1 Kriptografija ir kriptosistemos

1.1 Kriptografijos uždaviniai: duomenų konfidencialumas, neišsiginamumas, vientisumas (kokiomis kriptografijos priemonėmis jie sprendžiami)

Duomenų konfidencialumas (confidentiality):

- perduodamos nesaugiu ryšiu kanalu informacijos negali perskaityti trečioji šalis.
- Užtikrinamas šifruojant duomenis

Neišsiginamumas (non-repudiation):

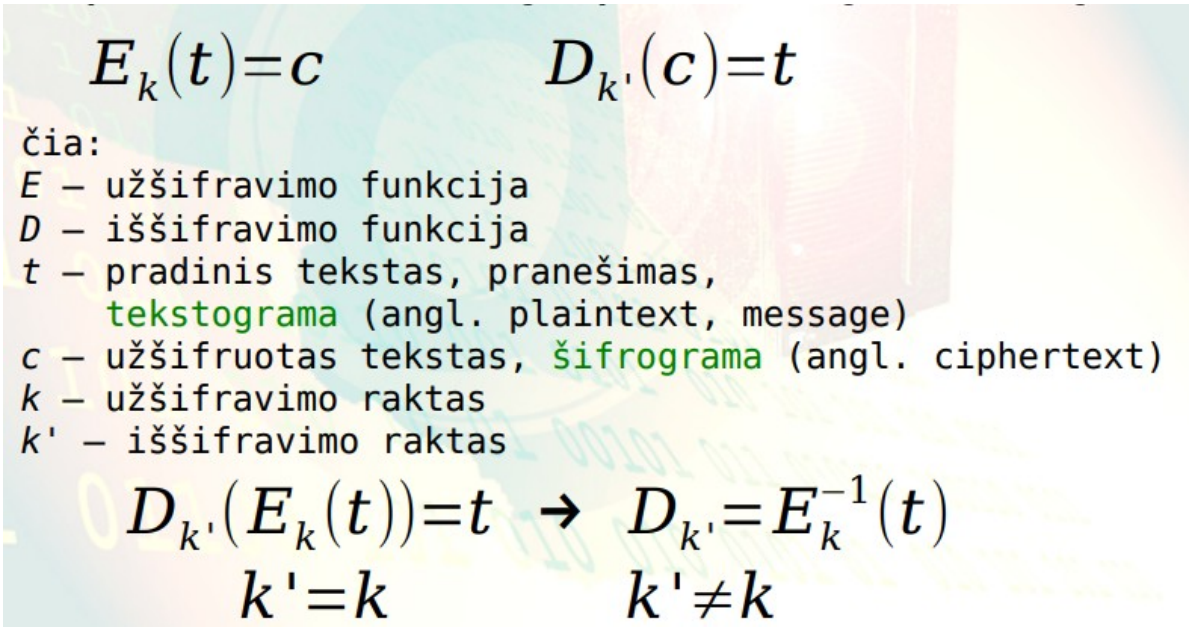
- Gavėjas turi turėti galimybę įsitikinti, jog duomenis tikrai pasiuntė siuntėjas, o ne juo apsimetanti trečioji šalis
- Užtikrinama naudojant skaitmeninius parašus ir/arba pranešimo autentifikavimo funkcijas

Vientisumas (intengrity):

- Siunčiamos informacijos turi būti neįmanoma pakeisti, sugadinti (tyčia ar netyčia) (taip, kad to nežinotų gavėjas)
- Maišos ir pranešimų autentifikavimo funkcijų naudojimas

1.2 Kriptosistema ir jos sudėtinės dalys (pagrindiai kriptografijos principai)

Kriptosistema – šifras arba kriptosistema yra pora abipus vienreikšmių (apverčiamų) funkcijų



Pagrindiniai principai:

- Kriptosistemos saugumas privalo būti pagrįstas jos parametrų slaptumu, tačiau turi būti nepriklausomas nuo algoritmo slaptumo

- Iššifravimo funkcija turi būti atvirkštinė užšifravimo funkcijai
- Funkcija E ir D turi būti abipus vienareikšmė (kiekvieną t atitinka vienas ir tik vienas c)
- Funkcijų E ir D išraiškos turi būti viešai žinomos
- Dažniausiai c, E ir D yra žinomi

1.3 Piktavalių tipai

Tipai:

- Pasyvieji:
  - Stebi informacijos mainus, gali ją kaupti, analizuoti
  - Pažeidžia informacijos konfidencialumą
- Aktyvieji
  - Stebi duomenų srautą ir gali patys imtis aktyvių veiksmų, nutraukti srautą, įsiterpti į duomenų srautą
  - Gali patys siųsti suklastotus duomenis
  - Perimti, sugadinti (pakeisti) ir persiųsti duomenis
  - Apsimesti kuria nors šalimo, realizuoti apsimetimo ataką (impersonation attack)
  - Pažeidžia dar ir vientisumą bei neišsiginamumą

1.4 Kriptosistemų atakų tipai

Atakų tipai:

- Dažnio analizė – šifrogramoje reikia surasti dažniausiai pasikartojančia raidę, apskaičiuoti per kiek pozicijų surasta raidė skiriasi nuo raidės „E“ („E“ dažniausia raidė anglų žodyne)
- Žodyno ataka (dictionary attack) – raktus bandome ne visus, o tik iš tam tikro sąrašo
- Pilno raktų perrinkimo ataka (brute force) – raktas turi būti ilgas, galimų rakto reikšmių turi būti daug

1.5 Dažnio analizės ataka

- Tarkime, norime sužinoti k, kai žinome jog:
  - naudojamas Cezario šifras
  - tekstogramos kalba yra anglų
- Anglų kalboje dažniausiai naudojama raidė „E“
- Šifrogramoje reikia surasti dažniausiai pasikartojančia raidę
- Apskaičiuoti per kiek pozicijų surasta raidė skiriasi nuo raidės „E“, tai ir bus raktas k

1.6 Lyginių aritmetika: mokėti patikrinti ar 2*2 lygsta -3*(-3) moduliu 5, žinoti ką reiškia atvirkštinis skaičius moduliu m

2*2=4

-3*(-3)=9

(4-9)/5=-1 (dalinasi be liekanos, reiškia, kad lygsta)

Žymime:

a=b (mod m)

Atvirkštinis skaičius moduliu m:

- Sveikam teigiamam skaičiui d<m (jei d ir m yra relatyviai pirminiai) egzistuoja atvirkštinis skaičius moduliu m, žymimas d’:
  - d’<m
  - d*d’=1 (mod m)
- Atvirkštinis skaičius yra lyginio sprendinys:
  - d*x=1 (mod m)
- Randamas sprendžiant lyginį

19 yra skaičiaus 4 atvirkštinis moduliu 25

19*4=1 mod 25

76=1

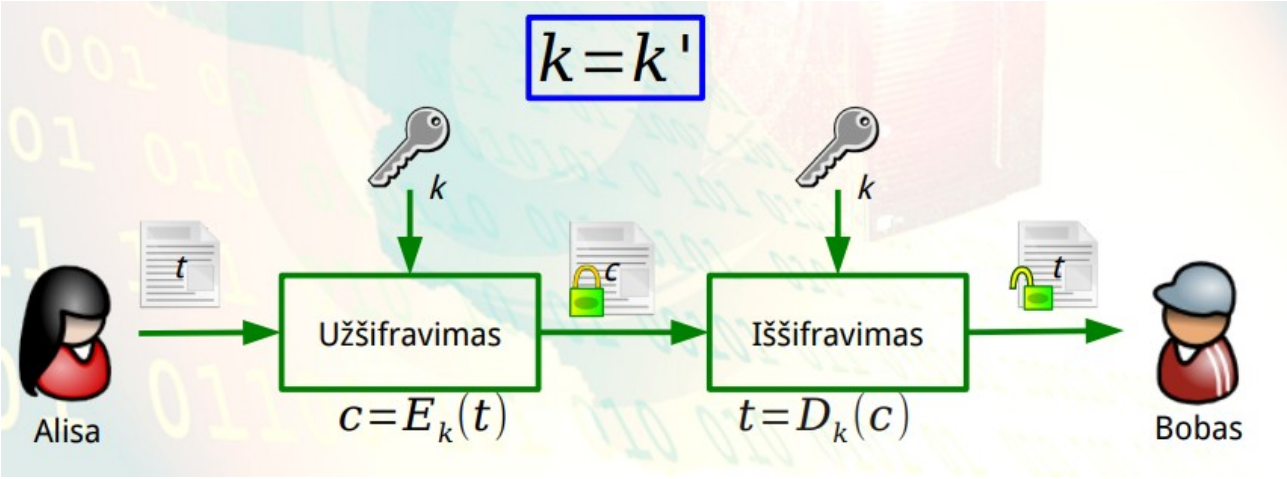
(76-1)/25=3

2 Simetrinės kriptosistemos

2.1 Simetrinių kriptosistemų tipai, bendra schema

Tipai:

- Blokiniai šifrai – tai simetrinis šifras, kuriuo užšifruotas tekstogramos blokas priklauso tik nuo pačios tekstogramos ir slaptojo rakto:
  - Kiekvienas duomenų blokas šifruojamas vienodu algoritmu
  - Blokai paprastai būna 64, 128, 512 bitų dydžio (priklauso nuo šifravimo algoritmo)
- Srautiniai šifrai (Stream) - kai šifruojamas duomenų srautas:
  - turi užtikrinti didelę užšifravimo spartą
  - turi užtikrinti darbą prijungties režimu



2.2 Šenono principai (paskleidimas ir sumaišymas)

Šenono principai (norint išvengti statistinės analizės), reikia naudoti:

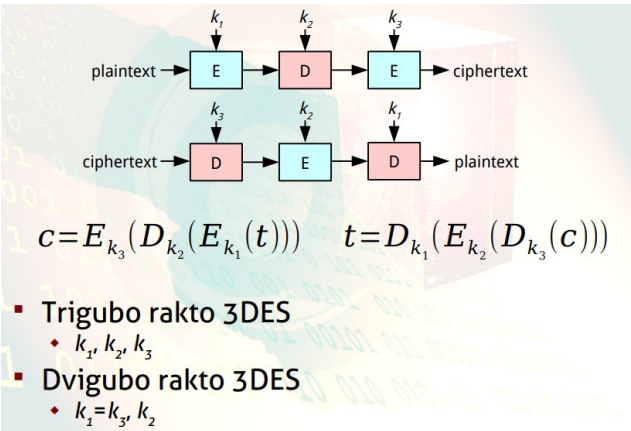
- Paskleidimo (Diffusion) mechanizmą – vieno bito pasikeitimas tekstogramoje turi pakeisti visą šifrogramą
- Sumaišymo (Confusion) mechanizmą – ryšius tarp šifrogramos ir rakto padaro kuo sudėtingesnius (sudėtinga funkcija E)

2.3 Blokinio šifro naudojimo schema

2.4 Blokiniai simetriniai šifrai (DES, 3DES, AES)

Blokiniai simetriniai šifrai:

- DES:
  - 64 bitų raktas
  - Blokas 64 bitų
  - Naudoja sukeitimo ir perstatymo operacijas per 16 vienodų raundų
  - Naudoja tik standartines kompiuterio aritmetines ir logines operacijas
- 3DES:



- AES:
  - blokas 128 bitų
  - raktas 128, 192 arba 256 bitų
  - raundų skaičius priklauso nuo rakto ilgio (10,12 ir 14)

2.5 Blokinių šifrų režimai (ECB ir CBC)

Blokiniai šifrų režimai naudoja norint užšifruoti didelį duomenų kiekį

ECB (electronic codebook):

- Tekstograma suskaitoma į m n bitų ilgio blokų
- Jei tekstogramos ilgis nėra n kartotinis, tai ji papildoma iki pilno bloko
- Kiekvienas blokas užšifruojamas slaptuoju raktu atskirai

CBC (Cipherblock chaining):

- Tekstogramos bloko užšifravimas priklauso ir nuo visų anksčiau užšifruotų blokų (Reikia IV)

2.6 Srautiniai simetriniai šifrai (RC4)

RC4:

- Naudojamas SSL, WEP
- WEP laikomas nesaugiu dėl neteisingo įgyvendinimo
- Rakto suratas – baitai, rakto ilgis 0-256 baitai
- Naudoja CRC

