

1. Jvadas

1.1. Kokius informacijos saugos uždavinius sprendžia kriptografija?

Pagrindiniai kriptografijos mokslo tikslai – sukurti priemones, kurios gali būti naudojamos informacijos slaptumui, vientisumui bei autentiškumui garantuoti, ryšio subjektų identitetui patikrinti, išsižadėjimams paneigti.

1.2. Suformuluokite kriptosistemos apibrėžimą.

Kriptosistema – įrankių sistema, naudojama duomenų apsaugai. Tai aibų trejetas $\langle M, K, C \rangle$, kur:

- M – galimų šifruoti pranešimų aibė
- K – galimų naudoti raktų aibė
- C – šifrų aibė

$$e(\cdot|K) : M \rightarrow C, \quad d(\cdot|K) : C \rightarrow M, \quad K \in \mathcal{K}.$$

- $e(\cdot|K)$ – šifravimo algoritmas, kurį valdo raktas K ;
- $d(\cdot|K)$ – dešifravimo algoritmas, kurį valdo raktas K ;

1.3. Kas suformulavo moderniosios kriptografijos principus? Suformuluokite bent vieną iš jų.

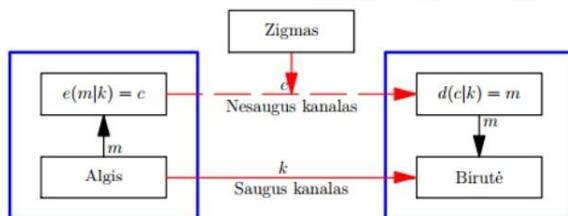
Kerckhoffas. Principai (ne visi aišku...)

- Sistema turi būti praktiškai neiššifruojama. Teoriškai galbūt ją ir galima jveikti perrenkant visus raktus, tačiau jeigu tam reiktų sugaišti keletą metų, praktiškai tokia galimybė neturi jokios reikšmės.
- Priešininkas, net ir žinodamas, kokia šifravimo sistema naudota, neturi ištengti iššifruoti šifro. Svarbus yra raktas, o ne šifravimo algoritmas.

1.4. Kokios kriptosistemos vadinamos simetrinėmis?

Tokios kriptosistemos, kuriose šifravimui ir dešifravimui naudojami vienodi raktai, o jei jie skirtini – lengvai gaunami vienas iš kito.

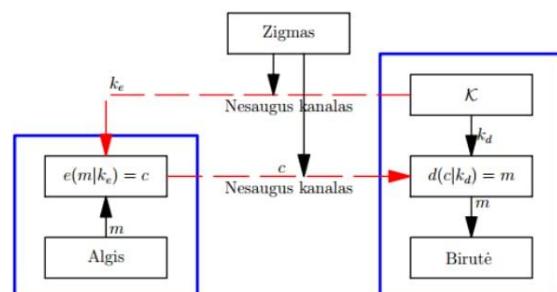
1.5. Paaiškinkite simetrinės kriptosistemos naudojimo diagramą.



1.6. Kokias kriptosistemas vadiname nesimetrinėmis (viešo rakto)?

Tokios kriptosistemos, kurios turi skirtinges raktus šifravimui ir dešifravimui. Šifravimo raktas yra viešas, pasiekiamas visiems, dešifravimo – privatus.

1.7. Paaiškinkite nesimetrinės kriptosistemos naudojimo diagramą.



1.8. Paaiškinkite, kaip naudojamos skaitmeninių parašų schemas.

Siuntėjas siunčia pranešimą, užšifruotą privačiu savo raktu. Šis šifras kartu yra ir pranešimas, ir jo parašas. Gavėjas dešifruoja pranešimą viešuoju siuntėjo raktu. Tą gali padaryti kaip ir bet kas, tačiau pašalinis žmogus, perskaitęs pranešimą, negali jo pakeisti ir persiųsti gavėjui, apgaudamas, jog tai originalus siuntėjo pranešimas.

1.9. Kas yra pavienių šifrų ataka? Kas yra teksto-šifrų porų ataka?

Pavienių šifrų ataka – atakų klasė, kai žinomas tik šifras. Uždavinys – rasti algoritmą arba raktą k , kuris kiekvienam šifrui gauna jį atitinkantį pradinį tekstą

Teksto-šifrų porų ataka – atakų klasė, kai žinomas pradinis tekstas ir jį atitinkantis šifras. Uždavinys tas pats.

1.10. Kokia kriptosistemas vadinama besalygiškai saugia (unconditional security)?

Kriptosistema $\langle M', K', C' \rangle$ vadinsime besalygiškai saugia tada ir tik tada, kai su visomis M' ir C' reikšmėmis M, C teisinga lygybė $P(M' = M | C' = C) = P(M' = M)$.

Jei net turėdamas beribius skaičiavimo resursus/resultatus negali nežinodamas raktą iš šifro nustatyti, koks pranešimas buvo siūstas. Tai griežčiausias saugios kriptosistemos apibrėžimas.

1.11. Kokia kriptosistemas vadinama saugia skaičiavimo požiūriu?

Jeigu turimas/pasiektas skaičiavimų resursų lygis yra pernelyg žemas, kad naudojant geriausias žinomas atakas, sistema būtų įveikta.

2. Simetrinės kriptosistemos

2.1. Kas yra simbolų dažniai natūraliojoje kalboje ir kaip jie keičiasi, kai naudojame kriptosistemą su perstatomis?

Simbolio dažnis – jo pasikartojimo tekste skaičius. Kadangi perstatų šifras nieko nekeičia, tik pakeičia simbolų eiliškumą, dažnis nesikeičia. Raidžių pasitaikymo tikimybė šifruotame ir nešifruotame tekste sutampa.

2.2. Paaiškinkite, kaip veikia skytalės šifras.

Tekstas surašomas eilutėmis po n raidžių. Užšifruotas tekstas – tekstas, skaitomas tais pačiais parašytais n stulpeliais. LABAS RYTAS po 5 raides \rightarrow LRAYBTAASS.

Graikiijoje originaliai skytalės buvo siaura ilga juostelė. Ji buvo vyniojama ant pagaliuko (jo storis buvo raktas) taip, kad sluoksniai būtų vienas šalia kito. Ant susuktos juostelės rašomas tekstas vis ją pasukant.

2.3. Kas yra simbolų dažniai natūraliojoje kalboje ir kaip jie keičiasi, kai naudojame kriptosistemą su keitiniais?

Simbolio dažnis – jo pasikartojimo tekste skaičius. Naudojant keitinių šifrą, pavienių simbolų dažnis išnyksta, lieka šifruojamų „žodžių“ ($|\text{žodis}| > 1$) dažniai. // Kažkaip mažoka info...

2.4. Paaiškinkite, kaip konstruojamos kriptosistemos naudojantis Polibijaus kodo idėja.

Polibijaus kodo idėja - keisti raides tam tikrais susitartais kodais. Šia idėja paremtose kriptosistemose simboliai keičiami susitartais kodais. Pvz. Moržės abécélė arba šiai laikais naudojamas ASCII kodavimas.

2.5. Paaiškinkite Cezario kriptosistemą, naudodami lyginius.

Teksto ir kodo abécélės sutampa, skiriasi jų tvarka – kodo abécélė yra tokia pati, tik per k (raktas) paslinkta į vieną pusę. Šifro lyginys su raktu 2 atrodys taip: $(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{array})$.

Koduojant, pirmos eilutės raidę keičiam antrosios, dekoduojant – antros keičiam į pirmosios.

2.6. Cezario kriptosistemos abécélė A = {0, 1, 2, 3, 4, 5, 6}. Šifras c = <3, 2, 4, 5> gautas naudojant kartą k = 3. Dešifruokite šifrą.

