# Aibių teorija

1. Aibės apibrėžimas, aprašymo būdai

Aibė – tai objektų rinkinys, kuriems galioja tam tikras bendras požymis. Elementai aibėse nesikartoja, jų išsidėstymo tvarka nėra svarbi. Aibės dažniausiai žymimos didžiosiomis lotyniškomis raidėmis. Aibė, kuri neturi nei vieno elemento vadinama tuščia aibe ir žymima Ø. Jei x yra aibės A elementas, sakysime, kad x priklauso aibei A ir žymėsime xA. Jei x nėra aibės A elementas, žymėsime xA. Aibės nusakymas išvardinant elementus A={a, b, c, … }. Aibės galia – aibės elementų skaičius, žymėjimas - |A|. Aibė vadinama baigtine, kai jos galia baigtinė, ir begaline, kai galia begalinė. Jei aibės A visi elementai priklauso aibei B, tai aibė yra vadinama aibės B poaibiu.

1. Veiksmai su aibėmis. Veno diagramos ir jų panaudojimas

Sąjunga – aibė, kurioje yra abiejų aibių elementai. Žymima AᴜB.

Sankirta – aibė, kurioje yra tik bendri abiejų aibių elementai. Žymima A∩B.

Skirtumas – aibė, kuri susideda iš A aibės ir neturi tų pačių elementų kaip aibė B. Žymima A\B.

Veno diagramos – diagramos, skirtos vaizduoti grafiškai ryšius tarp aibių ir veiksmus su aibėmis. Veno diagramose aibe vaizduojama kaip skritulys. Jei aibės turi vienodų elementų, tai aibių skrituliai susikerta.

1. Pagrindiniai dėsniai taikomi veiksmams su aibėmis
2. Jei aibė A yra aibės B poaibis, o B aibės C poaibis, tai aibė A yra aibės C poaibis.
3. Idenpotitiškumas - aibės A sąjunga arba sankirta su aibe A yra lygu aibei A.
4. Komutatyvumas - AᴜB = BᴜA, A∩B= B∩A
5. Asociatyvumas – (AᴜB)ᴜC=Aᴜ(BᴜC)
6. Distributyvumas - A∩(BᴜC)=(A∩B)ᴜ(A∩C)
7. Padengimas - (AᴜB)∩A= A, (A∩B) ᴜA= A
8. Santykiai (Sąryšiai)

Santykis – dviejų aibių Dekarto sandaugos poaibis. Pvz. A={a, b}, B={1, 2, 3}. AxB={(a, 1),(a, 2), (a, 3), (b, 1), (b, 2), (b, 3)}. „Daugiau“ santykio pvz.: >:R(NxN) R= {(2,1), (3,1), (3,2),…}

Santykių savybės:

1. Refleksyvus – jei visame a R a visiems a A (visi elementai sąryšyje su pačiais savimi)
2. Simetriški – jei a R b reiškia, kad b R a (sąryšis abipusis)
3. Antisimetriškis – jei a R b ir b R a galioja tik tuomet, kai a = b (sąryšis neabipusis)
4. Tranzityvus – jei a R b, b R c reiškia, kad a R c (sąryšis perduodamas)
5. Funkcijos. Funkcijų tipai: injekcija, siurjekcija, bijekcija

Funkcija – tai santykis, kuris sieja vieną aibės elementą tik su vienu kitu aibės elementu. Pirmoji aibė vadinama funkcijos apibrėžimo sritimi, antroji – reikšmių sritimi.

Tipai:

1. Injekcija – funkcija, kuri skirtingiems aibės A elementams priskiria skirtingus elementus iš aibės B.
2. Siurjekcija – funkcija, kuri skirtingiems aibės A elementams priskiria bent po vieną elementą iš aibės B.
3. Bijekcija – funkcija, atvaizduojanti aibę A ir aibę B taip, kad kiekvienam a yra tik vienas b, ir kiekvienam b yra tik vienas a. Bijekcija, jei funkcija yra injekcinė ir siurjekcinė.

