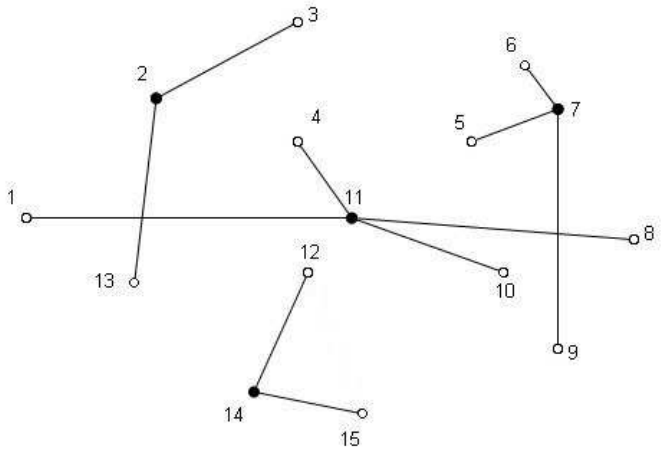
Konstruirati graf sa savršenim kodom je jednostavno, za razliku od pronalaženja istog u danom grafu, što može biti vrlo težak problem. U sljedećih nekoliko koraka opisat ćemo konstrukciju grafa sa savršenim kodom:

- Nacrtamo proizvoljan skup vrhova (za našu svrhu najbolje između 15 i 25), te ih numeriramo zbog lakšeg snalaženja.
- Odaberemo savršen kôd $\mathbf{C}$, odnosno neke od vrhova, te ih zapišemo. Ovi vrhovi predstavljaju naš *tajni ključ*.



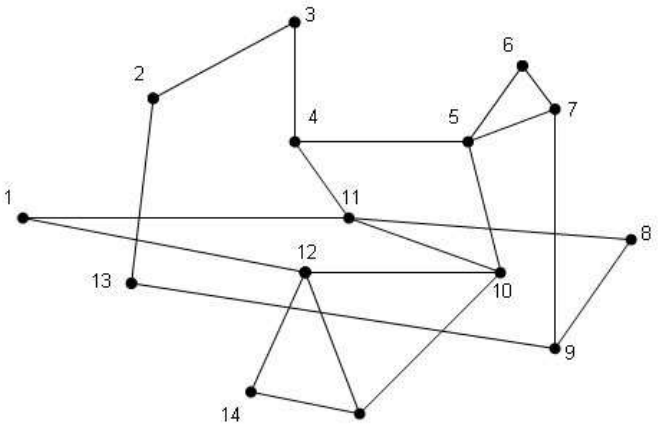
Slika 3: Savršeni kôd $\mathbf{C} = \{2, 7, 11, 14\}$

- Povlačimo bridove od vrhova iz $\mathbf{C}$ ka ostalim vrhovima tako da svaki vrh povezan s točno jednim vrhom iz $\mathbf{C}$. Tako ćemo dobiti "zvijezde" čija su središta točke iz $\mathbf{C}$, a ostali vrhovi predstavljaju "vanjske točke". Na Slici 3 prikazana je jedna od mogućnosti kako to možemo napraviti.



Slika 4: "Zvijezde" sa središtima iz $\mathbf{C}$

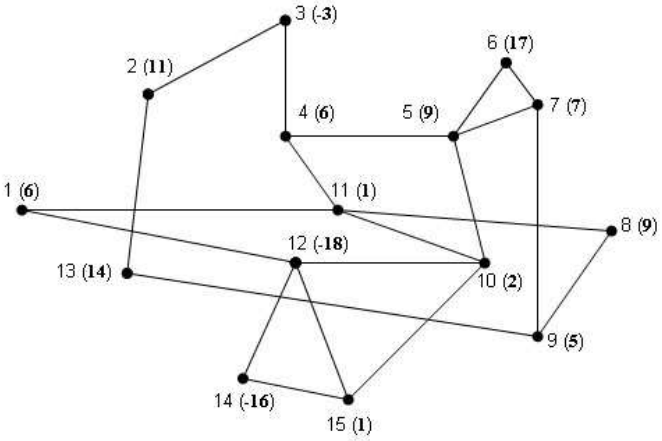
- Prikrivamo formu "zvijezda" tako što povlačimo po volji mnogo bridova između "vanjskih" vrhova. Nipošto ne smijemo vući nove bridove iz središta "zvijezda", jer bi tako pokvarili savršen kôd. Naša konstrukcija je gotova kada se središta "zvijezda" mogu teško uočiti. Ovako dobiveni graf predstavlja *javni ključ*.



