19 veikla

Vaikai šnipai. Viešojo rakto kriptografija

Santrauka

Kriptografija – tai mokslas apie matematikos ir informatikos metodus informacijai šifruoti ir iššifruoti. Kriptografija leidžia saugoti ypač slaptą informaciją ir siųsti ją nesaugiais tinklais (pvz., internetu), kad jos negalėtų perskaityti niekas kitas, o tik teisėtas gavėjas.

Šifravimas yra informacijos saugumo esmė. Anksčiau, jei viena pusė norėdavo nusiųsti slaptus duomenis kitai, pirma turėdavo duomenis užšifruoti tam tikru raktu, paskui rasti būdą, kaip saugiai tą raktą pateikti kitai pusei. Šią saugumo problemą išsprendė viešojo rakto kriptografija. Šiuolaikinis informacijos šifravimas grindžiamas dviem raktais – viešuoju (duomenims užšifruoti) ir privačiuoju (duomenims iššifruoti). Viešasis raktas gali būti duodamas kam tik norima, o privatusis – saugomas. Viešuoju raktu užšifruoti duomenys gali būti iššifruoti tik privačiuoju raktu.

Paprasčiau kalbant, kas nors nusiperka spyną, ant jos užrašo savo vardą ir padeda ant stalo, kad kiti galėtų ja naudotis. Raktas, žinoma, lieka pas spynos savininką. Tarkime, kad kas nors nori jums išsiųsti pranešimą, taigi įdeda tą pranešimą į dėžutę, užrakina ją jūsų spyna ir išsiunčia. Net jei ta dėžutė nukeliautų klaidingu adresu, niekas negalėtų jos atidaryti, nes raktą nuo spynos turite tik jūs. Dėl šios priežasties nėra būtinybės perduoti spynos rakto siuntėjui.

Šios veiklos skyriuje aiškinama, kaip tai galima padaryti skaitmeniniu būdu. Skaitmeniniame pasaulyje naudojama „spynos“ kopija. Jei realiame pasaulyje būtų daroma spynos kopija, būtų išsiaiškintas jos užraktas ir, aišku, atkurtas raktas. Tačiau skaitmeniniame pasaulyje nereikia išrasti naujo rakto, o tik nukopijuoti „spyną“ visiškai nesigilinant, kas joje.

Atrodo, kad tai neįmanoma. Pažiūrėkime ir įsitikinkime.

Ryšiai su ugdymo programomis

- ✓ Technologija: viešojo rakto kriptografija, slaptas kodas

Gebėjimai

- ✓ Ryšių nustatymo

Amžius

- ✓ Nuo 11 metų

Priemonės

- ✓ Projektorius „Vaikų šnipų pranešimo užšifravimas“ pateikčiai demonstruoti
- ✓ Lipniųjų lapelių schemoms komentuoti

Kiekvienai mokinių grupei reikės:

✓ Dviejų darbo lapų „Vaikų šnipų žemėlapiai“

Vaikai šnipai

Įvadas

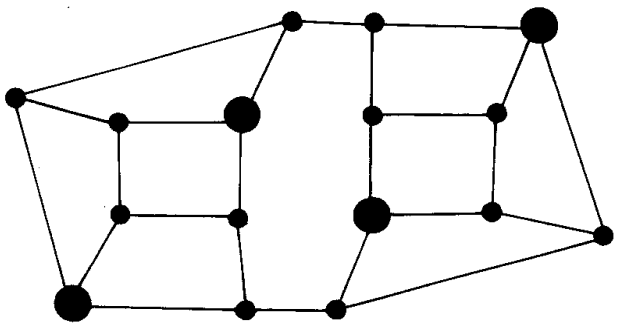
Ši veikla techniškai yra sudėtingiausia iš visų šioje knygoje aprašytų veiklų. Norint ją sėkmingai atlikti iki galo reikia kruopštaus darbo ir susikaupimo. Mokiniai turi būti susipažinę su vienos krypties funkcijomis (15 veikla Turistų miestas). Būtų lengviau atlikti šią veiklą, jei mokiniai atliktų šios aukščiau aprašytas šios dalies veiklas (17 veiklą Dalijimasis paslaptimi ir 18 veiklą Monetos metimas). Čia mokiniams bus reikalinga tai, ko išmoko atlikdami 1 veiklą Taškų skaičiavimas ir 5 veiklą Dvidešimt spėjimų..