# Kodavimo teorija

1. Kodavimo sistemos

Yra pozicinės skaičiavimo sistemos ir nepozicinės. (Pozicinės, kur skaičiaus dydis priklauso nuo jo pozicijos)

1. Dešimtainė skaičiavimo sistema.
2. Sveikųjų skaičių. N=2k.
3. Slankaus kablelio. N=±M\*P±r M – mantisė, r – eilė (sveikasis skaičius), P – skaičiavimo sistemos pagrindas.
4. Dekartinės koordinatės.
5. Abėcėlinis kodavimas.
6. Optimalus kodavimas.
7. Šenono – Fano kodas.
8. Hafmeno kodas.
9. Romėniški skaičiai.
10. Grėjaus kodas. Cikliniai / acikliniai kodai. Hemingo atstumas

Grėjaus kodas – dvejetainis kodas, kurio bet kurios dvi gretimos kombinacijos skiriasi tik per vieną poziciją.

Cikliniai kodai – tiesinis kodas, kuriam nuosekliai didėjant skaičiui, kinta tik viena skiltis vienu metu (pvz. Grėjaus kodas).

Aciklininiai kodai – tiesinis kodas, kuriam nuosekliai didėjant skaičiui, kinta ne tik viena skiltis vienu (pvz. Paprastas dvejetainis sk. Didinimas).

Hemingo atstumas – skaičius, kuris rodo neatitikimų kiekį tarp dviejų sekų (Grėjaus kode visada 1).

1. Grėjaus kodo savybės ir pritaikymai

Grafų teorijoje - Hamiltono ciklų generavime ir kt. Uždaviniuose.

Bulio funkcijų minimizavimams – Karno diagramos konstravimas.

Klaidas taisančiuose koduose informacijos perdavime.

Kampinio pasisukimo šifravime.

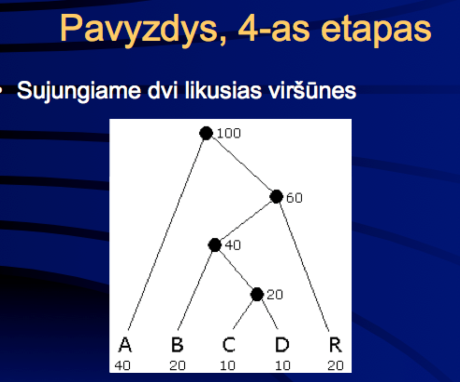
1. Duomenų kodavimas. Kodavimo tikslai

Kodavimas – informacijos pakeitimas kodu (simbolių seka) arba vieno kodo pakeitimas kitu. Kodavimo tikslas – pritaikyti informacijos formą konkrečiam taikymui. Kodavimas naudojamas – duomenų vaizdavimas kompiuterio atmintyje, informacijos apsauga, klaidų ištaisymas siunčiant nepatikimais ryšių kanalais, duomenų spaudimas duomenų bazėje.

1. Duomenų suspaudimas, tiksliai ir kriterijai, būdai, panaudojimo sritys

Duomenų spaudimas – duomenų kodavimas, leidžiantis gauti trumpesnį kodą nei pradinis. Spaudimo kokybė išreiškiama spaudimo koeficientu, kuris matuojamas procentais ir parodo kiek procentų suspaustas pranešimas yra už orginalą. Panaudojimo sritys – duomenų perdavimas iš vienos vietos į kitą, duomenų bazių dydžių mažinimas. Tikslas – kuo didesnis spaudimo koeficientas neprarandant orginalių duomenų.

Lempelo – Zivo algoritmas.



1. Hafmeno algoritmas

Hafmeno kodavimas – mažos reikšmės užkoduojamos trumpais žodžiais.

Algoritmas – nustatomas koduojamų simbolių dažnis tekste – dvejetainio medžio

konstravimas (koduojamus simbolius medyje atitinka kabančios

viršūnės) – simbolių kodų generavimas.

1. RLE algortimas

Suranda pasikartojančių duomenų seką ir ją pakeičia trumpesne struktūra (pvz. aaaabbbedffff – a4b3e1d1f4 arba a4b3edf4).