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \end{pmatrix} \quad <3, 2, 4, 5> \text{ dešifruojamas į } <6, 5, 0, 2>$$

2.7. Paaiškinkite, kaip veikia Hilo kriptosistemą.

Raktas yra $n \times n$ matrica K (sudaryta iš skaičių). Šifruojamos simbolių sekos po n elementų – žodžiai. Vieno žodžio šifras = žodžio išraiškos skaičiais ir matricos K sandauga moduliu n (abécélės dydis).

Dešifruojama šifruotą žodį ilgio n dauginant iš atvirkštinės matricos K.

Tekstas * Matrica = Šifras :

$$(m_1 \dots m_n) \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{n1} & \dots & c_{nn} \end{pmatrix} = (c_1 \dots c_n) \bmod N, \quad \text{kur } N - \text{abécélės dydis}$$

2.8. Hilo šifro abécélė A = {0, 1, 2, 3, 4, 5, 6}. Užšifruokite porą <3, 5> naudodami raktą

$$(3 \ 5) \cdot \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \bmod 7 = \begin{pmatrix} 3*1 + 5*2 \\ 3*3 + 5*4 \end{pmatrix} \bmod 7 = \begin{pmatrix} 12 \\ 29 \end{pmatrix} \bmod 7 = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \rightarrow (5 \ 1)$$

$$K = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

2.9. Paaiškinkite Plaifairo šifrą.

Abécélė surašoma į stačiakampį (sutarta tvarka, bet dažniausiai), kurio pirmosios raidės bus naudojamas raktas. Šifruojamos raidžių poros, joms iš stačiakampio parenkant atitinkamą porą pagal taisykles:

- Jei abi šifruojamos raidės yra vienoje eilutėje/stulpelyje, jas atitiks sekancios eilutėje/stulpelyje parašytos raidės.
- Jei šifruojamos raidės yra skirtinose eilutėse ir stulpeliuose, galima padaryti „jų ribojamą stačiakampį“, šifras – priešingų kampų raidės.
- Nepatartina šifruoti vienodų simbolių, geriau daryti gramatinės klaidas (moon -> mon)

Dekodavimas vyksta analogiškai, tais pačiais principais, tik atvirkščia tvarka.

2.10. Kas yra homofoniniai keitiniai ir kaip jie gali būti naudojami kriptosistemose?

Homofoninių keitinų kriptosistemoje raktas ir tekstas vienareikšmiškai neapibrėžia šifro.

$k : A \rightarrow P(B)$, $k(m) \cap k(n) = \emptyset$, jei $m \neq n$, kur A – teksto abécélė, B – šifro abécélė.

Homofoninis keitinys – keitinys simboliumi sudarytas iš galimai daugiau nei vieno simbolio (vieną simbolį atitinkti gali keli elementai (aibė)). Šio keitinio naudojimą apibrėžia raktas ir jo taikymo taisyklys.

Šio keitinio naudojimas yra saugesnis nei paprasto, nes du skirtinės tekstus gali reikti skaityti vienodai, o vieną tekštą galim užkoduoti skirtiniais būdais, priklausomai nuo rako taisyklių.

2.11. Kaip keičiasi simbolių dažnai, kai naudojame homofoninius keitinius?

Naudodami homofoninius keitiniais grindžiamus šifrus, galime panaikinti ryšį tarp atviro teksto simbolių dažnių lentelės bei šifro simbolių dažnių lentelės.

Parinkdami funkcija k taip, kad homofono k(a) elementų skaičius būtų proporcingas simbolio a dažniui atvirame tekste, galime pasiekti, kad šifruotame tekste visu simboliu pasiodymo dažniai mažai skirtus.

3. Vigenere kriptosistemų, mechaniniai įrenginiai.

3.1. Apibrėžkite Vigenere kriptosistemą naudodami lyginius.

Vigenere šifras – perstatu šifras, tik raktas nebūtinai yra vienas skaičius. Raktas – perstumimų skaičių aibė. Pavyzdžiu:

Abécélę {A, B, ... Ž} atitiks skaičiai {0, 1, ... 31}. Tada tekštą PASLAPTIS atitiks skaičiai <21, 0, 23, 17, 0, 21, 25, 12, 23>. Pasirinkime raktą <3, 5, 8>. Naudojant tą pačią formulę kaip ir Cezario šifrui, keitinys tekstu PASLAPTIS atrodys taip:

$$\begin{pmatrix} P & A & S & L & A & P & T & I & S \\ 21 & 0 & 23 & 17 & 0 & 21 & 25 & 12 & 23 \\ 3 & 5 & 8 & 3 & 5 & 8 & 3 & 5 & 8 \\ 24 & 5 & 31 & 20 & 5 & 29 & 28 & 17 & 31 \\ \checkmark & D & \checkmark & O & D & V & \checkmark & L & \checkmark \end{pmatrix}. \text{Šiuo pavyzdžiu parašysiu šifrą keitiniais.}$$

Šifruosime blokais po rakto ilgį raidžių.

Tekstas <m₁, m₂, m₃>. Raktas <k₁, k₂, k₃>. Šifras <c_i = (m_i + k_i) mod N : i = 1, 2, 3>

3.2. Vigenere kriptosistemos abécélė A = {0, 1, 2, 3, 4, 5, 6}. Užšifruokite pranešimą P = 166166 su raktu k = 23.

(M+K) mod N

$$\begin{pmatrix} 1 & 6 & 6 & 1 & 6 & 6 \\ 2 & 3 & 2 & 3 & 2 & 3 \\ 3 & 2 & 1 & 4 & 1 & 2 \end{pmatrix}. \quad 166166 \text{ (1) su raktais } 232323 \text{ (2) užšifruojamas kaip } 321412 \text{ (3)}$$

3.3. Vigenere kriptosistemos abécélė A = {0, 1, 2, 3, 4, 5, 6}. Iššifruokite pranešimą C = 166166, jei jis sudarytas su raktu k = 23.

(C-K) mod N

$$\begin{pmatrix} 1 & 6 & 6 & 1 & 6 & 6 \\ 2 & 3 & 2 & 3 & 2 & 3 \\ -1 & 3 & 4 & -2 & 4 & 3 \end{pmatrix}. \quad 166166 \text{ (1) su raktais } 232323 \text{ (2) dešifruojamas kaip } 634543 \text{ (3)}$$

3.4. Paaiškinkite, kaip galima analizuoti Vigenere kriptosistemą, naudojant rako ilgi.

Galima šifrą suskaidyti į blokus po rakto ilgio skaičių raidžių. Tada kiekvieną bloką galima bandyti analizuoti naudojant vieną, tačiau kiekvienam savę abécélę

3.5. Paaiškinkite, kaip Vigenere šifro analizei galim taikyti Kassiskio testą.

Teskast skirtas rako ilgiui šifro sudaryme analizavimui.

Šifre ieškome vienodų raidžių porų/blokų, randami atstumai tarp jų. Išnagrinėję atstumus tarp vienodų porų/blokų, sudaroma duomenų lentelė, kiek atstumų dalinasi iš skaičių 2, 3, 4... Tikimybiškai, daugiausiai kartotinių turintis skaičius, iš kurio dalinom, bus labiausiai tikėtinės rako ilgis.