Ema planuoja siųsti Bilui slaptą žinutę. Paprastai slapta žinutė suprantama kaip sakinys ar keletas sakinių, tačiau šiame pratime Ema siųs tik vieną skaičių, kuris simbolizuoja vieną ženklą. Iš tikrųjų tai atrodo labai paprasta, turint galvoje, kad ji galėtų siųsti sakinį, sudarytą iš tokių ženklų, be to, tai bus padaryta dar ir kompiuteriu. Tačiau kartais net labai trumpi pranešimai yra labai svarbūs: vienas žinomiausių pranešimų istorijoje, siųstas Polo Reviro (Paul Revere), turėjo tik dvi galimas reikšmes. Emos pranešimas bus siunčiamas naudojant Bilo viešąjį raktą, todėl, net jei patektų į kitas rankas, jo nebūtų galima iššifruoti. Tik Bilas gali iššifruoti Emos pranešimą, nes tik jis turi raktą nuo „spynos“.

Pranešimas užšifruojamas naudojantis žemėlapiu. Tai ne Lobių salų žemėlapis iš ankstesnės veiklos, o panašus į Turistų miesto žemėlapį iš 15 veiklos. Jame linijos vaizduoja gatves, o taškai atitinka gatvių sankryžas. Kiekvienas žemėlapis turi viešąją (spyną) ir privačiąją (raktą) versijas.

Diskusija

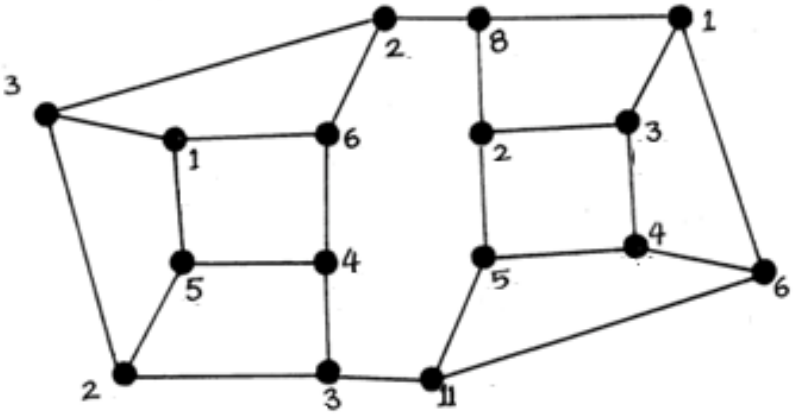
Darbo lape „Vaikų šnipų pranešimo užšifravimas“ vaizduojamas Bilo viešasis žemėlapis. Jis nėra slaptas, Bilas jį pateikia viešai (ant stalo ar tinklalapyje), kad kiekvienas galėtų jį pamatyti, arba duoda jį tam žmogui, kuris nori jam išsiųsti pranešimą. Ema taip pat turi šio žemėlapio kopiją.



Paveiksle dešinėje yra Bilo privatusis žemėlapis. Jis panašus į viešąjį, tik kai kurie taškai paryškinti. Šis žemėlapis yra saugomas, kad niekas jo nematytų.

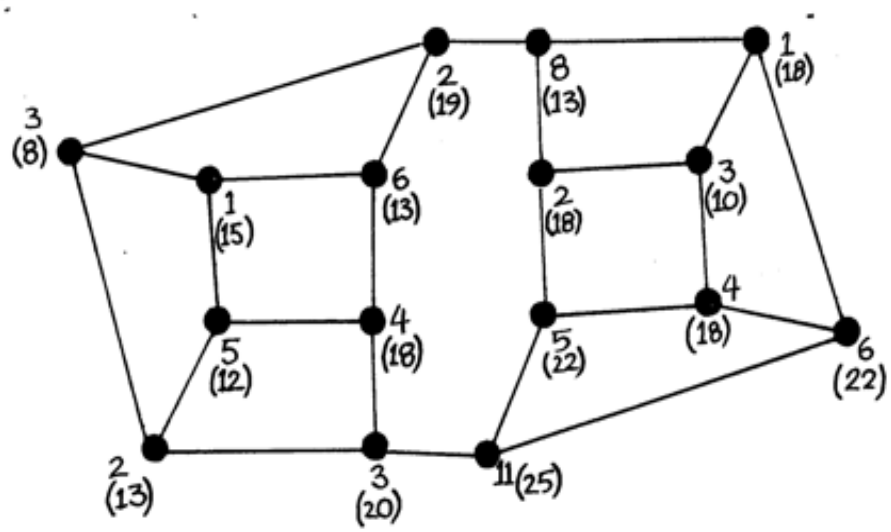
Rekomenduojama šią veiklą atlikti su visa klase, nes čia reikia daug kruopštaus darbo. Nors viską padaryti nėra sunku, tačiau nedidelė klaida sukelia nemažai problemų. Svarbu, kad mokiniai įsitikintų, jog šis šifravimo būdas iš viso įmanomas. Taigi jiems reikės palaikymo atliekant šią daug pastangų reikalaujančią užduotį. Mokinius motyvuoja tai, kad šiuo metodu galima perduoti slaptus pranešimus vienas kitam ir net mokytojas, nors žino, kaip pranešimai buvo užšifruoti, negali jų iššifruoti.