# Kombinatorika

1. Įvadas. Kombinatorikos objektai ir uždaviniai

Kombinatorika – matematikos sritis, kuri nagrinėja kiek skirtingų kombiancijų, tenkinančių vienokių ar kitokių kombinacijų galima sudaryti iš turimų objektų. Kombinatorikos objektas – baigitnės diksretinės aibės. Pagrindiniai uždaviniai:

1. Perskaičiavimas ir išvardymas – rasti kiek duotosios aibės elementų tenkina tam tikrą sąlygą
2. Išvardijimas – rasti visus elementus, kurie tenkina nurodytą sąlygą
3. Klasifikacija – galimi uždavinio sprendimai klasifikuojami tik pagal tam tikrą požymį
4. Optimizavimas – uždaviniai, kuriuose apibrėžiama tikslo f-ija ir ieškoma jos ektremumo
5. Duotosios aibės poaibiai. Sutvarkytos aibės

Jei aibės A visi elementai priklauso aibei B, tai aibė yra vadinama aibės B poaibiu. Aibė A, kurioje apibrėžtas tvarkos sąryšis R, vadinama sutvarkyta. Sutvarkyta aibė vadinama visiškai sutvarkyta, jei bet kurie du aibės A elementai yra palyginami. Tokiu atveju sąryšis R vadinamas tiesinės tvarkos sąryšiu. Priešingu atveju sąryšis R vadinamas dalinės tvarkos sąryšiu, o aibė iš dalies sutvarkyta.

1. Junginiai (deriniai, kėliniai, gretiniai)

Bet koks n-elementinės aibės k-elementinis poaibis yra vadinamas tos aibės deriniu iš n elementų po k elementų. Derinių skaičius lygus:

Skirtingos surikiuotos aibės aibės, besiskiriančios tik elementų aibės tvarka, vadinamos kėlinais.

Bet koks surikiuotas n-elementinės aibės k-elementinis poaibis yra vadinamas tos aibės gretiniu iš n elementų po k elementų. Gretinių skaičius:

1. Skaidiniai. 2-os eilės Stirlingo skaičiai. Belo skaičius

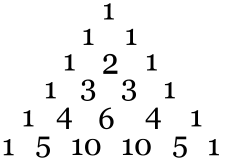
Aibės A poaibiai B1, B2, ... Bk yra tokie, kad :

1. Bj≠ Ø
2. Bi∩Bj=Ø visiems i ≠j
3. B1ᴜ B2ᴜ ... ᴜBk=A

Tada poaibių B1, B2, ... Bk rinkinys yra aibės A skaidinys. Tokių skaidinių skaičius vadinamas 2-os eilės Stirlingo skaičiumi. Visų aibės A (|A|=n) skaidinių skaičius vadinamas Belo skaičiumi.

1. Polinominė formulė. Niutono binomas. Binominiai koeficientai

Niutono binominė formulė – teorema, padedanti rasti dvianrio, pakelto n –tuoju laipsniu skleidinį.

1. Binominės tapatybės. Paskalio trikampis
2. 

Paskalio trikampis

1. Rekurentinių išraiškų metodas. Fibonači skaičiai

Rekurentinių išraiškų metodas – kombinatorikos uždavinio sprendimas, kai turime objektą su n elementų, susideda į analogiško uždavinio sprendimą su mažesniu objektų skaičiumi: tai atliekama rekurentinės išraiškos pagalba. Fibonači skaičiai – begalinė skaičių seka, kurio n-tasis narys yra lygus n-1 ir n-2 narių sumai.

1. Aibių sąjungos elementų skaičiaus radimas. Priskirties / išskirties metodas

n(A1ᴜA2ᴜ...ᴜAn) = n(A1) + n(A2) + ... + n(An) - (A1∩A2) - (A1∩A3) - ... - (An-1∩An) - n(An-1∩An) + ... + (-1)n-1n(A1∩A2∩...∩An)

Ši formulė gali būti įrodoma matematinės indukcijos metodu:

1. Teorema galioja, kai n = 2
2. Ji galioja, kai elementų skaičius n-1
3. Reikia parodyti, kad ji teisinga, kai elementų skaičius n.