3.6. Kas yra koincidencijų (sutapimų) indeksas?

Sutapimų skaičiavimas – sudėti du tekstus vieną šalia kito ir skaičiuoti, kiek kartų tose pačiose vietose atsirandantis pačios raidės abiejuose tekstuose. Šis skaičius ir yra sutapimų indeksas. Lietuvių kalbos sutapimų indeksas yra $\kappa_{lit} = p_0^2 + p_1^2 + \dots + p_{31}^2 \approx 0,069$

3.7. Kaip taikomas kappa testas?

Jis taikomas rako ilgiui rasti. Gretinamas originalus šifras, iš tas pats šifras, tik atmetus pirmuosius d simbolių. Pažiūrime, kokio skaičiaus kartotinių skaičių raidžių atmetus sutapimų indeksai didžiausi. Šis skaičius turbūt ir bus rako ilgis.

3.8. Paaiškinkite šifravimą su Jeffersono cilindrais.

Yra vienas cilindras, su ant jo užvertais pvz. 36 diskų, ant kurio po vienodą dalį užima visos angliskos abécélės raidės ($26 = N$) vis kita tvarka. Taip susidaro įvairios N eilučių raidžių. Pasukame diskus taip, kad pradinėje eilutėje atsidurtų šifruojamas 36 simbolių tekstas. Taip kiekviena likusi eilutė gali būti to teksto šifru. Šifro gavėjas turi turėti tokį pat cilindrą, kuriame vienoje eilutėje susikęs šifras, tekštą gus vienoje iš likusių eilučių. Čia raktas – diskų išdėstymo tvarka.

3.9. Paaiškinkite šifravimą su rotoriu įrengimais principu.

Rotorius – diskas, turintis po N kontaktų abiejose pusėse, kurie sujungti poromis kontaktais. Kontaktas tarp raidžių atitinka šifrą. Tarkime turime t rotorius, sujungtų vienas šalia kito, gretimų rotoriu kontaktai sujungti poromis. Šifruojama viena raidė pereina kelis tokius keitinius. Po kiekvienos užšifruotos raidės, rotoriai pasisuka glimi skirtinę skaičių kartą. Taip pasikartojimai tarp sukimus yra labai reti, gaunamas Vigenere šifras su rakto ilgiu... dideliu.

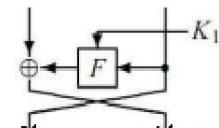
3.10. Teksto ir šifro abécélė $A = \{0, 1, 2, 3, 4\}$, šifravimui naudoti du rotoriai, abiejų jungtys aprašomas tuo pačiu keitiniu $\lambda = [2, 0, 1, 4, 3]$. Kokia raide šifruojama raidė 0, jei ji tekste yra 12-oji?

// I forgot how this works... Hope i don't get this one...

4. Feistelio iteracijos, DES ir AES

4.1. Paaiškinkite brėžiniu šifravimo, naudojant Feistelio iteracijas, idėją.

Koduojama blokais. Jie skaidomi į dvi dalis, atliekamos tam tikros operacijos, susikeičia/užšifruojami duomenys. Galima pasirinkti operaciją/iteracijų skaičių.



4.2. Feistelio schemas funkcija $f(x_1, x_2, y_1, y_2) = z_1 z_2$, kur $z_1 = x_1 \text{ (xor)} y_1$, $z_2 = x_2 y_3$ (probs meant 2). Kokį pranešimo 0111 šifrą gautume po dviejų iteracijų, jei abiejose naudojamas tas pats raktas $k = k_1 k_2$ (išreikškite šifrą rako bitais).

$$L = 01, \quad R = 11, \quad K = mn.$$

$$L = R = 11, \quad R = \neg m \neg n, \quad \text{nes } f(R, K) \text{ XOR } L = (z_1 = 1 \text{ XOR } m, z_2 = 1 \& n) \text{ XOR } L = (\neg mn) \text{ XOR } L$$

$$L = R = \neg m \neg n, \quad R = m \neg n \quad \text{nes } f(R, K) \text{ XOR } L = (z_1 = \neg m \text{ XOR } m, z_2 = \neg n \& n) \text{ XOR } L = 10 \text{ XOR } L$$

$$0111 \rightarrow RL = m \neg n \neg m \neg n$$

4.3. Kaip dešifruojamas šifras, gautas naudojant Feistelio iteracijas?

Naudojamos tos pačios funkcijos. Paduodame šifrą, ir raktus ATVIRKŠČIA tvarka (3, 2, 1, o ne 1, 2, 3). Vykdomi tie patys šifravimo veiksmai, tik naudojama raktų tvarka yra kita.

4.4. Nubraižykite vienos DES iteracijos schema.

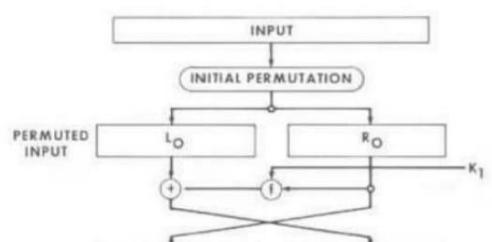
Simple way of explaining it :

Originalus pranešimo, kurį koduosime, ilgis yra 64 bitai.

Nežinau, kuris variantas labiau tikėtinės, nes pagal skirtinias schemas atsakymai skirtinė:

- 1) 64 praplečiami į 96 bitus. Skeliamas pusiau. Gaunami du blokai po 48 bitus – tokio ilgio yra ir raktas.
- 2) 64 bitai skeliamas pusiau, gaunami 2 blokai po 32 bitus, kurie praplečiami iki 48 bitų blokų.

Toliau atliekamos tokios pats operacijos, kaip ir Feistelio iteracijose.



4.5. Kokio dydžio informacijos blokus šifruoja DES ir kokius raktus naudoja?

DES rako ilgis – 48 bitai. Informacijos blokas – 64 bitai, suskaidyti į dvi dalis po 32.

4.6. Paaiškinkite, kokie pranešimo bloko pertvarkiai sudaro vieną AES iteraciją.

4.7. Paaiškinkite, kaip DES buvo panaudota UNIX sistemoje autentifikavimui slaptažodžiais.

Vartotojo slaptažodis būna sutrumpinamas tik iki 8 baitų. Šie sutrumpinami į blokelius tik po 7 bitus, gaunant 56 bitų seką – DES raktą. Šiuo raktu užšifruojama nulinį bitų seka, vėl ir vėl 25 kartus. 12 bitų „druska“ (random duomenys) naudojama užšifravimo algoritmui sumaišyti (?), kad nebūtų galim naudoti standartinės DES implementacijos užšifravimui. „druska“ ir galutinis užšifruotas tekstas užkoduojamas spausdinama eilute. Taip kiekvienas slaptažodis gauna hash reikšmę. Keli slaptažodžiai gali gauti tą pačią hash reikšmę, bet šis algoritmas naudojamas tik patikrinimui, ar slaptažodis sutampa, o ne dešifravimui.

4.8. Paaiškinkite blokinių kriptosistemų naudojimą CBC rėžimu.

Tai šifru blokų grandinės rėžimas. Kiekvieno bloko šifrevimas/dešifrevimas priklauso nuo ankstesnio rezultato.

Šifruojant:

Pirmas raktas pasirenkamas, nebūtinai slaptai, ir naudojamas užšifruojant pirmą bloką (pagal schemą atliekamas XOR). Šis blokas šifruojamas su funkcija, gaunamas šifras patampa antruoj raktu, naudojamu antro bloko šifrevimui ir t.t.

Dešifrevimas:

Pirmiausiai atliekami dešifrevimo funkcijos veiksmai, gaunamas duomenų blokas. Jam atlikus pagal schemą XOR operaciją su pirmuoju raktu, gaunam originalų tekštą. Tolimesni raktai yra pirminio šifro blokai.

Taip blokai pasidaro vienas nuo kito priklausomi, sunkiau dešifruoti nežinant sąryšio

4.9. Paaiškinkite blokinių kriptosistemų naudojimą OFB rėžimu.

Tai šifru blokų grandinės rėžimas. Kiekvieno bloko šifrevimas/dešifrevimas priklauso nuo ankstesnio rezultato.