1. Mokiniams parodomas Bilo viešasis žemėlapis („Vaikų šnipų pranešimo užšifravimas“). Sugalvojamas skaičius, kurį Ema norėtų siųsti. Prie kiekvienos gatvių sankryžos žemėlapyje surašomi atsitiktiniai skaičiai, kurių suma lygi siunčiamam Emos skaičiui. Žemiau pavyzdyje Ema sugalvojo siųsti 66, todėl prie gatvių sankryžų surašyti galimi skaičiai, kurių suma yra 66. Prireikus galimi ir neigiami skaičiai.



2. Toliau Ema turi nuspręsti, ką nusiųsti Bilui. Žemėlapio ji siųsti negali, nes bet kas kitas gali nesunkiai iš jo perskaityti pranešimą.

   Taigi ji pasirenka bet kurią sankryžą ir sudeda jos skaičių su trijų gretimų sankryžų skaičiais. Gautą sumą Ema užrašo skliaustuose (arba kita spalva) po pasirinktos sankryžos skaičiumi. Pavyzdžiui, žemiau pateikto viešojo žemėlapio dešinėje pusėje, apačioje, esančios sankryžos, pažymėtos skaičiumi 6, gretimų sankryžų skaičiai yra 1, 4 ir 11. Visų keturių skaičių suma yra 22– ji užrašyta skliaustuose po 6. Šiuos skaičiavimus reikia pakartoti su kiekviena sankryža žemėlapyje. Taip gausime skaičius skliaustuose.



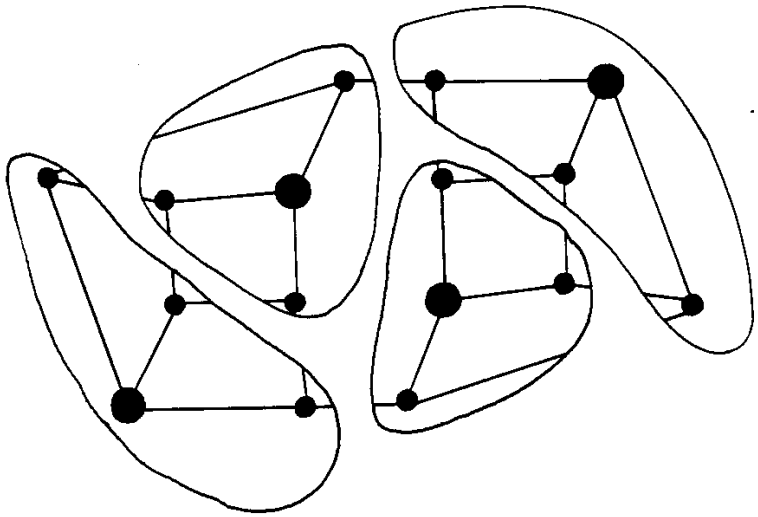
3. Ema nusiunčia Bilui žemėlapį, kuriame prie gatvių sankryžų surašyti tik skaičiai skliaustuose.

   Prieš siunčiant Bilui galima nutrinti ne skliaustuose esančius skaičius arba perrašyti skaičius skliaustuose į žemėlapio kopiją. Tada galima paprašyti mokinių spėti, kokie buvo pirmieji užrašyti skaičiai. Vargu ar jiems tai pavyks.

