Aktivnost 18

Kriptografija – Skritopis

Kako se lahko dva človeka – ali računalnika na internetu – pogovarjata tako, da ju nihče ne more razumeti? Saj to ve vsak otrok: tako, da sporočila zašifrirate. Že, že, kako pa se dogovorita za geslo? Če jima nekdo prisluškuje, bo izvedel tudi geslo, ne? Ne nujno: naučili se bomo, kako si zagotoviti varnost tako, da uporabljamo – javna gesla!

Trajanje

Dve uri

Namen

Spoznavanje preprostih postopkov šifriranja in njihovih omejitev. Razumevanje koncepta javnih ključev.

Potrebščine

Za vsakega učenca

- poli z nalogami iz Cezarjevega šifriranja in tabelo za Vigenerjevo šifro

Za vsako skupino (tri do šest otrok)

- Pola s preprosto mrežo za šifriranje z javnim ključem

Vir: vidra.fri.uni-lj.si; izvirnik: csunplugged.org

Motivacija

Najpomembnejši del aktivnosti, delo z javnim ključem, zahteva precej vztrajnosti in natančnosti, zato je potrebno učence dobro motivirati.

Danes bomo počeli nekaj posebej zanimivega: učili se bomo šifrirati sporočila. Naučili se bomo pošiljati sporočila tako, da jih bodo videli vsi, prebrati pa jih bodo znali samo tisti, ki so jim namenjena. Najprej bomo spoznali preprost način, ki ste se ga morda že domislili tudi sami. Potem pa bomo počeli še nekaj veliko nenavadnejšega: za šifriranje in dešifriranje sporočil navadno potrebujemo skrivne ključe, gesla. Preden nekomu pošljemo skrivno sporočilo, se moramo dogovoriti, na kakšen način ga bomo zašifrirali in s kakšnim geslom. A kaj, če je ta, ki mu pošiljamo sporočilo, nekje na internetu (ali na drugi strani učilnice): kako naj mu sporočimo način šifriranja in geslo, ne da bi ga slišali nepridipravi, ki nam prisluškujejo?

Izmislili si bomo tako imeniten način šifriranja, da boste lahko vsi vsem povedali, kako šifrirate in kakšno geslo uporabljate. Vsak vam bo lahko poslal šifrirano sporočilo, ki ga bodo videli vsi – prebrali pa ga boste lahko še vedno samo vi.

Kako – se to sploh da? Če lahko vsak šifrira sporočilo, ki mi ga pošilja, ga lahko menda tudi vsak prebere? Ne, ne. Počakajte, pa boste videli.

Stari skritopisi

Skritopis je za otroke vedno privlačen. Za začetek pokažimo nekaj starejših načinov šifriranja besedil, ki jim jih ne bo težko uporabljati. Morda so se jih domislili tudi že sami.

Cezarjeva šifra

1. Rimski cesar Julij Cezar naj bi uporabljal naslednji način šifriranja: vse A-je zamenjamo z B-ji, B-je s C-ji, C-je s Č-ji in tako naprej. Ž zamenjamo z A-jem. JOŽE IMA RAD RAČUNALNIŠTVO se tako spremeni v KPAF JNB SBE SBDVOBMOJTUZP.

   Razdeli otrokom pole s Cezarjevo šifro. Naj na enak način skrijejo sporočilo ALENKA PA MATEMATIKO!

2. Kako beremo takšna sporočila? Samo obratno zamenjavo moramo narediti: B zamenjamo z A, C z B, Č z C in tako naprej, do tega, da zamenjamo A z Ž..

   Otroci naj dešifrirajo sporočilo UPOF RB BMFOLP. (Odgovor: TONE PA ALENKO.)

3. V resnici je bil Cezar (ali pa tisti, ki mu je svetoval) še bolj pretkan. Ni vedno zamenjal črke z naslednjo. Včasih se je premaknil tudi za več črk, recimo za tri. Tako je A zamenjal s Č, B z D, C z E, Č z F in tako naprej do konca: V je zamenjal z A, Z z B in Ž s C. Če je hotel na ta način ukazati V NAPAD!, je zapisal A RČŠČG! Tisti, ki je bral sporočilo, je moral vedeti, za koliko črk ga zamakniti.

   Otroci naj preberejo sporočilo DSMZH UH JČOEHA? Lahko si pomagajo s spodnjo sliko, ki kaže, katera črka se spremeni v katero. Pri šifriranju spreminjamo črke iz prve vrstice v one v drugi, pri branju pa obratno.

   ABCČDEFGHIJKLMNOPRSŠTUVZŽ
   ČDEFGHIJKLMNOPRSŠTUVZŽABC

4. Vprašaj otroke, ali se jim zdi Cezarjev način šifriranja varen? Pogovorite se o tem, kdaj je šifriranje varno. Kako bi otroci definirali "varnost" v šifriranju? Pripelji jih do neformalne definicije varnosti: vedno moramo predpostaviti, da prisluškovalec ve, kakšen način šifriranja uporabljamo – to so stvari, ki se razvedo. Šifriranje je varno, če prisluškovalec kljub temu ne more prebrati sporočila, če nima gesla.