Priskirties / išskirties metodas taikomas dviejų aibių sąjungos atveju:

1. Dviejų - |AᴜB| = |A| + |B| -|A∩B|
2. Trijų - |AᴜBᴜC| = |A| + |B| + |C| -|A∩B|-|A∩C|-|B∩C|+|A∩B∩C|
3. Generuojančių funkcijų metodas. Enumeratoriai. Denumeratoriai

Kombinatorinių uždavinių, kuriuose reikia apskaičiuoti objektų, tenkinančių nurodytas sąlygas, sprendinys dažnai būna seka a0, a1, a2, ... , an. ak – ieškomų k „matavimų“ objektų skaičius. Sekai gali būti priskiriama formali eilutė: A(x) = a0 + a1x + a2x2+...+anxn. Ji vadinama šią seką generuojančia funkcija.

Enumeratorius: e\*(z) = (1+ a1z)(1+ a2z)...(1+ anz) Atskliaudę gauname:

e\*(z) = 1+ (a1+ a2+... an)z + (a1a2+ a1a3+...+ an-1an)z2+ ... + (a1a2...an)zn

Taip išvardinami visi deriniai po vieną elementą (prie z), po du elementus(prie z2) ir t.t.

Denumeratorius: d\*(z)= (1+z)n=1 + Cn1z+Cn2z2+...+ Cnnzn. Atitinkami koeficientai yra galimų derinių skaičiai.

# Kriptografija

1. Įvadas. Kritografijos tikslai, uždaviniai, pagrindinės sąvokos

Kriptografija – mokslo šaka, sprendžiantielektroninnės infromacijos saugumo problemas.

Tekstograma – pradinis neužšifruotas tekstas.

Šifrograma – užkoduotas tekstas.

Šifras – algortimas paverčiantis tekstogramą į šifrogamą.

Raktas – tam tikra svarbi informacija, kurią žino tik siuntėjas ir gavėjas.

Kriptoanalizė – šifrogramos analizė nežinant šifro ir rakto.

Užkodavimas – tekstograma paverčiama į šifrogramą.

Dekodavimas – šifrograma paverčiama į tekstogramą.

1. Kritptografinių sistemų saugos analizė. Informacijos konfidencialumas. Informacijos vientisumas. Informacijos šaltinio autentifikavimas

Visiškai saugių kriptografinių sistemų nėra. Bet kurią kriptografinę sistemą galima nulaužti. Tačiau kartais reikalingi resursai norint nulaužti sistemą kainuos daugiau nei gaunama nauda iš nulaužtos sistemos. Informacija gali būti nebeaktuali kai sistema bus nulaužta. Tokios sistemos laikomos pakankamai saugiomis. Kriptologija yra naudojam tam, kad užtikrinti informacijos perdavimo saugumui. Saugumas reikalauja, kad informacija būtų pasiekama tik tam, kam ji skirta.

Informacijos konfidencialumas – siunčamos informacijos užtikrinimas, kad ją galės perskaityti tik siuntėjas.

Informacijos vientisumas – siunčiant informaciją ji nebuvo pakeista.

Subjekto autentifikavimas – turi būti galimybė įsitikinti, kad duomenų siuntėjas yra tikrai tas, kas ir turi būti.

1. Įsibrovimo tipai (pasyvus / aktyvus)

Pasyvieji – tik stebi perduodamos informacijos srautą, į jį nesikiša.

Aktyvieji – ne tik stebi, bet ir patys įsiterpia, bando suklastoti ar perimti duomenų paketus, apsimeta legaliais vartotojais.

1. Klasikinė kriptografija. Monoalfabetiniai šifrai. Cezario šifras

Klasikinė kriptografija – vieno slapto rakto sistema.

Monoalfabetinia šifrai – kai vienas tekstogramos simbolis visada atitinka vienas ir tas pats šifrogramos simbolis.

Cezario šifras – užšifravimo būdas, kuomet viena lotyniškos abecelės raidė pakeičiama „kažkiek“ toliau esančia raide. Lotyniška abecelė turi 26 skirtingas raides. Maksimalus raktų skaičius – 25. Jei tekstą pastumsime per 26 pozicijas, gausime orginalų raštą.