Šifruojant:

Pirmas raktas pasirenkamas ir užšifruojamas. Rezultatas – sekantis raktas. Ji pagal schemą XORinamas su teksto bloku, gaunamas šifras.

Dešifrevimas:

Analogiškas. Pirmas raktas dešifruojamas su funkcija, patampa nauju raktu. Tektas gaunamas raktą XORinant su pirmo bloko šifru. Grandine einama toliau, kol dešifruojama viskas.

4.10. Paaiškinkite blokinių kriptosistemų naudojimą CRT rėžimu.

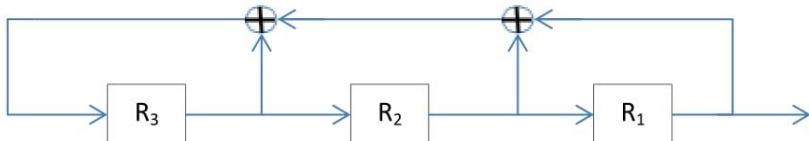
Raktai čia kiekvienam blokui sukuriami skaitliuko pagalba atskirai. Sukurtas raktas užšifruojamas su funkcija, rezultatas XOR tekstas – gauname šifrą. Skaitliukui pritaikę dešifrevimo funkciją, XOR operacija su šifru – gauname tekštą.

Grandinės funkcijos nebelieka. Dešifrevimui reikia žinoti skaitliuko rako gaminimo funkciją.

5. Srautiniai šifrai

- 5.1.** Nubraižykite kokią nors tiesinių registrų sistemos su trimis registrais schemą ir paaiškinkite, kaip sistema generuoja raktą srautą.

Kiekviename žingsnyje registruose esantys bitai perstumiami į dešinę per vieną. Pirmo registro bitas patenka į generuojamą srautą. Paskutinis bitas gaunamas pagal schemą XOR operaciją atliekant tam tikriems bitams. Šiuo atveju – buvusiems 3 ir 2 registrų bitams.



- 5.2.** Irodykite, kad tiesinė registrų sistema generuoja periodinę bitų seką.

Tiesinė registrų sistema generuoja periodines bitų sekas, kurių periodas yra ne didesnis už $2^n - 1$.

Tarkime, pradinės registrų reikšmės $x(0)$ nėra nulinis vektorius (kitu atveju visada generuojami tik nuliai).

Apibrėžkime matricą C , kuri nebus išsigimusi, nes $\det C = c_n = 1$.

$$C = \begin{pmatrix} c_1 & 1 & 0 & \dots & 0 \\ c_2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & 0 & 0 & \dots & 1 \\ c_n & 0 & 0 & \dots & 0 \end{pmatrix}$$

Tada galime perrašyti $x(t+1) = x(t)C$. $x(t+1)$ yra nulinis, tik jei $x(t)$ yra nulinis vektorius. Pritaikę lygybę t kartą, gauname $x(t) = x(0)C^t$. Taip gauname, jog $x(t)$ nėra nulinis vektorius visiems t . Pažymėjė $m = 2^n - 1$, galime tvirtinti, kad sekoje lygybių $x(t) = x(0)C^t$, kur $t \leq m$, būtinai gausime pasikartojimų, nes yra tik m skirtingų nenuliniai n -mačių vektorių.

Galime rasti tokius t ir s , kad $x(0)C^s = x(0)C^{s+t}$.

Kadangi C nėra išsigimusi, turi atvirkštinę, tai $x(t) = x(0)C^t = x(0)C^{s+t}C^{-s} = x(0)$.

Dabar su bet kokiai $r \geq 0$, gausime $x(r+t) = x(0)C^{r+t} = x(0)C^rC^t = x(t)C^r = x(0)C^r = x(r)$.

Taip įrodome, kad generuojama bitų seka turi periodą.

- 5.3.** Kas yra registrų sistemos charakteringasis daugianaris ir kaip nuo jo savybių priklauso generuojamas sekos periodas?

Tiesinės registrų sistemos charakteringuoju daugianariu vadinsime daugianarj. Jei $P_n(x) = 1 + c_1x + \dots + c_nx^n$, $c_n \neq 0$. šis daugianaris primitivus, registrų sistema generuoja maksimalaus periodo seką.

- 5.4.** Kaip atlikti kryptosistemos, kurioje naudojama registrų sistema, teksto-šifro poros ataką

- 5.5.** Paaiškinkite, kaip veikia šifras A5/1.

- 5.6.** Paaiškinkite, kaip veikia šifras RC4.

Raktas sudarytas iš L baitų $K[0] \dots K[L-1]$. Pradinė inicializacija:

```

j:=0
for i= 0 to 255 do S[i] = i end
for i= 0 to 255 do
    j = j + S[i+K[i mod L]]
    S[i] <-> S[j]
end
I = j = 0
  
```

Rakto konstravimas:

$$\begin{aligned} i &= i+1 \\ j &= j + S[i] \\ S[i] &\leftrightarrow S[j] \\ S[S[i] + S[j]] &\rightarrow \text{rakto srautas} \end{aligned}$$

5.7. Paažinkite, kaip galima jungti tiesinių registru sistemas, kad būtų panaikinti tiesiniai rakto srautų bitų ryšiai.

6. h-funkcijos

6.1. Paažinkite, kas yra h-funkcija, kam ji naudojama kriptografijoje.

h-funkcija – funkcija $h(m)$, argumentui m priskirianti pseudoatsitiktinį skaičių (fiksuočią eilutę), vadinamą maišos kodu. Jie ji nėra atsitiktinė, tam pačiam m turi gražinti tą patį kodą.

Hash (maišos) funkcija sukuri duomenų santrumpas, naudojamas duomenų paieškos organizavimui, duomenų sutapimo, vientisumo tikrinimui. Maišos kodų aibė turi būti mažesnė, nei galimų argumentų funkcijai aibė.

6.2. Kas yra h-funkcijos sutapimas (kolizija)?

Tai kai skirtiniems funkcijos $h(m)$ parametrambs gražinamas tas pats hash kodas.

6.3. Kokios h-funkcijos vadinamos wcf ir scf h-funkcijomis?

WCF – weekly collision free – silpnai atsparumams atspari hash funkcija – tokia, kuriai nėra efektyvaus algoritmo, kuris rastą parinktam skaičiui x kitą skaičių x' , kad $h(x) = h(x')$

SCF – strongly collision free – stipriai sutapimams atspari hash funkcija – tokia, kuriai nėra efektyvaus algoritmo rasti **kokį nors** sutapimų porą.

6.4. Kas yra h-funkcijos gimtadienių ataka?

Tai ataka prieš hash funkciją naudojant gimtadienių sutapimų uždaviniu ir tikimybų teorija.

Pasirenkami atsitiktiniai N argumentai. Randamos visų jų hash funkcijų reikšmės. Tarkime, galimų visų hash funkcijų reikšmių yra M .

Jei nors dvi rastos funkcijų reikšmės sutapo, sutapimas rastas. Atlikus eksperimentą su daug reikšmių, galim gauti apytiksliai, kaip dažnai kokios hash reikšmės gaunamos.

6.5. Paažinkite Merkle-Damgaardo schemą maišos funkcijoms konstruoti.

Pirmiausiai pasinaudojama kažkokia funkcija gauti input data, kurios dydis yra fiksuoto skaičiaus kartotinis (512, 1024...). Tada hash funkcija suskaido rezultatą į blokus po fiksuočią dydį, po vieną apdoroja suspaudimo funkcija, kaskart panaudojant input bloką, bei praeitą rezultatą. Kad konstrukcija būtų saugi, pasiūlyta taip pat užkoduoti originalaus pranešimo ilgį.