5. Je torej Cezarjev način šifriranja varen? Otroci naj poskusijo prebrati sporočilo na dnu učnega lista, FICDU, TDCM VI EUAŽAVD. Daj jim dovolj časa in morda bodo nekateri uspeli.

6. Če je kdo uspel, naj razloži, kako. Sicer namigni: ker je možnih premikov le toliko, kolikor je različnih črk, lahko z malo potrpežljivosti preberemo vsako besedilo. Najprej poskusimo, ali je morda zamaknjeno za eno črko: pač dešifriramo ga, kakor da bi bilo zamaknjeno za eno črko. Če dobimo kaj smiselnega, je to to. Sicer poskusimo, ali je morda zamaknjeno za dve črki. Če še vedno ne dobimo nič

smiselnega, poskusimo s tremi, štirimi in tako naprej. Če ne kasneje, nam bo uspelo pri pomiku za 24 črk naprej (ali eno nazaj, kar je eno in isto).

Skupaj preberite sporočilo FICDU, TDCM VI EUAŽAVD. (Rešitev: CEZAR, PAZI SE BRUTUSA. Besedilo je zamaknjeno za štiri črke.).

7. Brutus je bil eden od izdajalcev, ki so ubili Cezarja. Žal takšnega sporočila Cezarju ni poslal nihče. Če bi mu ga, pa bi ga Cezar najbrž uspel prebrati – če je bil res tako pameten. Sporočila, skrita s Cezarjevo šifro, je, kot vidimo, čisto lahko brati tudi brez ključa. Cezarjeva šifra torej ni uporabna za kaj drugega, kot za igro.

Vigenerjeva šifra

Spoznajmo še en način šifriranja, ki je podoben Cezarjevi šifri.

1. Otroke spomni, kje je problem Cezarjeve šifre: "geslo", ki ga je potrebno vedeti za branje, je zamik. Različnih zamikov pa je tako malo, da lahko poskusimo vse. Problem Cezarjeve šifre bomo je v tem, da moramo le uganiti zamik, pa smo zmagali. Rešili jo bomo tako, da bomo za vsako črko uporabili drugačen zamik. Lahko bi, recimo, zamaknili prvo črko za pet znakov, drugo za deset, tretjo za tri, četrte ne zamaknemo, peto zamaknemo za štiri... Takšno zamikanje bi opisali kot 5, 10, 3, 0, 4. Iz besede CEZAR bi tako nastalo GOBAU – C smo premaknili za 5 znakov (v G), E za 10 (v O), Z za 3 (v B), A za 0 (v A) in R za štiri (v R).

   Lahko pa se dogovorimo, da bomo zamikanja opisovali drugače: namesto 5 bomo rekli D, namesto 10 I, namesto 3 C, namesto 0 A in namesto 4 Č. Namesto 5, 10, 3, 0, 4 bi torej rekli DICAČ. Torej: če besedo CEZAR skrijemo s ključem DICAČ, dobimo GOBAU.

   Takšen dogovor je praktičen, ker lahko za ključ uporabimo kar besedo ali stavek.

2. Učencem razdeli list s tabelo za Vigenerjevo kodiranje (lahko pa si prihraniš kopiranje tako, da ga projeciraš, če bodo otroci lahko razbirali stolpce in vrstice na projekciji).

   Razloži, kako se uporablja tabelo. Na tablo napiši

   D I C A Č
   C E Z A R

   _ _ _ _ _

   Črko D je potrebno premakniti za G. Poiščemo stolpec D in pogledamo, kaj je v vrstici C (ali obratno, ni pomembno). Tam najdemo črko G (napiši jo na prvo črtico). Tako nadaljujemo z ostalimi črkami.

3. Otroci naj s ključem TEGA NE POVEM NIKOMUR skrijejo sporočilo PETER JE HRENOVKE. Posebnih učnih listov ni – naj pišejo sami. Da jih ne bodo begali presledki, pa na tablo napiši

T E G A N E P O V E M N I K O
P E T E R J E H R E N O V K E

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

V geslu smo ignorirali presledke in ga razpisali nad črke sporočila. Uporabili smo le toliko gesla, kot smo ga potrebovali.

Skupaj poiščite prvih nekaj črk (KJCEF...)

4. Otroci naj odkrijejo, kako beremo na ta način skrita sporočila. Recimo, da je naslednje sporočilo UMJG SJUFN skrito s ključem TUDI TEGA NE. Na tablo napiši

T U D I T E G A N

_ _ _ _ _ _ _ _ _
U M J G S J U F N

Otroci naj ga poskusijo prebrati.