1. Šifravimo būdai. Kriptoanalizė. Polialfabetiniai šifravimo būdai

Pagrindiniai šifravimo būdai – raidžių pakeitimas, sukeitimas vietomis. Monoalfabetiniai šifravimo būdai nėra saugūs, nes juos galima nulaužti žinant kokia kalba jie buvo parašyti, turint omenyje kokios tos kalbos savybės – raidžių dažnumas ir pan.

Kriptoanalizė – šifrogramos analizė nežinant šifro ir rakto.

Polialfabetinis šifravimas – šifravimas, kuriame negalime nustatyti vienareikšmės atitikties: vieno teksto simbolio su šifrografiniu simboliu. Vienas tekso simbolis gali būti koduojamas skirtingai įvairiose pozicijose.

1. Šiuolaikinės šifravimo sistemos. Srautiniai ir blokiniai šifratoriai

Šiuolaikinės šifravimo sistemos:

Elektroninis parašas – asimetrinis šifravimas, kai duomenys užšifruojami privačiu raktu, o atšifruojami viešu raktu.

Veišojo rakto (asimetrinė) kriptosistema (VRK) – sistema, kurios kriptografinės funkcijos realizuojamos naudojant matematiškai susijusią raktų porą. Du raktai: privatus (žinomas tik savininkui), viešas (prieinamas visiems).

Blokinis šifravimas – tekstograma suskaidoma į blokus ir kiekvienas blokas šifruojamas atskirai. Blokiniais šifrais užšifruojami dideli fiksuoto ilgio duomenų blokai.

Srautinis šifravimas – naudojamas, kai visos tekstogramos negalima užšifruoti iš karto. Tad naudojant srautinį šifravimą galima šifruoti kiekvieno pranešimo simbolį atskirai, todėl kiekvienas simbolis užšifruotas vis kia f-ija. Srautiniai šifrai atsparūs perdavimo klaidų išplitimui. Taip pat būdinga greitaeigiškumas.

1. Šiuolaikinių šifravimo sistemų tipai: simetrinė / asimetrinė

Simetrinė šifravimo sistema – naudoja vieną slaptą raktą, žinomą tik siuntėjui ir gavėjui. Privalumas: greitis. Trūkumas: raktą galima pamesti, jį gali sužinoti kiti asmenys, raktą reikia perduoti saugiais šaltiniais.

Asimetrinė šifravimo sistema – viešojo rakto sistema. Informacija yra užkoduojama gavėjo/siuntėjo viešuoju raktu, o siuntėjas/gavėjas išsiširuoja privačiu raktu. Privalumai: gera apsauga, nereikia specialių kanalų raktams perduoti. Trūkumai: ilgas užšifravimas/atšifravimas.

1. Simetrinės šifravimo sistemos principai

Simetrinė šifravimo sistema – sistema, kai visoms kriptografinėms funkcijoms atlikti naudojamas tas pats slaptas raktas. Naudojami du pagrindiniai principai – pakeitimas ir perstatymas.

1. Asimetrinės šifravimo sistemos prinicipai

Kiekvienas vartotojas turi savo privatų ir viešą raktą. Žinutė yra užkoduojama siuntėjo/gavėjo privačiu/viešu raktu ir atkoduojama siuntėjo/gavėjo viešu/privačiu raktu. Pagrindinis trūkumas – greitaveika. Taip pat pažeidžiamas brute-force tipo atakoms.

1. Dviejų pagrindinių šifravimo sistemų palyginimas

Simetrinės sistemos raktas turi būti slaptas, jį turi žinoti abi bendraujančios pusės. Asimetrinėje sistemoje tik privatūs raktai turi būti saugomi. Reikia patikimos sistemos, kur būtų saugomi asimetriniai viešieji raktai. Simetrinės sistemos reikalauja daugybės raktų dideliame tinkle. Asimetrinius raktus nėra būtina keisti dažnai, simetrinius reikia keisti dažnai. Tekstogramos užšifravimas simetriniu būdu užtrunka daug kartų greičiau nei asimetrinių. Simetriniai raktai kelis kartus trumpesni, nei asimetriniai.