Taip sukuriamas kolizijoms atspari hash funkcija.

6.6. Kaip maišos funkcijos gali būti konstruojamos naudojantis kriptosistemomis?

Maišos funkcijas galima konstruoti naudojant blokines kriptosistemas.

Blokinės kriptosistemos ima du fiksuoto ilgio duomenų blokus, ir gražina tokio pat ilgio rezultatą. Paprastas blokines sistemas nesunku palaužti, todėl pridėta patobulinimų.

Tokių hash funkcijų konstravimo metodų pavyzdžiai - Matyaso-Meyerio-Oseaso, Davieso-Meyerio ir Miyaguchi-Preneelio metodai.

6.7. Bendrais bruožais paaiškinkite maišos funkcijos MD5 struktūrą.

Duomenų bloko ilgis – 512 bitų. Santrauka – 128 bitai – gaunama atliekant 4 iteracijas.

Pradinis kontrolinis blokas užpildomas kažkokiais duomenimis. Naudojamos 4 pagalbinės funkcijos, kurios operuoja trimis 32 bitų žodžiais, gražina vieną 32 bitų žodį.

Su kiekvienu bloku atliekamas kontrolinio bloko skaičiavimas, naudojamas ankstesnis kontrolinis blokas. Atliekama daugiau skaičiavimų, kurių neiškalsiu. Gaunami 4 žodžiai po 32 bitus, kas ir bus hash reikšmė.

6.8. Paaiškinkite Keccac maišos funkcijos struktūrą.

Tai tarsi kempinė struktūra. Pirmiausiai informacija suspaudžiamą, o paskui išspaudžiama lauk.

Suspaudimo dalis : teksto dalys yra xor operacijos pagalba suspaudžiamos su talpos dalimi, vėliu transformuojamos į visą talpos dydžio bloką.

Išspaudimo dalis: iš suspaustos informacijos išspaudžiama iš dalies talpos, pakoreguojamos su būsenos funkcija.

7. Matematiniai viešo rakto kriptografijos pagrindai

7.1. Paaiškinkite Euklido algoritmą skaičių bendram didžiausiam dalikliui rasti.

Pažymėkime du skaičius A ir B, kur $A > B$.

// šiek tiek kosmiškesnis paaiškinimas

Žmogiškas paaškinimas:

1. Rasti A dalybos iš B liekaną.
 2. Pakeisti A reikšmę B reikšme.
 3. Pakeisti B liekana, rasta 1 žingsnyje.
 4. Kartoti žingsnius 1-3, kol B bus 0.
 5. BDD bus A reikšmė.

$$\begin{aligned} a &= q_0 b + r_0, & 0 < r_0 < b, \\ b &= q_1 r_0 + r_1, & 0 < r_1 < r_0, \\ r_0 &= q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ &\dots\dots\dots \\ n-2 &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ n-1 &= q_{n+1} r_n, \\ r_n &= (a, b). \end{aligned}$$

7.2. Užrašykite veiksmų, atliekamu skaičių 27 ir 15 bendro didžiausio daliklio Euklido algoritmu, lygubes.

$$a = 27, b = 15$$

// šalia nupiešiu ta lentelę magiška, gal paaiškės kas nors...

- 1) $27(a) = 1(q_0)*15(b) + 12(r_0)$
 - 2) $15(b) = 1(q_1)*12(r_0) + 3(r_1)$
 - 3) $12(r_0) = 4(q_2)*3(r_1) (+ 0(r_2))$
 - 4) $3(r_2) = (27, 15)$

7.3. Paaiškinkite kėlimo laipsniu duotuoju moduliui algoritma.

7.4. Paaiškinkite kėlimo laipsnių duotuoju moduliui algoritmą skaitiniu pavyzdžiu $7^{14} \text{ mod } 5$.

7.5. Apibrėžkite Oilerio funkciją.

Eulerio (Oilerio) funkcija – funkcija

$$\varphi(n) = |\{m : 1 \leq m < n, (m, n) = 1\}|$$

Žmogiškai – $\varphi(n)$ = kiek tarpusavy pirminiu skaičiu yra skaičiu n aibėje [1; n].

7.6. Suformuluokite Oilerio teoremq.

Jei p yra pirminis skaičius, o $(a, p) = 1$, tai $a^{p-1} \equiv 1 \pmod{p}$.

Jei p yra pirminis skaičius, $(a, p) = 1$, tai $a^{p-1} - 1$ dalijasi iš p .

7.7. Apskaičiuokite $\varphi(50)$.

Pasinaudojus savybe, kad jei $(m,n) = 1$, tai $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

$$50 = 25 \cdot 2. \quad (25, 2) = 1.$$

$$\varphi(50) = \varphi(25) \cdot \varphi(2) = 20 \cdot 1 \quad (\text{šiaip } \varphi(a^2) = a^2(1-1/a))$$

7.8. Suformuluokite Kinų liekanos teoremq.

Tegul skaičiai $n_1 \dots n_k$ yra tarpusavyje pirminiai, skaičiai $y_1 \dots y_k$ yra bet kokie skaičiai.

$$n = n_1 \cdot \dots \cdot n_k$$

$$m_i = n / n_i$$

$$d_i m_i \equiv 1 \pmod{n_i}$$

Tada skaičius $y = y_1 d_1 m_1 + \dots + y_k d_k m_k$ tenkina visus lyginius $y \equiv y_i \pmod{n_i}$

7.9. Pasinaudokite Kinų liekanos teorema, raskite skaičių x , tenkinantį lygybes $x \equiv 2 \pmod{3}$ ir $x \equiv 3 \pmod{17}$.

$$n = n_1 \cdot n_2 = 51$$

$$n_1 = 3, \quad y_1 = 2, \quad m_1 = 17, \quad d_1 \cdot 17 \equiv 1 \pmod{3} \quad \rightarrow \quad d_1 = 2$$

$$n_2 = 17, \quad y_2 = 3, \quad m_2 = 3, \quad d_2 \cdot 3 \equiv 1 \pmod{17} \quad \rightarrow \quad d_2 = 6$$

$$y = x = 2 \cdot 2 \cdot 17 + 3 \cdot 6 \cdot 3 = 122.$$

7.10. Kas yra elemento atvirkštinis moduliui n ? Kokie elementai turi atvirkštinius?

Atvirkštinius elementus turi tik Z_n^* elementai

7.11. Apskaičiuokite $3^{-1} \pmod{17}$ pasinaudoję Euklido algoritmu.

8. RSA kriptosistema

8.1. Kaip sudaromi RSA kriptosistemos raktai?

Parenkami du pirminiai skaičiai p ir q , gaunamas $n = pq$.

Privatus raktas - skaičius d , tenkinantis sąlygą $(d, \varphi(n)) = 1$.

Viešas raktas – pora $\langle n, e \rangle$, tenkinanti sąlygas $e \cdot d \equiv 1 \pmod{\varphi(n)}$

8.2. Sudarykite RSA raktų porą su pirminiais $p = 5$ ir $q = 7$.

$$\varphi(n = 5 \cdot 7) = 4 \cdot 6 = 24$$

$$\text{Pasirenku } e = 11. \quad e \cdot d \equiv 1 \pmod{\varphi(n)}. \quad d = e^{-1} \pmod{24} = 11 \quad // \text{ Thanks, Sage Math!}$$

Privatus raktas $\langle 11 \rangle$, viešas raktas $\langle 35, 11 \rangle$

8.3. Kaip šifruojama ir dešifruojama RSA kriptosistemoje?

Šifras = Tektas $\xrightarrow{\text{Viešas raktas } E} (\text{mod } n)$

Tektas = Šifras $\xrightarrow{\text{Privatus raktas } D} (\text{mod } n)$

8.4. *Irodykite, kad RSA kriptosistemos dešifravimo algoritmas veikia teisingai.*

8.5. *Kuo remiasi RSA kriptosistemos saugumas?*

Saugumas remiasi dideliu skaičiu skaičiavimo sudėtingumo (dideliu skaičiu skaidymo pirminiais daugikliais sudėtingumu)

8.6. *Kaip RSA galima naudoti kaip skaitmeninio parašo schema?*

Kaip ir naudojant paprastą kriptosistemą, sudarome raktų porą $K_p = \langle d \rangle$ ir $K_v \langle e, n \rangle$.