4. Tik su Bilo privačiuoju raktu galima iššifruoti Emos pranešimą. Bilo privačiajame žemėlapyje yra pažymėti (padidinti) taškai.

   Norėdamas iššifruoti pranešimą Bilas pasižiūri į pažymėtus taškus ir sudeda jų skaičius. Pavyzdyje Bilas sudeda skaičius 13, 13, 22 ir 18. Suma yra 66 – Emos siųstas pranešimas.

5. Kaip tai veikia? Viskas priklauso nuo žemėlapio. Privačiajame Bilo žemėlapyje pasirenkama viena iš pažymėtų sankryžų ir apvedama sritis, apimanti ją ir gretimas, per vieną gatvę nuo jos esančias sankryžas. Taip padaroma ir su kitomis pažymėtomis sankryžomis, kaip parodyta žemiau paveiksle. Tokiu būdu žemėlapis padalijamas į nesusikertančias sritis. Kiekvienos srities pažymėtos sankryžos skaičius gaunamas sudėjus visų tos srities sankryžų pradinius skaičius. Kadangi sritys nesusikerta, pažymėtų sankryžų suma yra visų sankryžų pradinių skaičių suma ir lygi siunčiamam skaičiui.



Atrodo, tiek daug darbo siunčiant vieną skaičių! Pažiūrėkime, kas buvo atlikta: persiųstas visiškai slaptas pranešimas naudojant viešąjį raktą, be jokio išankstinio dalyvių susitarimo. Dabar galima skelbti savo viešąjį raktą skelbimų lentoje (ar kur kitur) ir bet kas gali siųsti slaptas žinutes, bet niekas negali jų iššifruoti be privačiojo rakto. Realiame gyvenime visus skaičiavimus atlieka programinės įrangos paketas, paprastai integruotas į interneto naršyklę, todėl sunkiai dirba tik kompiuteris.

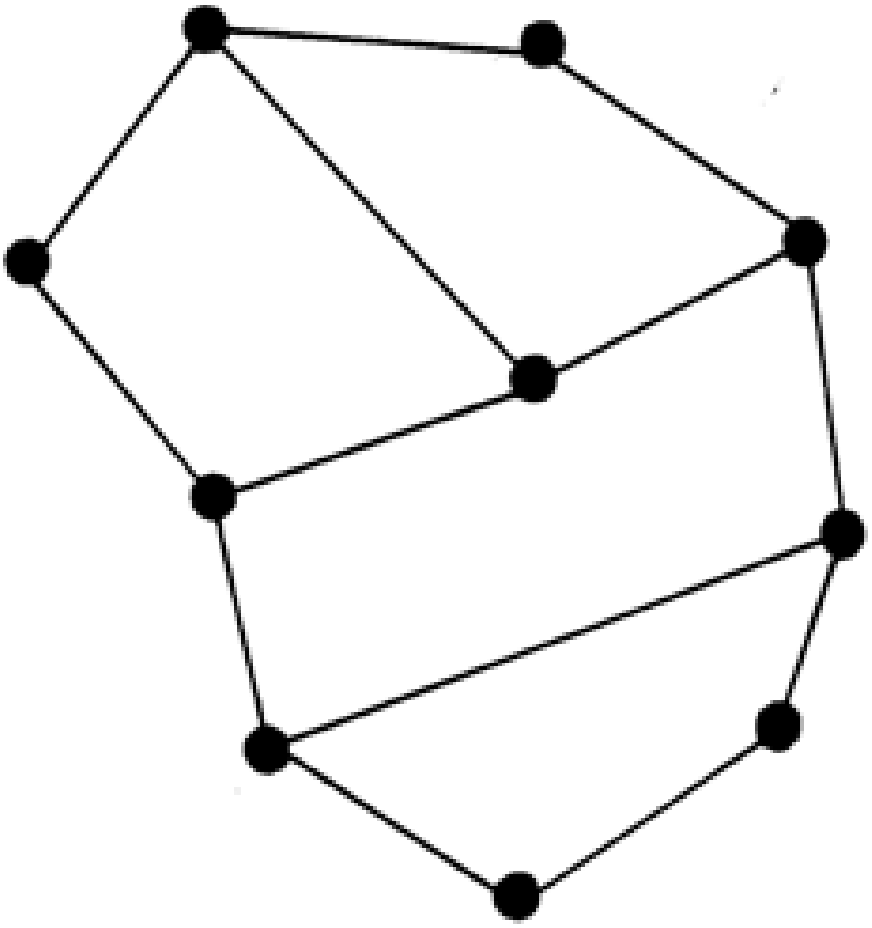
Tikriausiai mokiniams įdomu sužinoti, kad dabar jie yra išskirtinės grupės nariai, kurie naudodami viešąjį raktą šifravo rankiniu būdu. Informatikai mano, kad ši užduotis yra beveik neįmanoma, ir tik keletas žmonių yra bandę tai daryti.