5. Prva črka je bila šifrirana s T in dobili smo U. Zanima nas torej, katero črko (vrstica) bi stolpec T spremenul v U. Pogledamo stolpec T in v njem poiščemo črko U. Nahaja se v drugi vrstici, torej vrstici B. Prva črka skritega sporočila je torej B.

   Skupaj z otroki poišči še drugo črko (R). Nadaljujejo naj sami.

6. Mora biti geslo (vsaj) tako dolgo kot sporočilo? Ni nujno. Po potrebi ga lahko ponavaljamo. Če imamo geslo BRUTUS in bi radi skrili besedilo DANES BO PO CEZARJU!, bomo geslo "razširili" v BRUTU SB RU TUSBRUT.

Pogovor

Otrokom povej, da so si to šifro izmislili pred skoraj 500 leti. Skoraj istočasno so se je domislili različni ljudje, po enem od njih jo danes imenujemo Vigenerjeva šifra (izg. Viženerova, gre za Francoza z imenom Blaise de Vigenère). Verjeli so, da je tako skrito besedilo nemogoče prebrati, če nimaš ključa.

Je to res? Se zdi otrokom takšno šifriranje varno? Bi lahko nekdo, ki nima gesla, prebral takšno sporočilo?

Otrokom se bo zdelo to šifriranje verjetno dovolj zapleteno, da je *prav zagotovo tudi varno*.

Razloži jim, da je s stvarjo takole. Če je besedilo dovolj dolgo, geslo pa kratko, tako da ga moramo ponavljati, obstaja relativno preprost postopek, s katerim lahko uganemo geslo in preberemo besedilo. Pred 150 leti ga je odkril Charles Babbage, ki si je, mimogrede, izmislil tudi prvi računalnik. (Vendar ta še ni bil na elektriko, temveč je bil mehanskih – namesto iz čipov je bil sestavljen iz zobatih koles, kot kaka stara ura). Tule si ga ne moremo ogledati, ker bi z daljšimi besedili izgubili preveč časa.

Če je geslo daljše od besedila, pa je postopek – kot so dokazali matematiki – popolnoma varen. Prepričani smo lahko, da besedila, zapisanega na ta način, ne more prebrati nihče.

Da je res tako, je kar lahko videti. Recimo, da prisluškovalec prestreže skrivno sporočilo ŠVIJŽ. Če je geslo IVTTB, se originalno sporočilo glasi JANEZ. Če pa je geslo MEIUU, se sporočilo glasi FRANC.

Z otroki se lahko prepričaš o gornjem. Lahko pa vprašaš otroke, kakšen bi moral biti ključ, da bi bilo originalno sporočilo PETER. Torej, kateri ključ bi zakodiral PETER v ŠVIJŽ?

Vendar zahteva varno šifriranje z Vigenerjevo kodo še dve stvari. Geslo ne sme biti smiselno besedilo, biti mora popolnoma naključno. TEGA NE POVEM NIKOMUR je slabo geslo; dobro geslo bi bilo, recimo ASJI EAIHI SBRHK. Poleg tega smemo vsako geslo uporabiti samo enkrat. Vigenerjevo geslo bo varno le, če upoštevamo ti pravili.

Vprašaj otroke, ali se jim zdi to nerodno.

V resnici je to kar precej zoprno. Takšno šifriranje je uporabno, kadar, recimo, pošiljamo vohuna v daljno deželo, predtem pa si izmislimo zelo zelo dolgo geslo (recimo kar knjigo, ki pa vsebuje le naključne črke).

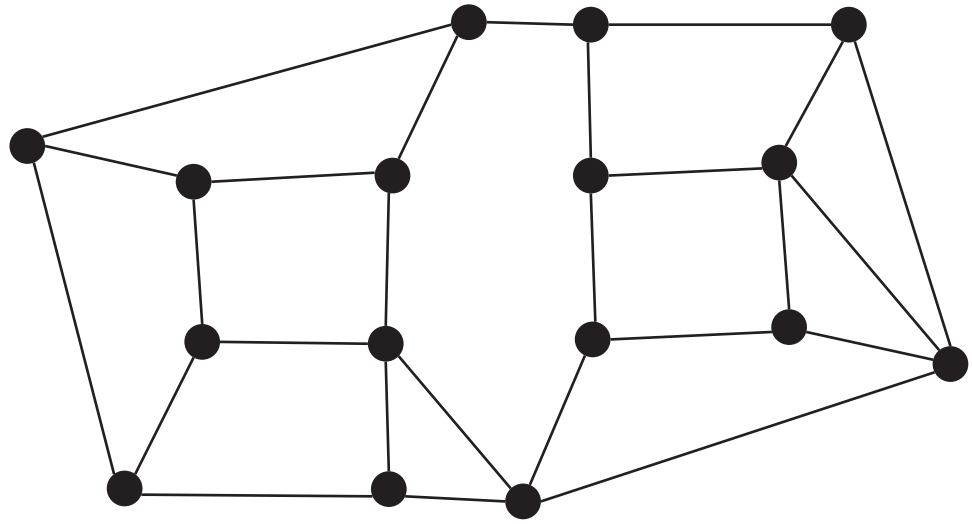
Če se hočemo začeti pogovarjati z nekom, s katerim se poprej nismo na štiri oči dogovorili za geslo, pa imamo problem. Kako naj nekomu pošljemo sporočilo, če mu moramo prej poslati geslo? Prisluškovalec bo pač najprej prisluškoval geslu, potem pa še sporočilu – pa imamo!