Pranešimai, kuriuos galime pasirašinėti yra aibės $\{1, 2, \dots, n\}$ skaičiai.

Parašo sudarymas : $y = x^d \text{ mod } n$

Parašo tikrinimas : $x \equiv y^e \text{ mod } n \rightarrow$ nepripažystamas kitu atveju

8.7. *Paažinkite kaip atlikti RSA kriptosistemos vienodu modulių ataką.*

9. Kuprinės ir Rabino kriptosistemos

9.1. *Suformuluokite kuprinės uždavinį.*

Turime natūraliųjų skaičių (svorių) rinkinį $W = \{w_1, \dots, w_n\}$ ir norimą svorį w .

Ar egzistuoja tokie skaičiai x_i iš aibės $\{0, 1\}$, kad $w = w_1x_1 + \dots + w_nx_n$

9.2. *Kokios svorių sistemos vadinamos sparčiai didėjančiomis?*

Svorių sistema sparčiai didėjanti, jei kiekvienas elementas yra didesnis nei visų prieš jį buvusių elementų suma.

9.3. *Pateikite sparčiai didėjančios svorių sistemos pavyzdį.*

$\{1, 2, 4, 8, 16, \dots\}$ – dvejeto laipsniai.

9.4. *Kaip spręsti kuprinės uždavinį, kai svorių sistema sparčiai didėjanti?*

Jei svorių sistema sparčiai didėjanti, kuprinės uždavinys sprendžiamas polinominiu algoritmu.

(Bendras) Kuprinės kraustymas:

// Sparčiai didėjančios svorių sistemos kuprinės

$v = w_1x_1 + \dots + w_nx_n$

// uždavinio sprendimas probably identiškas.

Sprendimo algoritmas:

$w = v; j = n;$

// Žiūrėti analogišką uždavinį 9.5

do {

jei $w > w_j$, tai $x_j = 1$

jei $w < w_j$, tai $x_j = 0$;

$w = w - w_jx_j$

Jei $j = 0$, $w = 0$, išraiška rasta. Break

} until $w = 0$.

Jei $j = 0$, $w \neq 0$, išraiška neegzistuoja

9.5. *Išspręskite kuprinės uždavinį, kai svorių sistema $W = \{1, 3, 5, 12, 23, 45\}$, o svoris $m = 62$.*

$x_6 = 1; m = 62 - 45 = 17$ // nes svorių sistemą sudaro 6 elementai, $n = 6$

$$\begin{aligned}x_5 &= 0; m = 17 \\x_4 &= 1; m = 17 - 12 = 5 \\x_3 &= 1; m = 5 - 5 = 0 \quad \rightarrow \quad \text{Išraiška rasta! } 62 = 5 + 12 + 45\end{aligned}$$

9.6. Kaip sudaromi Merkle ir Hellmano kuprinės kriptosistemos raktai?

Privatus raktas $K_p = \langle W, s \rangle$: W – sparčiai didėjanti svorių sistema $\{w_1, w_2, \dots, w_n\}$; $w_1 + \dots + w_n < p$; $(s, p) = 1$
Viešas raktas $K_v = \langle v_1, v_2, \dots, v_n \rangle$, kur $v_i \equiv w_i s^{-1} \pmod{p}$

9.7. Kaip šifruojama ir dešifruojama naudojantis Merkle ir Hellmano kuprinės kriptosistema?

Privatus raktas $K_p = \langle W, s \rangle$
Viešas raktas $K_v = \langle v_1, v_2, \dots, v_n \rangle$
Šifruojama: $C = e(m_1 \dots m_n | K_v) = m_1 v_1 + \dots + m_n v_n$
Dešifruojama: $C_1 \equiv Cs \pmod{p}$, kur $C_1 = m_1 w_1 + \dots + m_n w_n$
 $m_1 \dots m_n = d(C | K_p)$ // wat..?

9.8. Irodykite, kad kuprinės kriptosistemos dešifravimo algoritmas veikia teisingai.

9.9. Apibrėžkite Rabino kriptosistemą.

Privatus raktas - $K_{pr} = \langle p, q \rangle$, p, q – pirminiai skaičiai, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$.

Viešas raktas $K_v = \langle n = pq \rangle$

Šifravimas $c = e(m | K_v) = m^* m \pmod{n}$
Dešifravimas $m_1 = c^{(p+1)/4} \pmod{p}$ // shit load of text and letters to remember...
 $m_2 = c^{(q+1)/4} \pmod{q}$
 $uq \equiv 1 \pmod{p}$; $vp \equiv 1 \pmod{q}$
 $m \equiv \pm m_1 uq \pm m_2 vp \pmod{n}$

9.10. Lyginio $x^2 \equiv 14 \pmod{43}$ sprendinys tikrai egzistuoja. Kaip galima greitai jį rasti?

9.11. Paaiškinkite, kaip dešifruojamas Rabino kriptosistemos šifras.

Dešifravimas $m_1 = c^{(p+1)/4} \pmod{p}$ // shit load of text and letters to remember...
 $m_2 = c^{(q+1)/4} \pmod{q}$
 $uq \equiv 1 \pmod{p}$; $vp \equiv 1 \pmod{q}$
 $m \equiv \pm m_1 uq \pm m_2 vp \pmod{n}$

10. Diskretus logaritmas ir jo taikymai

10.1. Kaip generuojamas grupės Z_p elementas?

10.2. Kaip ieškoti grupės Z_p generuojančio elemento?

Reikia rasti g , kurį keliant laipsniais $0, 1, \dots, p-1$, mod p gauname aibę elementų, visas įmanomos liekanas $0, 1, \dots, p-1$.

G yra primityvi vieneto šaknis moduliu p (generuojantis elementas) tada ir tik tada, kai kiekvienam netrivialiam $p-1$ dalikliui d galioja $g^d \not\equiv 1 \pmod{p}$.

10.3. Patikrinkite, ar $g = 2$ yra Z_7 generuojantis elementas.

$$\begin{array}{ll} g^0 \bmod 7 = 1 & g^4 \bmod 7 = 2 \\ g^1 \bmod 7 = 2 & g^5 \bmod 7 = 4 \\ g^2 \bmod 7 = 4 & g^6 \bmod 7 = 1 \\ g^3 \bmod 7 = 1 & \end{array}$$

Gaunama liekanų aibė yra tik $\{1, 2, 4\} \rightarrow 2$ nėra generuojantis elementas

10.4. Suraskite vieną Z_{11} generuojantį elementą. Užrašykite, kokius skaičiavimus atlikote.

10.5. Kas yra elemento $x \in Z_p$ diskretus logaritmas, pagrindu g ?

Kai p yra pirminis skaičius, o g – generuojantis grupės elementas, tai skaičiaus x diskretus logaritmas pagrindu g yra skaičius A , su kuriuo :

$$g^A = x, \quad 0 \leq A \leq p-2.$$

Diskretus logaritmas žymimas $A = \log_g x$

10.6. Kaip šifruojama ir dešifruojama El Gamalio kriptosistemoje?

p – pirminis skaičius. g - generuojantis elementas moduliu p , $0 < a <= p-1$

$$K_v = \langle p, g, \beta \rangle, \quad \beta = g^a \pmod{p}, \quad K_p = \langle a \rangle.$$

Iš grupės Z_p^* parenkamas skaičius k .