Viešojo žemėlapio sudarymas yra labai panašus į ledų furgonų sustatymą Turistų mieste (15 veikla). Žemėlapį nesunku sudaryti, jei pradedama nuo sričių braižymo privačiajame žemėlapyje, lygiai kaip žymint sankryžas, kur turėtų stovėti ledų furgonai, o paskui sujungiant jas gatvėmis „Turistų miesto“ uždavinyje. Spręsti „Turistų miesto“ uždavinį labai sudėtinga, jis sprendžiamas perrinkimo metodu. Tarkime, Bilas pradėtų nuo labai sudėtingo žemėlapio su 50 ar 100 sankryžų. Regis, niekas negalėtų įveikti tokio šifro, net protingiausi matematikai, kaip ir „Turistų miesto“ uždavinyje įrodyti, kad parinktas furgonų skaičius yra mažiausias.

6. Su visa klase išnagrinėjus vieną pavyzdį mokiniai padalijami į grupes po 4. Kiekvienai grupės porai duodamas Darbo lapas su viešuoju žemėlapiu. Kiekviena pora susigalvoja siunčiamą „pranešimą“ (tai gali būti bet koks sveikasis skaičius), užšifruoja jį ir perduoda savo rezultatą kitai grupės porai. Šie bando iššifruoti, bet, aišku, jiems prireikia privačiųjų žemėlapių. Ar pavyksta mokiniams iššifruoti pranešimus su privačiuoju raktu?
7. Kiekviena pora gali pabandyti sukurti savo žemėlapį. Privatųjį žemėlapį jie saugo, o viešąjį duoda kitai grupės porai arba pakabina klasės lentoje. Žemėlapio kūrimo metodika panaši kaip ir ledų furgonų – sužymimi taškai ir tada sujungiami gatvėmis. Privačiajame žemėlapyje nubraižomos sritys, kuriose pažymimas vienas taškas ir iš jo išvedami du ar trys keliai, kurių gale pažymimas kitas taškas. Šie taškai sujungiami gatvėmis su kitų sričių tokiais pat taškais.

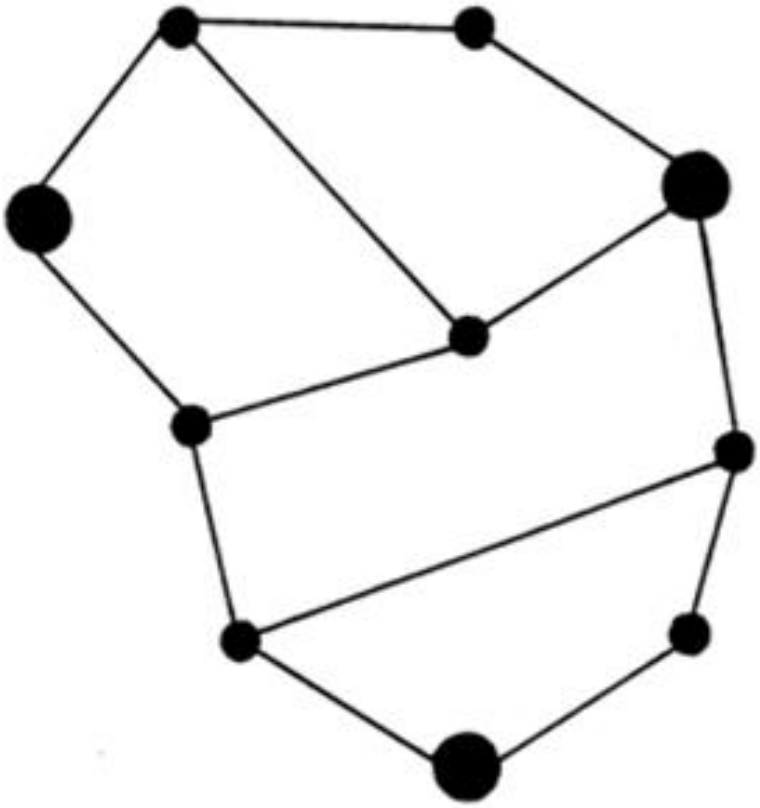
Darbo lapas *Vaikų šnipų viešasis žemėlapis*

Naudodamiesi žemėlapiu užšifruokite pranešimus.