Je to nerešljiv problem? Za računalnikarje – posebej, če jim pomagajo matematiki – ni nerešljivih problemov.

Skrita sporočila v mrežah

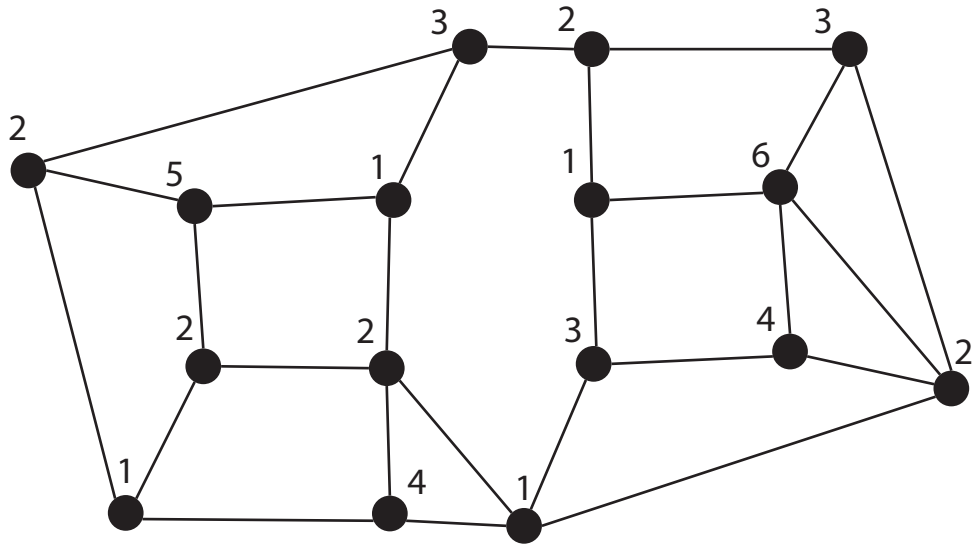
Za začetek si bomo namesto sporočil pošiljali samo številke.

Bob želi, da bi mu lahko drugi pošiljali skrivna sporočila, zato javno objavi svoje geslo. Geslo tokrat ne bo številka (zamik), kot pri Cezarjevi šifri, ali stavek, kot pri Vigenerjevi. Geslo bo mreža! Bobova mreža je takšna:



Ta mreža je javna: Bob jo lahko objavi na spletu, obesi na tablo, pošlje po elektronski pošti vsakemu, ki bi mu rad poslal skrivno sporočilo.

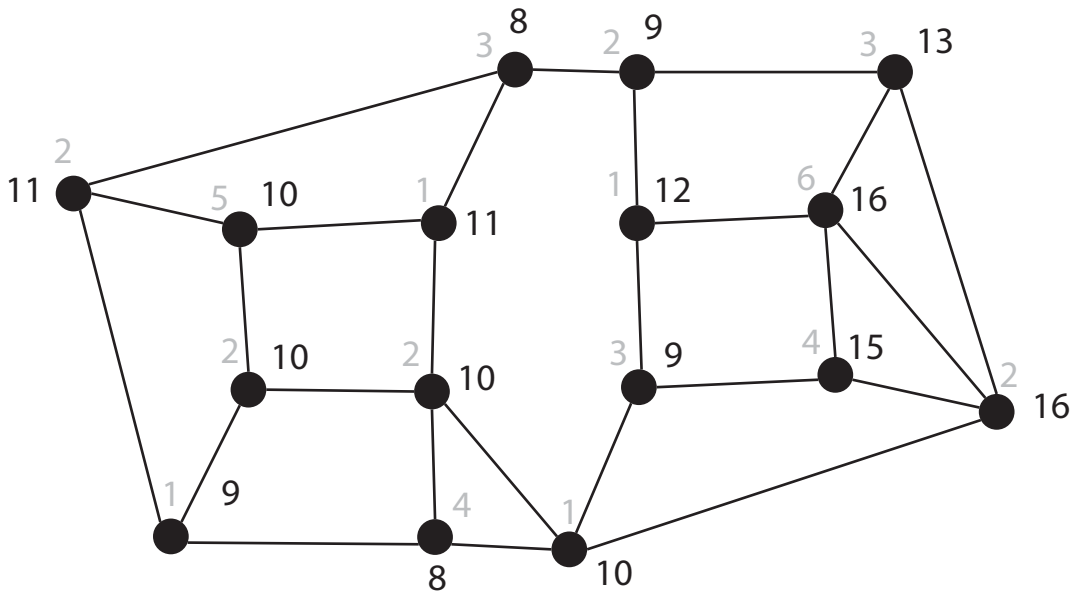
Če želi Ana poslati Bobu skrivno sporočilo, recimo številko 42, naredi tole. Vzame Bobovo mrežo; javna je, torej lahko pride do nje kjerkoli – recimo, da jo je Bob objavil kar na spletu, torej jo Ana pobere od tam. K vsaki točki v mreži napiše številko, tako da je vsota vseh številk 42. Uporabljati sme poljubna, tudi negativna števila. Naredi lahko, recimo, takole:



Opomba: primer po možnosti delaj z otroki. Otroci naj predlagajo svojo številko in sodelujejo pri razporejanju števil. Da se izogneš negativnim številom (tudi, če jih otroci

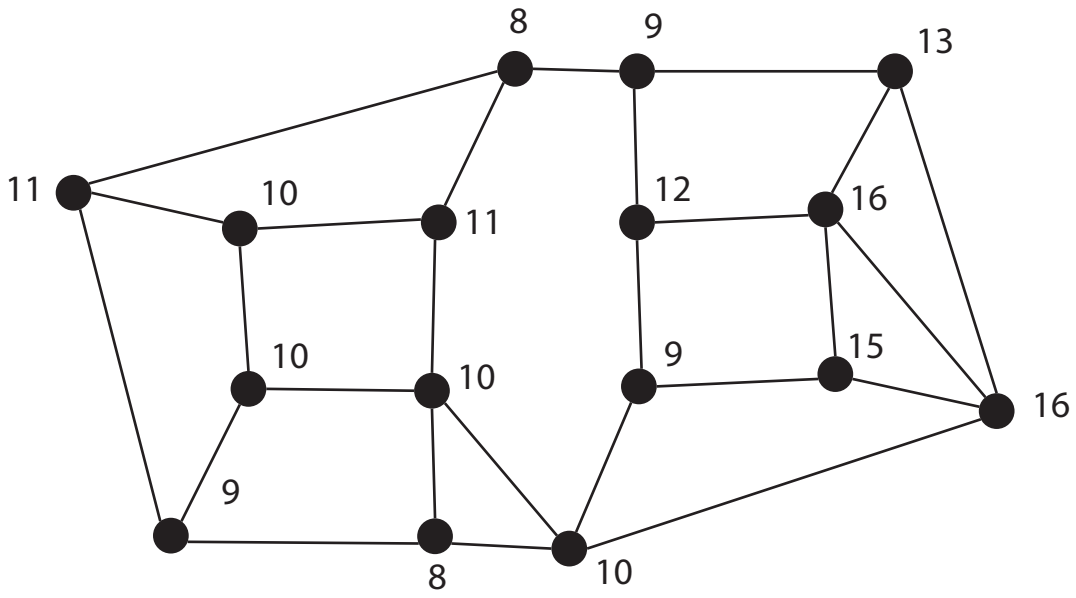
poznajo, se jim izogibaj, ker se boš zaradi njih motil), naj bo predlagano število nekajkrat večje od števila točk, torej vsaj 40.

Nato mora Ana k vsaki točki prišteti številke v vseh točkah, s katerimi je posamezna točka povezana. Vsote napiše k točkam. Za primer: v najbolj levi točki je številka 2, točka pa je povezana s točkami, ki imajo številke 3, 5 in 1. Ana izračuna 2+3+5+1 in k najbolj levi točki zato pripiše 11. To ponovi za vse točke in dobi takšno mrežo.



Opomba: ko delaš z otroki, se utegneš kje pri seštevanju zmotiti. To ni preveč hudo, pazi le, da se ne zmotiš pri tistih štirih točkah, ki jih bo Bob v resnici potreboval v nadaljevanju zgodbe. Ko končaš računanje – vsekakor pa še preden otrokom razkriješ, kako Bob dešifrira sporočilo – preveri, ali vsota v teh štirih točkah ustreza sporočilu, ki ga je poslala Ana! Če ni, si se nekje zmotil; popravi.