1. Maišos (hash) funkcija. Reikalavimai maišos funkcijoms. Jos panaudojimo sritys

Kriptografine maišos funkcija vadinama dėsninga procedūra, kuri paiima bet kokį informacijos kiekį ir po tam tikro operacijų skaičiaus grąžina fiksuoto ilgio maišos funkcijos reikšmę. Maišos reikšmė yra tokia, kad bet koks pradinės informacijos pakeitimas privers grąžinti kitokią reikšmę. Reikalavimai maišos funkcijoms:

1. Maišos funkcija turi būti paskaičiuojama nesudėtingai bet kokiam informacijos pranešimui
2. Neįmanoma sugeneruoti pranešimo, kuris jau turi duotąją maišos reikšmę
3. Neįmanoma pakeisti pranešimo nepakeičiant maišos rezultato reikšmės
4. Neįmanoma rasti dviejų skirtingų pranešimų su ta pačia maišos rezultato reikšme

Naudojimas: pranešimo autentifikavimo koduose (MAC), skaitmeniniams parašams realizuoti, aptikti netyčinį arba sąmoningą pakeitimą koduose.

1. Pranešimo autentifikavimo kodas (MAC)

Pranešimo autentifikavimas siejasi:

1. Pranešimo vientisumo užtikrinimas
2. Pranešimo šaltinio nustatymas
3. Užtikrina, kad siuntėjas negali paneigti, jog išsiuntė pranešimą

Pranešimo kodo autentifikavimo sistemą sudaro: fiksuoto dydži duomenų masyvas ir raktas. Užtikrina, kad informacija nepakeista, leidžia identifikuoti siuntėją. MAC nėra skaitmeninis parašas, jis neužtikrina pasikartojimą. MAC gali sugeneruoti bet kas, kas turi simetrinį raktą, bet jį turi nevienas žmogus.

1. Skaitmeninis parašas

Skaitmeninis parašas patvirtina informacijos siuntėjo autentiškumą ir patvirtina, kad informacija nebuvo pakeliui pakeista. Skaiteminis parašas yra asimetrinė šifravimo sistema.

1. Skaitmeninio parašo patvirtinimas (CA – Certificate Authority). Viešo rakto infrastruktūra (PKI), jos f-ijos

Patvirtinti parašą reikalinga patikima trečioji šalis, kuri palaiko visą viešojo rakto infrastruktūrą. PKI jungia viešą raktą su asmeniu.

1. Matematiniai kriptografijos elementai. Pirminiai skaičiai. Eratosteno rėtis. Merseno pirminiai skaičiai

Eratosteno rėtis naudojamas rasti pirminiams skaičiams. Surašomi visi skaičiai nuo 2 iki n. Einama iš eilės. Randamas pirmasis neišbrauktas skaičius. Išbraukiami visi jo kartotiniai išskyrus jį patį. Taip atlikus su visais neišbrauktais skaičiais paeiliui, liks aibėje tik pirminiai skaičiai.

Merseno pirminiu skaičiumi vadinami skaičiai, kurių forma – 2p-1, kur p – pirminis skaičius. Ne visi Merseno skaičiai yra pirminiai.

1. Skaičių faktorizacija. Fundamentalioji aritmetikos teorema

Fundamentalioji aritmetikos teorema – kiekvieną natūralųjį skaičių galima išskaidyti pirminių skaičių sandauga (faktorizuoti). 288 = 2 \* 2 \* 2 \* 2 \*2 \* 3 \* 3

1. Didžiausio bendro daliklio radimas

Didžiausiu bendru dalikliu vadiname didžiasausią naturalųjį skaičių, iš kurio skaičiai a ir b dalinasi be liekanos. Skaičių galime išreikšti tokiu pavidalu: a = qb + r q- dalmuo, r- liekana. Kadangi dbd. Dalina qb be liekanos, tai ir r turi dalinti be liekanos tam, kad dalintų a. Taigi dbd(a, b)=dbd(b, r), kai a >= b.