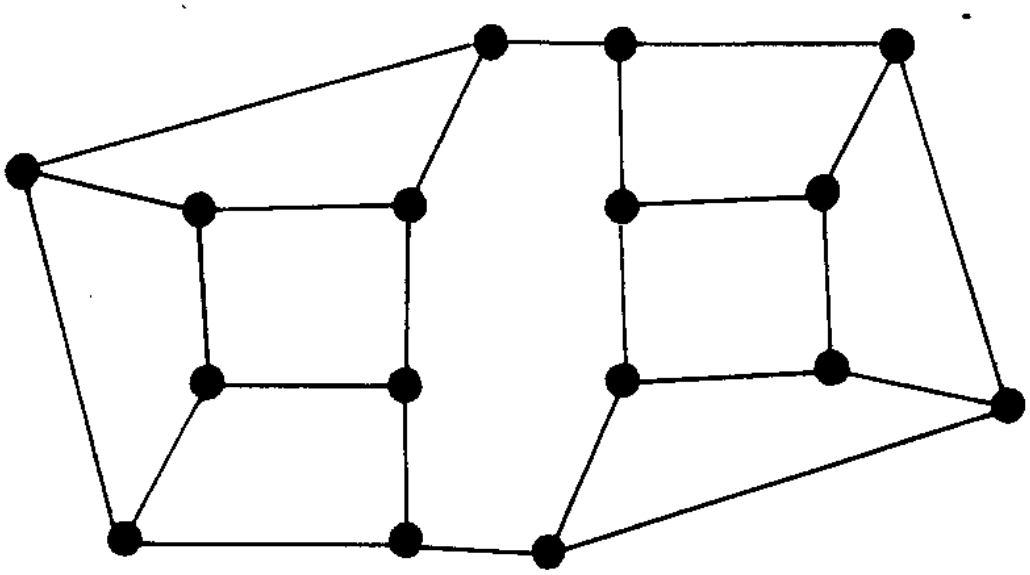
Darbo lapas *Vaikų šnipų privatusis žemėlapis*

Naudodamiesi šiuo žemėlapiu iššifruokite pranešimus.



Vaikų šnipų pranešimo užšifravimas

Šiuo žemėlapiu rodoma, kaip užšifruojamas pranešimas.



Apie ką visa tai?

Aišku, dauguma nori siųsti slaptus pranešimus kompiuterių tinklais taip, kad tik tikrasis gavėjas galėtų juos perskaityti. Be abejo, yra daug būdų tai padaryti, jei siuntėjas ir gavėjas dalijasi šifravimo raktu, bet viešojo rakto šifravimo esmė yra ta, kad siuntėjas gali siųsti slaptą pranešimą gavėjui be išankstinio susitarimo, tiesiog pasiėmęs viešosios „spynos“ kopiją tinklalapyje.

Saugumas yra tik viena kriptografijos pusė. Kita pusė yra autentifikavimas: ar gali Ema būti tikra, kad gautas pranešimas yra tikrai nuo Bilo, o ne nuo kokio apsimetėlio siuntėjo? Įsivaizduokime, Bilas siunčia elektroninį laišką: „Brangioji, aš nebeturiu pinigų ir negaliu grįžti. Prašau pervesti į mano banko sąskaitą 100 €. Mano sąskaita 0241–45–784329.Su meile – Bilas.“ Ar Ema gali būti tikra, kad laišką siuntė Bilas? Šiuo atveju gali būti naudojama viešojo rakto kriptosistema. Kai tik Ema nusiunčia Bilui slaptą pranešimą, kurį užšifruoja jo viešuoju raktu, šis gali siųsti jai pranešimą, kurį tik jis pats gali sugeneruoti užšifruodamas savo privačiuoju raktu. Jei gautą pranešimą Ema gali iššifruoti viešuoju Bilo raktu, vadinasi, pranešimas yra tikrai nuo Bilo. Žinoma, pranešimą gali iššifruoti bet kas kitas, nes naudojamas viešasis Bilo raktas, tačiau Bilas galėtų dar kartą užšifruoti siunčiamą pranešimą Emos viešuoju raktu. Šis dvigubas šifravimas užtikrina ir saugumą, ir autentifikavimą pagal tą pačią viešojo ir privačiojo rakto schemą.