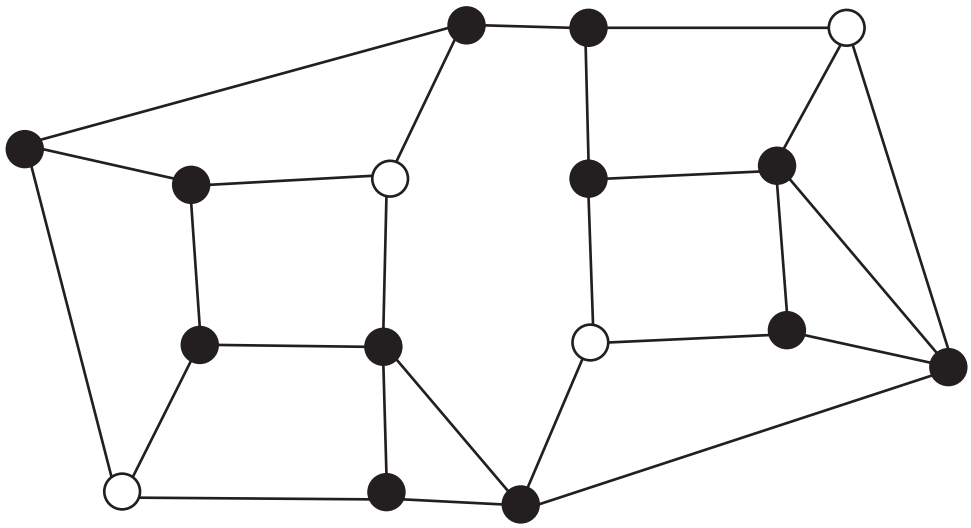
Zdaj skrbno pobriše številke, tako da ostanejo le vsote, ali pa vsote preprosto prepiše na nov list. Ostane ji tole:



Takšno mrežo pošlje Bobu.

Recimo, da Eva, ki jo srčno zanima, kaj Ana sporoča Bobu, slučajno vidi mrežo s temi številkami. Lahko iz njih izračuna številko, ki jo pošilja Ana? Ne, pa čeprav pozna Bobovo mrežo. Še več: če je Ana slučajno pozabila številko, ki jo sporoča Bobu, je iz te mreže ne more več dobiti! Čeprav je sama zašifrirala sporočilo, ga zdaj ne more več odšifrirati!

Odšifrira ga lahko samo Bob. Bob ima skrivnost. Posebno različico svoje mreže. To vestno skriva in je nikoli ne pokaže nikomur.



Če želi Bob prebrati številko, ki mu jo pošilja Ana, le sešteti mora številke v belih točkah njegove skrivne mreže. Te so 9, 11, 9, 13 in njihova vsota je res 42.

Bob ima torej poseben skrivnosten par mrež. Nekako mu je uspelo narediti takšno mrežo, v kateri s pomočjo seštevanja skrije neko številko in le on ve, v vsoti katerih točk mreže se skriva poslano sporočilo.

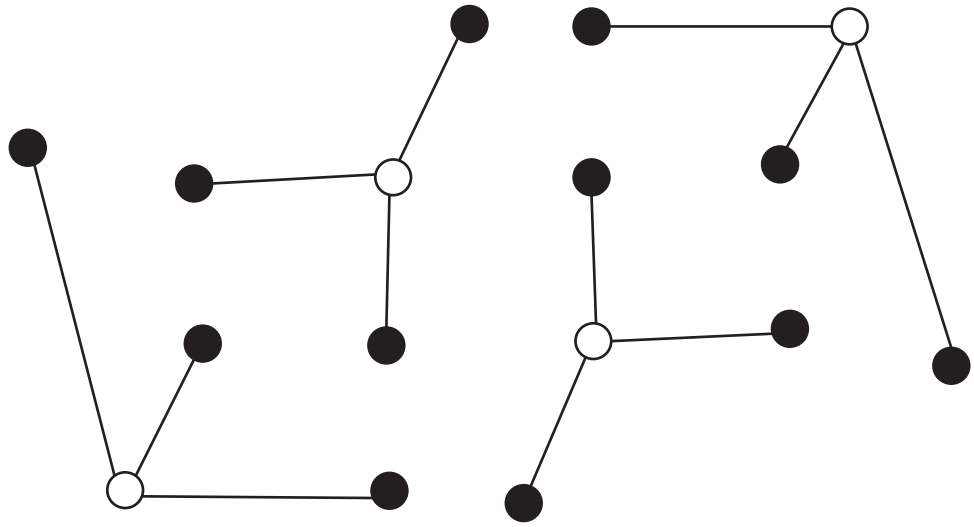
Vsote v ostalih točkah ga sploh ne zanimajo. Ana jih je računala brez potrebe. Pa bi lahko Ani povedal, katere vsote ga bodo v resnici zanimale, da ji ne bi bilo potrebno toliko računati? Ne! Ravno s tem bi razkril svojo skrivno mrežo! Če bi mu Ana poslala le te štiri številke, bi jih znala sešteti tudi Eva.

V dokaz, da postopek res vedno deluje, naj otroci poskusijo še s kakim drugim številom. Pri tem lahko ubereš bližnjico in izračunaš le nekaj točk, ki pa morajo seveda vključevati tudi te štiri.

Zakaj to deluje?