Šifras sudaromas taip:

$$\begin{aligned} C_1 &\equiv g^k \pmod{p}, \quad C_2 \equiv M\beta^k \pmod{p} \quad // M - šifruojama žinutė \\ e(M, K_v) &= \langle C_1, C_2 \rangle = C. \end{aligned}$$

Dešifruojama šitaip:

$$d(C, K_p) \equiv C_2 / (C_1^a) \pmod{p}.$$

10.7. Irodykite, kad El Gamalio kriptosistemoje dešifravimo algoritmas veikia teisingai.

10.8. Kuo pagrįstas El Gamalio kriptosistemos saugumas?

Saugumas pagrįstas tuo, kad diskretus logaritmo uždavinio sprendimas yra sunkus ir ilgas procesas...

10.9. Kaip sudaromas El Gamalio skaitmeninis parašas?

Privatus raktas $K_p = \langle a \rangle$, kur a priklauso grupei Z_{p-1}

$$\begin{array}{lll} \text{Viešas raktas } K_v = \langle p, \alpha, \beta \rangle, & \text{kur } p - \text{ didelis pirminis skaičius,} & \beta = \alpha^a \pmod{p} \\ \text{Parašo sudarymas:} & & // \text{SHIT LOAD OF INFO} \end{array}$$

Pasirenkamas atsitiktinis k , toks kad $(k, p-1) = 1$. Skaičiuojama:

$$\gamma = \alpha^k \pmod{p}$$

$$\delta = (x - a\gamma)/k \pmod{(p-1)}$$

$$\text{sig}(x | K_p) = \langle \gamma, \delta \rangle$$

- 10.10. Paaškinkite, kaip atlikti El Gamalio skaitmeninio parašo schemas ataką, turint du parašus, sudarytus su tuo pačiu parametru k.**

Taip galime rasti privatų raktą. $\text{sig}(x_1|K_p) = \langle \gamma, \delta_1 \rangle, \text{ sig}(x_2|K_p) = \langle \gamma, \delta_2 \rangle$
Turime dvi lygtis su trim
nežinomaisiais – pasirašyti duomenys ir privatus raktas. Kažkaip magiški iš to gauname privatų raktą.

- 10.11. Paaškinkite Shankso algoritmq diskrečiam logaritmui rasti.** // just no... like why...

11. Raktų nustatymo protokolai

- 11.1. Paaškinkite Wide-Mouth Frog protokolą.**

A ir B yra veikėjų ID, serveris S. T_a ir T_s yra atitinkamai generuojamos laiko žymės. K_{as} yra simetrinis raktas, žinomas veikėjui A ir serveriui S. K_{bs} yra asimetrinis raktas tarp B ir S. K_{ab} yra generuotas sesijos raktas.

A -> S: savo ID, Kas raktu užšifruota žymę T_a , B ID, K_{ab} (sesijos raktą).

S patiktina laiko žymę, jei viskas gerai –

S -> B: raktu K_{bs} užšifruotą savo laiko žymę, A ID, K_{ab} sesijos raktą.

Jei B gavės informacija patirkina, ar šios žinutės laiko žymė yra vėlesnė nei bet kurios kitos, gautos iš S.

Galimos problemos – laikrodžių sinchronizacija, raktų nustatymas.

- 11.2. Paaškinkite Needhamo-Schroederio raktų nustatymo protokolą.**

A ir B yra veikėjų ID. Serveris S. K_{as} yra simetrinis raktas, žinomas veikėjui A ir serveriui S. K_{bs} yra asimetrinis raktas tarp B ir S. N_a ir N_b yra A ir B generuoti skaičiai - žinutės. K_{ab} – sesijos raktas tarp A ir B.

A -> S: A ir B ID, N_a skaičių.

S -> A: K_{as} raktu užšifruota: žinutė N_a , sesijos raktas K_{ab} , B ID, K_{ab} ir A, užšifruota K_{bs} .

A -> B: K_{ab} ir A, užšifruota K_{bs} , kurį gavo iš S.

B -> A: N_b žinutė, užšifruot sesijos raktu – parodo, kad turi raktą.

A -> B: N_b -1, užšifruotas sesijos raktu. Taip parodo, kad susijungimas vis dar yra, ir abu turi raktus.

- 11.3. Paaškinkite Kerboros protokolą.**

Vartotojas A. Serveris S. Paslaugų teikėjo serveris P. K_a, K_s, K_p atitinkami raktai. K – sesijos raktas.

- 11.4. Paaškinkite Diffie-Hellmano raktų nustatymo protokolą.**

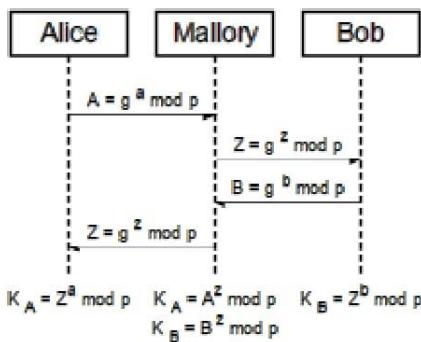
Naudojama ciklinė grupė G, p – didelis pirminis skaičius, g – generuojantis G elementas.

A -> B: $Y_a = g^u$, kur u – sugalvotas skaičius.

B -> A: $Y_b = g^v$, kur v – sugalvotas skaičius

$K = Y_b^u = Y_a^v = g^{uv}$.

- 11.5. Paaškinkite, kaip vykdoma įsiterpimo (man in the middle) ataka.**



11.6. Paaškinkite Diffie-Hellmano raktų nustatymo protokolą su parašais.

Tikslas – išvengti Man in the middle atakos. Susitariama dėl ciklinės grupės G , p didelis pirminis skaičius, g – G generuojantis elementas. K_{Ap} ir K_{Bp} yra CA sertifikuoti viešieji raktai.

$A \rightarrow B$: pasirenka atsitiktinį u . Skaičiuoja $Y_a = g^u$. Siunčia $\langle Y_a, \text{sig}(Y_a | K_{Ap}) \rangle$

$B \rightarrow A$: pasirenka atsitiktinį v . Skaičiuoja $Y_b = g^v$. Siunčia $\langle Y_b, \text{sig}(Y_b | K_{Bp}) \rangle$

Patikrinę parašus, A ir B randa sesijos raktą $K = Y_b^u = Y_a^v = g^{uv}$

11.7. Paaškinkite bendrais bruožais, kaip sertifikuojami vieši kriptosistemų raktai.

12. Paslapties pasidalijimas

12.1. Paaškinkite paslapties pasidalijimo su slenksčiu (t, w) schemas sąvoką.

Jei S yra paslaptis, o jos dalys yra S_1, S_2, \dots, S_w , kurias dalytojas įteikė dalyviams D_1, D_2, \dots, D_w .

Paslapties dalybos su slenksčiu t ($1 \leq t \leq w$) – toks paslapties padalijimas, kur galime paslapčią atkurti iš ne mažiau kaip t bet kurių paslapties dalių.

12.2. Kaip paslaptis padalijama ir atkuriama Shamiro schema su slenksčiu (w, w)?

Narių w . Sukurimas daugianaris $a(x) = S + a_1x + a_2x^2 + \dots + a_{w-1}x^{w-1}$, kur a_i – sugalvoti skaičiai.