Slika 5: Prikrivanje "zvijezda"

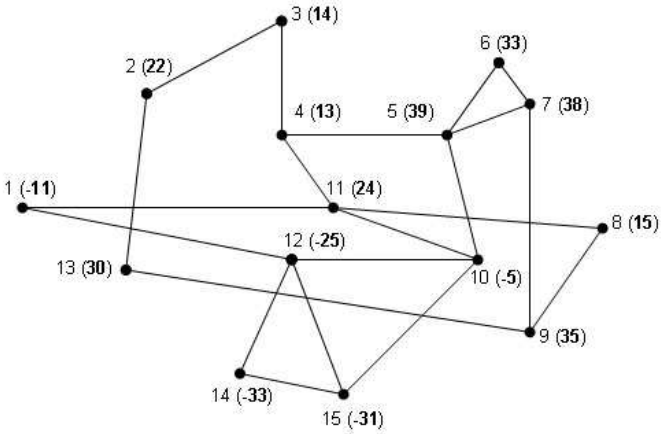
Pretpostavit ćemo da je naš otvoreni tekst neki cijeli broj m između 0 i 100. Šifriranje poruke provodi se u dva koraka, koje ćemo nazvati *plavi* i *zeleni*.

plavi Uz svaki vrh grafa upišimo cijeli broj (može i negativan) x_i tako da je $\sum x_i = m$. Dobro je ove brojeve napisati u nekoj drugoj boji od one kojom su označeni vrhovi, npr. u plavoj, te za njih koristiti naziv *plavi brojevi*. Napomenimo još da plavi brojevi ne bi trebali biti preveliki (po apsolutnoj vrijednosti) zbog lakšeg računanja sljedećeg koraka.



Slika 6: "Plavi" brojevi (u zagradama); otvoreni tekst je 51

zeleni Zbrojimo sve plave brojeve u susjedstvu svakog vrha (uključujući i sam taj vrh), te dobivene vrijednosti upišimo zelenom bojom. Tako smo dobili tzv. *zelene brojeve* i naša je poruka šifrirana! Otvorenim kanalom šaljemo graf na kojem su upisani samo zeleni brojevi i numeracija vrhova, odnosno graf bez plavih brojeva. U praksi vrhovi nisu numerirani, odnosno šalje se graf samo sa zelenim brojevima.



Slika 7: "Zeleni" brojevi (u zagradama)

Poruka se dešifrira tako što se zbroje svi zeleni brojevi uz vrhove iz savršenog koda. Zaista, svaki zeleni broj je zbroj plavih brojeva iz njegovog susjedstva. U zbroju zelenih brojeva iz savršenog koda pojavit će se svi plavi brojevi točno jednom, jer svaki vrh grafa leži u susjedstvu jednog i samo jednog vrha iz savršenog koda. Sigurnost ovog kriptosustava, leži u dobrom kamufliranju savršenog koda, a također i u nedovoljnom poznavanju linearne algebre (od strane protivnika). Naime, jasno je da izvornu poruku možemo odrediti ukoliko su nam poznati plavi brojevi. Njih možemo izračunati pomoću sljedećeg linearnog sustava:

$$\sigma_{1i}x_1 + \sigma_{2i}x_2 + \ldots + \sigma_{ni}x_n = z_i,\ i = 1, \ldots, n,$$

gdje su $x_1, x_2, \ldots, x_n$ plavi brojevi (odnosno nepoznanice), z_i je zeleni broj pri i-tom vrhu, a koeficijenti $\sigma_{1i}, \sigma_{2i}, \ldots, \sigma_{ni}$ su jednaki 0 ili 1. Ako se j-ti vrh nalazi u susjedstvu i-tog vrha, onda je $\sigma_{ji} = 1$, a inače je $\sigma_{ji} = 0$. Sustav se sastoji od n jednadžbi, odnosno onoliko koliko je i vrhova. Za primjer navodimo nekoliko jednadžbi vezanih uz graf sa Slike 6:

$$\begin{aligned}
x_1 + x_{11} + x_{12} &= -11 \quad \text{(iz vrha 1)},\\
x_2 + x_3 + x_{13} &= 22 \quad \text{(iz vrha 2)},\\
&\vdots\\
x_1 + x_{10} + x_{12} + x_{14} + x_{15} &= -25 \quad \text{(iz vrha 12)},\\
&\vdots\\
x_{10} + x_{12} + x_{14} + x_{15} &= -31 \quad \text{(iz vrha 15)}.
\end{aligned}$$

Rješavanjem ovog sustava možemo odrediti izvornu poruku bez poznavanja pripadnog savršenog kôda. No, čak i ako se ovakav sustav postavi, teško je očekivati da će ga učenici

moći riješiti (barem u nekom razumnom vremenu), budući da je n barem 15. Ovaj primjer će možda motivirati ambicioznije učenike da saznaju nešto više o rješavanju takvih sustava ili da se upoznaju s programskim paketima pomoću kojih se oni mogu riješiti.

Literatura

[1] A. V. Borovik, *Implementation of the Kid Krypto Concept*, MSOR Connections, Vol. 2, no. 3 (2002)
http://mathstore.ac.uk/newsletter/aug2002/pdf/crypto.pdf

[2] A. Dujella, *Vigenereova šifra*, math.e 1 (2004),
http://e.math.hr/vigenere/

[3] A. Dujella, *Uvod u teoriju brojeva*, skripta, PMF-Matematički odjel, Zagreb
http://web.math.hr/~duje/utb/utblink.pdf

[4] A. Dujella, *Kriptografija*, skripta, PMF-Matematički odjel, Zagreb
http://web.math.hr/~duje/kript/kriptografija.html

[5] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007 (u pripremi).

[6] M. R. Fellows, N. Koblitz, *Combinatorially based cryptography for children (and adults)*, Congr. Numerantium 99 (1994), 9–41.
http://citeseer.ist.psu.edu/95924.html

[7] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list 5 (2005), 101–112.

[8] N. Koblitz, *Cryptograpy as a teaching tool*, Cryptologia 21 (1997) 317–326.
http://www.math.washington.edu/~koblitz/crlogia.html