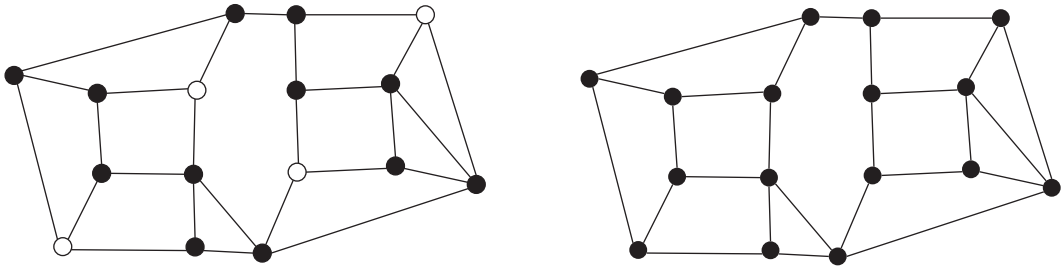
Kako sestavimo takšno mrežo.

Mrežo je dobil tako, da si je najprej izmislil štiri bele točke (lahko bi jih vzel tudi več ali manj) in okrog vsake dorisal nekaj črnih.



Predstavljajmo si, kaj bo (kasneje) naredila Ana: k točkam bo napisala številke, katerih vsota bo 42. Če k vsaki (črni) točki prišteje številke v vseh belih točk, s katerimi je črna točka povezana, bo vsota številk v črnih točkah ravno 42.

Nato je Bob kar naključno povezoval črne točke. Paziti mora le, da ne doda nobene povezave k belim točkam, tako da bodo vsote v njih ostale enake!



Navsezadnje je še pobarval vse bele točke s črno, da jih je prikril.

Lahko zdaj, ko vemo, zakaj postopek deluje in kako so sestavljene mreže, pomagamo Evi dešifrirati sporočilo? Ne: dokler samo Bob ve, katere so črne točke. To, da poznamo delovanje postopka in da vemo celo, kako je Bob sestavil mrežo, nam čisto nič ne pomaga.

Pa lahko iz mreže, ki jo Bob javno objavi (desna slika zgoraj) odkrijemo, katere točke so bile v začetku črne? Zdaj pobrskajmo po spominu: nismo takšnega sestavljanja mrež že nekoč videli? Seveda smo, pri sladoledarjih! Naloge, ki smo jo reševali takrat, je bila ravno določanje začetnih točk. Da bi lahko dešifrirali sporočila, bi morali znati dobro

razpostavljati sladoledarje. Prav ob sladoledarjih pa smo rekli, da gre za nalogo, ki je težka celo za računalnike.

Otroci naj zdaj poskusijo še sami. Uporabijo naj preprostejšo mrežo z druge pole.

1. Razdeli otroke v skupine.
2. Skupinam razdeli pole z javno mrežo; povej, da je to tvoja javna mreža, svoje skrivne pa jim (za zdaj) ne boš pokazal.
3. Vsaka skupina naj si izmisli število, ki ti ga želi poslati in ga zašifrira.
4. Ko ti oddajo pole, naj igrajo vlogo prisluškovalke Eve: premešaj pole med skupinami in vsaka skupina naj poskusi odkriti številko, ki ti jo pošilja neka druga skupina. Morda bo kateri skupini uspelo "razporediti sladoledarje"; če ne, pa bodo videli, za kako težak problem gre.
5. Razkrij jim skrivno mrežo (na dodatni poli). Z njo naj dešifrirajo sporočila.

Če so učenci zmožni, zainteresirani in je na voljo dovolj časa, lahko nadaljujemo tako.

1. Vsak učenec si izmisli svojo mrežo. Učence opozori, da morajo biti mreže preproste: imajo naj tri črne točke in največ pet belih.
2. Vsak učenec "javno objavi" svojo javno mrežo, tako da list z mrežo in svojim imenom prinese na določeno mizo.
3. Določi, kateri učenec naj pošlje skrivno sporočilo kateremu, tako da jim razdeliš skrivne mreže.
4. Vsak učenec naj si izmisli številko, jo zakodira (zapiše vsote na list z javno mrežo) in "pošlje", tako da list vrne lastniku mreže.
5. Lastniki mreže preberejo sporočilo. Pošiljatelj naj pove, ali je rezultat pravilen.

Pogovor

S to metodo kodiranja znamo pošiljati samo številke. Kako pa bi pošiljali, recimo, besedila in slike?

Že od prvih aktivnosti vemo, da lahko besedila in slike zapišemo s številkami. Besedilo spremenimo v številke in jih pošiljamo, kot smo se naučili.

Imate občutek, da je bilo potrebno za pošiljanje ene same številke potrebnega veliko dela? So računalniki dovolj hitri za to?

Računalnik bi bil dovolj hiter za računanje vsot iz te aktivnosti. Vendar bi bil tudi dovolj hiter, da bi razbil to šifro. Računalniki ne uporabljajo *tega* postopka, osnovna ideja *kriptografije z javnimi ključi* pa je takšna, kot smo jo spoznali. "Geslo" ima dva dela, javnega in skrivnega: javni je namenjen šifriranju, skrivni branju. Vsak, ki želi omogočiti drugim, da mu pošiljajo šifrirana sporočila, objavi svoj javni ključ.