Tada kiekviena paslapties dalis – funkcijos $a(x)$ reikšmė ($\text{mod } p$), jai paduodant vis skirtingą parametrą x .

Sudaroma w lygių sistema su w nežinomujų (visai su indeksas ir paslaptis S), naudojantis tuo daugianariu.

12.3. Padalykite paslapčią $s = 3$ trims dalyviams su slenksčiu $t = 2$ panaudoję modulį $p = 7$.

$$a(x) = 3 + a_1x + a_2x^2 = 3 + 4x + 2x^2$$

Visiems žinomas $p = 7$. Paslapties dalis - $\langle S_i, p \rangle$

$$S_1 = a(5) = 3 + 20 + 50 \pmod{7} = 3$$

$$S_2 = a(1) = 3 + 4 + 2 \pmod{7} = 2$$

$$S_3 = a(2) = 3 + 8 + 8 \pmod{7} = 5$$

12.4. Kas yra leidimų struktūra?

$D = \{D_1, \dots, D_n\}$ – dalyvių aibė. Jos poaibį sistemą G vadinsime leidimų struktūra, jeigu kiekvienos aibės A (poaibis G) viršaibis taip pat jeina į G .

Pakanka nurodyti tik tokią poaibį sistemos G posistemę Γ , kad su kiekviena aibe A ($A \in \Gamma$) jos poaibai nepriklausytų Γ .

// Understood nothing...

12.5. Yra trys paslapties schemas dalyviai 1, 2, 3. Leidimų struktūros branduolj sudaro du poaibiai {1, 2} ir {2, 3}. Padalykite paslaptj s = 2 pagal šia leidimų struktūrq.

12.6. Paaiškinkite Asmuth-Blumo paslapties padalijimo schemq.

Dalytojas pasirenka skaičius $p < p_1 < p_2 < \dots < p_n$, kad $(p_i, p_j) = 1$, $i \neq j$.

$$N = p_1 * p_2 * \dots * p_t$$

$$N^* = p_n * p_{n-1} * \dots * p_{n-t+2}$$

Paslaptis $S < p$. Dalytojas parenka skaičių r , kad $N^*/p < r < N/p - 1$.

Suskaičiuoja $S^* = S + rp$. Paslapties dalis $S_i \equiv S^* \pmod{p_i}$

Paslaptis atkuriama naudojantis kinų liekanų teoremą :

$$x \equiv S_{i,j} \pmod{p_{i,j}} \quad (j = 1, 2, \dots, t) \quad // I will not remember this...$$

$$x \equiv S^* \pmod{p_{i,1} * p_{i,2} * \dots * p_{i,t}}$$

$$S \equiv S^* \pmod{p}$$

13. Netiesioginiai įrodymai ir kita // Irena (I) įrodinėja Tomui(T)

13.1. Paaiškinkite interaktyvų Irenos įrodymą, kad ji žino diskrečio logaritmo reikšmę.

Viešos žinios : pirminis p , generuojantis elementas g ir y .

Irenos žinios : x , su kuriuo $y \equiv g^x \pmod{p}$

$I \rightarrow T$: parenka atsitiktinį r , siunčia $t \equiv g^r \pmod{p}$

$T \rightarrow I : c$ (parinktas atsitiktinis skaičius)

$I \rightarrow T : s \equiv r + cx \pmod{(p-1)}$. \rightarrow Tada T tikrina ar $g^s \equiv ty^c \pmod{p}$. Jei taip – priima Irenos žinojimą.

13.2. Paaiškinkite interaktyvų Irenos įrodymą, kad ji žino kvadratinio lyginio sprendinį (Fiat-Shamiro protokolas).

$I \rightarrow T$: pasirenka atsitiktinį skaičių r , atsitiktinai $\{-1, 1\}$, siunčia $x \equiv sr^2 \pmod{p}$

$T \rightarrow I : a_1, a_2, \dots, a_k$ – pasirinkti skaičiai, kur kiekvienas $= 0/1$

$I \rightarrow T$: suskaičiuoja $y \equiv r * (s_1^{a_1} * s_2^{a_2} * \dots * s_k^{a_k}) \pmod{p}$

T tikrina $y^2 \equiv \pm x(v_1^{a_1} * v_2^{a_2} * \dots * v_k^{a_k}) \pmod{p}$

Kartojama tol, kol Tomas patvirtina Irenos žinojimą.

13.3. Paaiškinkite, kaip sukuriamas skaitmeninis banknotas ECash schema.

A – veikėjas. B – bankas. A nori gauti 100 Eurų elektroniniai pinigais.

A sudaro n (nustatytą banko) skaitmeninių eilučių rinkinį $S = \{S_1, S_2, \dots, S_n\}$. Kiekvienoje eilutėje užrašyta A identifikuojanti informacija. Kiekviena eilutė kaip paslaptis padalijama į dvi dalis L_j ir R_j

A parengia n banknotų po 100 eurų $M = \{M_1, M_2, \dots, M_n\}$, (juose taip pat yra A identifikavimo informacija) kurie turi skirtingus identifikavimo numerius, juose sutartu būdu nurodoma banknoto vertė.

A maskuoja tuos banknotų numerius banko viešuoju raktu ir slaptu maskuojančiu daugikliu, siunčia bankui.

Bankas parenka $n-1$ atsiųstus banknotus, ir prašo, kad A nurodytų jiems kurti panaudotus maskuojančius daugiklius. Tada tikrina, ar banknotai sudaryti teisingai (vienodos vertės, skirtinti numeriai). Jei taip – pasirašo likusį vieną banknotą maskuojančiu daugikliu ir siunčia jį A, kuris pašalinės tą daugiklį gauna elektroninį banknotą ir tam tikrą jo priedą.

13.4. Išvardykite reikalavimus elektroniniams balsavimui.

1) Balsuoti gali tik užsiregistravę rinkėjai

2) Balsuoti galima tik kartą

- 3) Niekas negali sužinoti, už ką kas balsavo
(anonimiškumas)
- 4) Kiekvieno rinkėjo balsas turi būti užskaitytas
- 5) Rinkėjai negali kopijuoti vienas kito biuletenio.
- 6) Kiekvienas bandymas pakeisti biuletenius turi būti pastebėtas.

13.5. Paaiškinkite bendrais bruozias III elektroninio balsavimo protokolą.

Rinkėjas parengia n biuletenių, su skirtingais balsavimo rezultatais ir ilgais atsitiktiniais skaičiais.

Kiekvienas biuletenis maskuojamas ir siunčiamas CRK, kur pareikalaujama, jog rinkėjas atskleistų n-1 biuletenių. Tikrinama, ar jie sudaryti teisingai. Jei taip - likę neatskleisti pasirašomi, ir siunčiami atgal.

Rinkėjas pašalina maskuotę paskutiniojo biuletenio, pasirenka, už ką balsuos, sprendimą užšifruoja CRK viešu raktu, siunčia CRK, kuris dešifruoja biuletenį, tikrina parašą, tikrina, ar biuletenio skaičiaus dar nėra duomenų bazėje. Galiausiai, suskaičiuojami ir skelbiami rezultatai kartu su visų rinkėjų biuletenių numeriais, kad galėtų pasitikrinti, ar jų balsas įskaitytas.

13.6. Paaiškinkite monetos metimo protokolą, kuriame naudojami diskretieji logaritmai.

Lošėjai A ir B pasirenka pirminj skaičių ir du generuojančius elementus h ir s.

A atsitiktinai pasirenka skaičių x ir skaičiuoja $y \equiv h^x \pmod{p}$ arba $y \equiv s^x \pmod{p}$

H spėja, ar s, ar h buvo panaudotas skaičiavimui, A atsako, atspėjo ar ne. Tikrinimui, A atsiunčia B lošėjui x.