Reikia pripažinti, kad šioje veikloje aprašoma schema yra panaši į rimtą sudėtingą viešojo rakto šifravimo sistemą, tačiau praktiškai nėra saugi, nes realybėje naudojami daug didesni žemėlapiai.

Priežastis ta, kad, nors sprendimas, kaip išdėstyti mažiausiai ledų furgonų bet kuriame žemėlapyje, nežinomas ir šioje veikloje pateiktas būdas atrodo saugus, tačiau visiškai kas kita, kai norima nulaužti. Vargu ar šis klausimas iškils mokiniams, bent jau jaunesniems, tačiau reikia bent žinoti, kad tokia problema egzistuoja. Galite bent pasakyti, kad nagrinėjamas šifravimo būdas yra saugus, tačiau matematiškai nėra pagrįstas. Jei jums neįdomi matematika, galite ignoruoti tolesnius samprotavimus.

Sunumeruokime susikirtimų taškus žemėlapyje: 1, 2, 3 ir t. t. Pradiniai susikirtimų skaičiai žymimi b_1, b_2, b_3, ..., o perskaičiuoti $-t_1$, t_2, t_3, ... Tarkime, kad 1 susikirtimas yra sujungtas su 2, 3 ir 4. Tada

$t_1 = b_1+b_2+b_3+b_4$ (1)

Panašias lygybes galima pritaikyti visiems susikirtimams. Visose lygybėse yra nežinomieji kaip 1 lygybėje b_1, b_2, b_3, ... Visi mato viešąjį žemėlapį ir perskaičiuotus skaičius t_1, t_2, t_3, ..., gali išreikšti visus perskaičiuotus skaičius kintamaisiais, vaizduojančiais pradinius skaičius. Gautą lygybių sistemą galima išspręsti lygčių sprendimo programa. Nustatomi pradiniai skaičiai, apskaičiuojama jų suma ir gaunamas siųstas skaičius (pranešimas). Taigi nereikia atkurti privačiojo žemėlapio. Ši lygčių sistema sprendžiama Gauso eliminavimo metodu, todėl skaičiavimo laikas yra proporcingas lygčių skaičiaus kubui. Tačiau, kadangi šių lygčių dauguma koeficientų

lygūs 0, yra dar spartesnių sprendimo būdų. Palyginus šį būdą su eksponentiniu skaičiavimo laiku, iššifravimo žemėlapis sudaromas daug greičiau.

Tikimės, kad nesijaučiate apgauti! Tiesą sakant, skaičiavimai, susiję su realiomis viešojo rakto kriptosistemomis, yra labai panašūs į tuos, kurie buvo atliekami šioje veikloje. Tik realios viešojo rakto kriptosistemos šifruoja įvairiais ir daug sudėtingesniais metodais, kuriais šifruoti rankiniu būdu net neįmanoma. Vienas iš saugiausių viešojo rakto metodų, naudojamų šiuolaikinėse šifravimo sistemose, yra grindžiamas sudėtingu didelių skaičių daugiklių skaičiavimu.

Kokie yra 100 ženklų skaičiaus
9.412.343.607.359.262.946.971.172.136.294.514.357.528.981.378.983.082.541.347.
532.211.942.640.121.301.590.698.634.089.611.468.911.681 daugikliai? Neužtrukite per ilgai skaičiuodami!

Šio skaičiaus daugikliai yra
86.759.222.313.428.390.812.218.077.095.850.708.048.977 ir
108.488.104.853.637.470.612.961.399.842.972.948.409.834.611.525.790.577.216.753.

Tik šie du skaičiai yra pateiktojo 100–ženklio skaičiaus daugikliai ir jie yra pirminiai. Šių skaičių galingas superkompiuteris ieškojo keletą mėnesių.