Žal pa so postopki, ki jih uporabljamo v resnici, še veliko počasnejši od tega. Metode za šifriranje z javnimi ključi vedno zahtevajo veliko dela. V resnici zato namesto šifriranja z javnimi ključi *v glavnem* uporabljamo hitrejše postopke. Ti pa zahtevajo, da računalniku pošljemo geslo (tako kot smo videli pri Vigenerju, le da uporabljamo postopke, pri katerih se sme geslo večkrat ponoviti). Zato naredimo takole: javni ključ uporabimo zato, da šifriramo geslo (npr TEGA NE POVEM). Takšno geslo pošljemo drugemu računalniku; od tu naprej uporabljamo šifriranje s tem geslom.

Za učitelje: za kaj gre?

V zadnjih aktivnostih smo spoznali le nekaj nalog, ki jih imajo kriptografski postopki: za uvod smo se igrali z žrebanjem, nato smo spoznali enosmerne funkcije, s katerimi lahko skrijemo geslo tako, da ga lahko še vedno preverjamo, čeprav ga ne poznamo, in v tej aktivnosti smo se naučili nekaj o skrivanju sporočil. Še eno pomembno področje je podpisovanje: kako naj napišem sporočilo, za katerega bo nesporno, da sem ga napisal jaz. S tem je povezano tudi zagotavljanje integritete sporočila: kako preverjati, ali je sporočilo prišlo do naslovnika nespremenjeno? Ko prek spletne banke nakažemo denar na nek račun, je pomembno, da banka *ve*, da zahteva res prihaja od nas in da je na poti po internetu od našega računalnika do bančnega nihče ni spreminjal. Samo geslo, ki ga vtipkamo ob vstopu v banko, tu prav nič ne pomaga: kaj če nepridiprav prestreže promet po internetu in spremeni številko računa, na katerega nakazujemo?

Noben od postopkov, ki smo jih spoznali, ni prav varen. Da ni težko prebrati sporočila skritega s Cezarjevo šifro tudi brez ključa, se otroci naučijo sami. Branje Vigenerjeve šifre brez računalnika je prezahtevno za šolsko uro, sam postopek pa ni zapleten. Tule si zaradi poučnosti oglejmo, kako brez ključa brati številke, šifrirane z mrežami.

Označimo točke mreže s številkami 1, 2, 3, ... Originalne številke označimo z b_1, b_2, b_3,..., vsote pa s t_1, t_2, t_3,... Vsote t so izračunane iz b, recimo

$$t_1 = b_1 + b_2 + b_5$$
$$t_2 = b_3 + b_2 + b_8$$
$$t_3 = b_1 + b_3 + b_4$$

in tako naprej.

Prisluškovalec vidi vsote t, zanimajo pa ga b-ji. To pa ni nič drugega kot sistem linearnih enačb: enačb je toliko, kolikor je točk v mreži, neznank pa prav toliko. Bobova mreža ima 16 enačb s 16 neznankami; za računalnik je reševanje takšnih sistemov trivialno. Tudi pri deset tisoč enačb z deset tisoč neznankami se vaš prenosnik še ne bi začel potiti in poganjati ventilatorja.

Poučno pri zgodbi je to, da je razporejanje sladoledarjev sicer težko opravilo, vendar je mogoče šifro razdreti tudi po drugi poti.

Osnovno načelo kriptografije z javnimi ključi pa je v aktivnosti vseeno pravilno prikazano: lastnik skrivnega ključa *ve* nekaj, kar bi bilo iz javnega ključa zelo težko in zamudno izračunati. Pogosto uporabljani postopki temeljijo na praštevilih. Z računalnikom je preprosto poiskati dve stomestni praštevili. Če ju zmnožimo, dobimo dvesto mestno sestavljeno število; tega števila ne zna nihče razcepiti nazaj v prafaktorja. V postopku RSA, ki je osnova večine javne kriptografije in podpisovanja, sta tisto, kar *ve*, lastnik skrivnega ključa, prafaktorja, v javnem ključu pa je le njun produkt. Razumevanje postopka žal zahteva več matematike, kot jo poznajo šolarji, poleg tega pa ga je nemogoče izvajati ročno.

Kako varni so ti postopki? Kriptografija je zelo aktivno raziskovalno področje. Ali obstaja učinkovit algoritem iskanja prafaktorjev, ne vemo. (Vemo, da je razcep na prafaktorje trivialen za kvantne računalnike, vendar jih za zdaj še ne znamo izdelovati.)

Prav tako ne vemo, ali obstajajo tudi za postopke, kot je RSA, obvozi, ki ne zahtevajo faktorizacije, tako kot smo pravkar videli, da lahko šifriranje z mrežo razbijemo tudi brez iskanja optimalnega pokritja, s preprostim reševanjem sistema linearnih enačb.