1. Diffie-Hellman metodas rakto apsikeitimui

Diffie-Hellman raktų apsikeitimas pagrįstas diskretinio logaritmavimo problema. Jis laikoma saugiu, kai pasirenkami pakankamai ilgi raktai ir naudojami atitinkami generatoriai. Tuomet abu sugalvoja po atsitiktinį skaičių ir pakelia raktą tokiu laipsniu tuomet padalina iš atitinkamo generatoriaus skaičiaus ir persiunčia vienas kitam. Tuomet gautus skaičius pakelia sugalvoto skaičiaus laipsniu ir vėl padalina iš generatoriaus skaičiaus. Taip abu gauna vienodą liekaną.

1. Vienkartinio rakto prinicipas (OTP). Vernamo šifras

Vernamo šifras – šifravimo algoritmas, kuriame teksto kodavimui naudojamo rakto ilgis sutampa su paties teksto ilgiu. Kodavimui naudojama modulinė sudėtis. OTP yra nenulaužiamas, jei laikomasi šių taisyklių:

1. Raktas turi būti absoliučiai atsitiktinis. Jis negali būti sugeneruotas iš pseudoatsitiktinių skaičių generatoriaus ar panašiai
2. Raktas gali būti panaudotas tik vieną kartą
3. Raktas turi būti saugiai perduotas gavėjui

Vienkartiniu raktu užšifruotą tekstą yra galimybė iššifruoti į bet kokį kitą tokio paties ilgio raktą.

1. Vigenere šifravimas

Labai panašus į Cezario šifravimą, tik raidės pastumiamos į priekį pagal tai, kelintą vietą abecelėje nuo pradžių užiima rakto atitinkama raidė.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | b | d | e | f | g | h |
| t | e | k | s | t | a | s |
| t | g | o | x | l | h | a |

1. Feistel struktūra

Blokinio simetrinio šifratoriaus struktūra, kuri padalina tekstogramą į dvi dalis – kairę ir dešinę. Ir atlieka tokius veiksmus n kartų:

Li+1=Ri

Ri+1=Li⊕F(Ri, Ki) F – tam tikra funkcija, Ki-raktas

Iššifravimas

Ri=Li+1

Li=Ri⊕F(Li+1, Ki)

# Grafų sąvokos

Grafas neorientuotas, jei jis turi tik briaunas. Grafas orientuotas, jei turi tik lankus. Jei turi lankus ir briaunas – mišrus.

Multigrafas – bent dvi grafo viršūnės, jungiamos keliomis briaunomis.

Pilnasis grafas – jei kiekviena viršūnė jungiasi su visomis kitomis.

Dvidalis grafas – grafo viršūnių aibę galima išskaidyti į dvi aibes A ir B taip, kad kad kiekvienos jo briaunos skirting galai priklausytų skirtingoms aibėms A ir B.

Pilnasis dvidalis – jei kiekviena aibės A viršūnė jungiasi briauna su visomis aibės B viršūnėmis.

Įėjimo puslaipsnis – orientuotame grafe, kiek įeinančių lankų į viršūnę.

Išėjimo puslaipsnis – orientuotame grafe, kiek išeina lankų iš viršūnės.

Viršūnės laipsnis – gretimų viršūnių skaičius.

Reguliarus grafas – visų viršūnių laipsnių skaičius vienodas.

Grandinė – grandinė gretimų briaunų seka.

Ciklas – jei grandinės sekos pirmoji ir paskutinė sutampa.

Elementarus ciklas – jei seka eina tik per skirtingas viršūnes.

Viršūnės ekscentricitetas – ilgiausias grandinės kelias nuo viršūnės iki likusių viršūnių ilgis.

Grafo skersmuo – didžiausias viršūnių ekscentricitetas.

Periferinės viršūnės – viršūnės, kurių ekscentricitetas lygus skersmeniui.

Skersmens grandinė – skersmens ilgio grandinė, kuri jungia dvi periferines viršūnes.

Svorinis grafas – grafas, kurio kiekvienai briaunai priskirtas skaičius, vadinamas briaunos svoriu.