Dabar realioje viešojo rakto kriptosistemoje Bilas gali naudoti iš 100 skaitmenų sudarytą skaičių kaip viešąjį raktą ir du jo daugiklius kaip privatųjį raktą. Sukurti tokius raktus nėra sunku: reikia tik būdo pirminiams skaičiams rasti. Taigi randami gana dideli du pirminiai skaičiai, jie sudauginami. Sandauga yra viešasis raktas, o pirminiai skaičiai – privatusis raktas. Kompiuteris nesunkiai gali sudauginti du didelius skaičius. Kai toks didelis viešasis raktas, niekas negali įspėti privačiojo rakto, nebent galėtų prieiti prie superkompiuterio ir turėtų keletą mėnesių laiko. O jeigu vietoj 100 skaitmenų viešasis raktas būtų sudarytas iš 200 skaitmenų, daugiklių radimas užtruktų metų metus. Tokio rakto nulaužimo sąnaudos yra daug didesnės, negu informacijos, kuri būtų juo iššifruota, vertė. Praktiškai 512 bitų ar didesni raktai, kurie yra ekvivalentūs apie 155 skaitmenų po kablelio ar daugiau, dažnai sudaromi saugiems ryšiams užtikrinti.

Vis dar nėra būdo, kaip užšifruoti pranešimus pirminiais skaičiais grindžiamu viešuoju raktu, kad jo nebūtų galima iššifruoti be privačiojo rakto. Čia netinka metodas, kai du pirminiai skaičiai naudojami kaip privatusis raktas, o jų sandauga– kaip viešasis raktas, užuot skaičius išskaičiavus iš sandaugos. Raktą būtų galima nulaužti išskaidant skaičių dauginamaisiais. Šiaip ar taip, galima įveikti šiuos sunkumus ir sukurti tinkamą užšifravimo ir iššifravimo algoritmą, tačiau čia to nenagrinėsime. Jau ir taip daug ką padarėme.

Ar saugi pirminiais skaičiais grindžiama sistema? Didelių skaičių skaidymas dauginamaisiais – tai problema, kurią pasaulio matematikai sprendžia jau keletą šimtmečių, bet geresnio metodo, kaip perrinkti visus daugiklius, neatrasta (kad toks metodas neegzistuoja, taip pat neįrodyta). Vienaip ar kitaip, reikia būti budriems: jei

galima nulaužti Bilo raktą nesprendžiant „Ledų furgonų“ uždavinio, tai gali būti, kad pirminių skaičių raktas gali būti nulaužtas neperrenkant visų daugiklių.

Nerimą kelia tai, kad, jei yra tik keli galimi pranešimai, piktavalis asmuo bet kurį iš jų gali užšifruoti viešuoju raktu ir palyginti tikrąjį pranešimą su visomis galimybėmis. Emos metodu galima to išvengti, nes atsiranda daug būdų, kaip užšifruoti tą patį pranešimą, priklausomai nuo prie kodų vertės pridedamų skaičių. Praktiškai kriptografijos sistemos kuriamos taip, kad būtų per daug galimų pranešimų, todėl net nevertėtų visų jų bandyti net labai sparčiu kompiuteriu.

Iki šiol nežinoma, ar galima greitai išspręsti skaidymo pirminiais dauginamaisiais uždavinius. Niekam nepavyko sukurti , bet taip pat niekas neįrodė, kad tokio metodo nėra. Jei būtų surastas efektyvus šio uždavinio sprendimo algoritmas, daugelis šiandieninių kriptografijos sistemų taptų nesaugios. IV dalyje buvo aptarti NP sudėtingumo uždaviniai: jei bent vienas iš jų būtų išsprendžiamas, būtų galima išspręsti juos visus. Kadangi tiek daug (nesėkmingų) pastangų įdėta ieškant efektyvaus NP sudėtingumo uždavinių sprendimo algoritmo, tai skaidymo daugikliais uždaviniai puikiai tiktų kuriant saugias kriptosistemas. Šiandien kriptografija yra aktyvi informatikos tyrimų sritis.

Daugiau informacijos

1987 m. Davido Harelo knygoje „Algorithmics“ aptariami skaitmeniniai parašai ir su jais susiję kriptografijos protokolai. Joje aprašoma, kaip žaisti pokerį telefonu.

1982 m. Dorothy Denning knygoje „Cryptography and data security“ išsamiai aprašoma kriptografija.

1989 m. Alexanderio Keewatino Dewdney knygoje „Turing Omnibus“ yra skyrius apie Bulio logiką, kuriame aptariamas loginių schemų sudarymas.