2.7 Pseudoatsitiktinės sekos generatorius, rakto srautas

Pseudoatsitiktinės sekos generatorius – neprognozuojamos rakto srautas

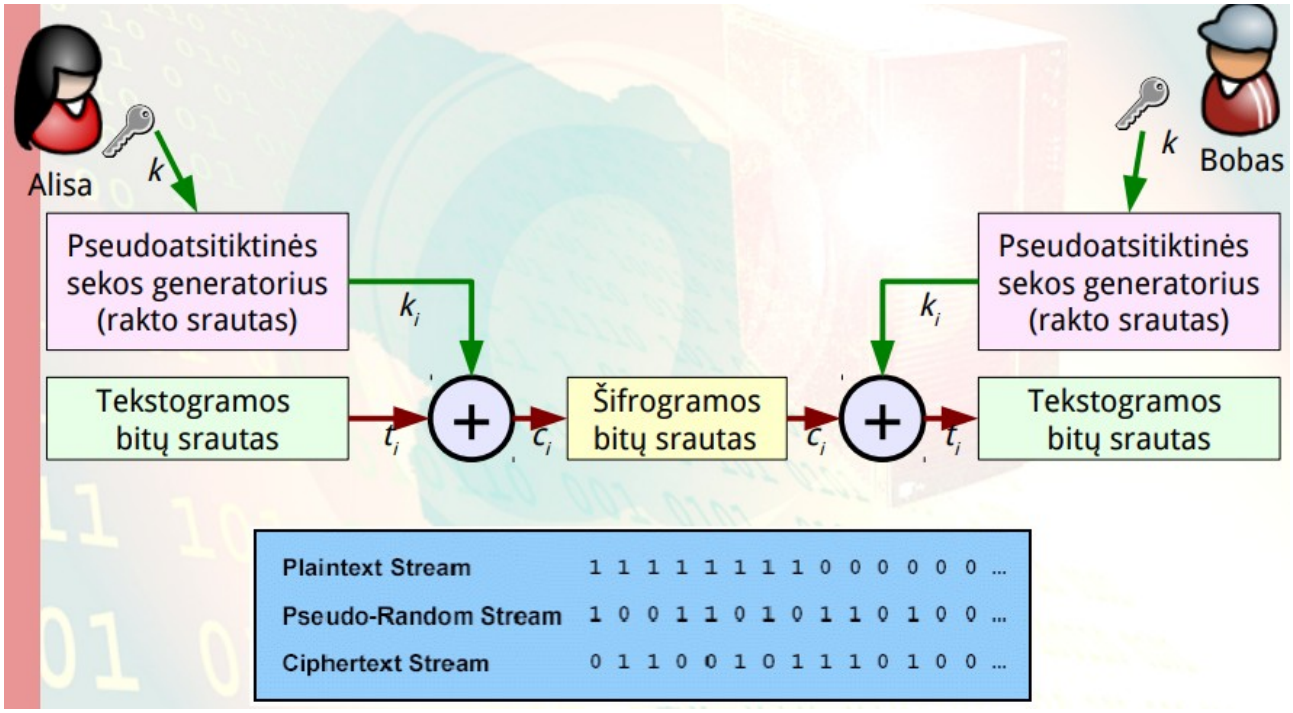
Rakto srautas -

2.8 Srautinio šifro naudojimo schema, savybės

Savybės:

- Didelė šifravimo sparta
- Darbas prijungties režimu
- Šifruoja nenutrūkstamą duomenų srautą, kurio mažiausias vienetas gali būti bitas, baitas ir pan.
- Būtinas labai ilgas raktas arba rakto srautas
- Paprasta šifravimo funkcija (pvz suma moduliu 2)

Schema:



2.9 Blokinio šifro OFB režimas

Blokinio šifro OFB režimas (output feedback):

- Iššifravimas ir užšifravimas visiškai vienodi
- IV būtina žinoti
- Negalima šifruoti lygiagrečiai
- Blokinį šifrą OFB režime, galima panaudoti kaip srautinį šifrą

2.10 Kriptografiniai protokolai

Kriptografiniai protokolai:

- protokolas – žingsnių seka, apimanti kelias šalis, suprojektuota įvykdyti tam tikrą užduotį:
  - turi žingsnių seką
  - turi pradines sąlygas
  - turi galutines sąlygas
- kiekvienas žingsnis vykdomas griežtai nustatytu laiku

2.11 Slaptojo rakto protokolų savybės ir trūkumai

SR protokolo savybės ir trūkumai:

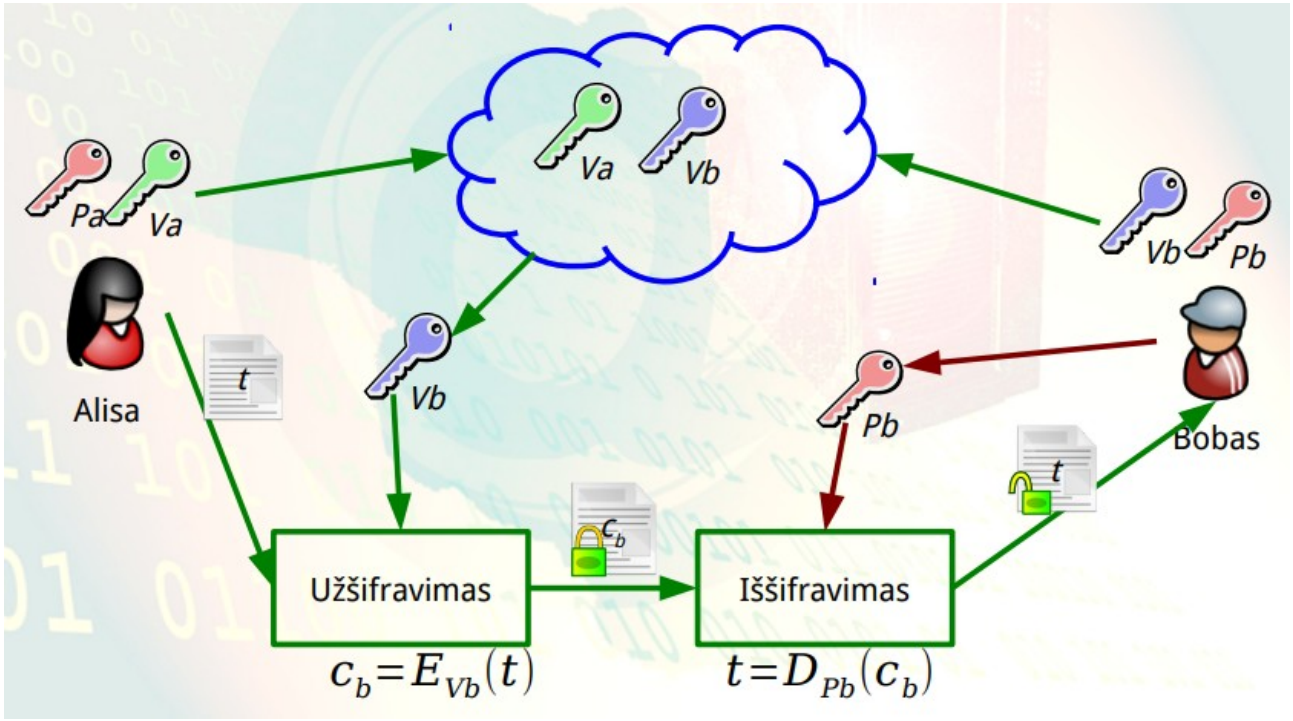
- reikalingas saugus būdas išplatinti raktus
- rakto atskleidimas – kompromituoja visus pranešimus

- jeigu kiekvienai vartotojų porai naudojami skirtingai raktai, tai raktų skaičius labai greitai auga didėjant vartotojų skaičiui

3 Asimetrinės kriptosistemos

3.1 Asimetrinio šifro naudojimo schema, savybės, raktai, raktų saugojimas ir administravimas

Schema:



Savybės:

- Kiekvienas subjektas turi vieną porą matematiškai susietų raktų
- Vienas poros raktas skirtsa užšifruoti, kitas iššifruoti
- Vienas yra viešasis, kitas privatusis
- Žinant viešąjį raktą, neįmanoma sužinoti privačiojo

3.2 RSA, faktorizavimo ir diskrečiojo logaritmo uždaviniai

RSA – viena iš populiariausių asimetrinių sistemų:

- pirmas praktiškai įgyvendintas metodas
- laikomas patikimu ir vienas populiariausių iki šiol
- remiasi faktorizavimo uždavinio sudėtingumu
- nuo 300 skaitmenų RSA laikoma patikima

Faktorizavimas:

- Žinome, jog n=p*q, čia p ir q pirminiai skaičiai
- **Uždavinys:** duotas n, rasti p ir q:
  - Tikrinti visus galimus skaičius iki √n
  - Netikrinti lyginių skaičių √n/2
  - Tikrinti tik pirminius skaičius

Diskrečiojo logaritmo uždaviniai:

- Modulinė eksponentė $y=g^x \pmod p$:
  - Pvz. Jei g=5, x=3, o p=13, tai y=8

3.3 RSA asimetrinė kriptosistema

Rakto generavimas:

1. Imkime du pirminius skaičius p ir q
2. Apskaičiuokime n=p*q
3. Apskaičiuokimo skaičių (Oilerio funkcijos reikšmę) m=(p-1)(q-1)
4. Imkime skaičių e, 1<e<m; (e, m)=1
5. Apskaičiuojame e atvirkštinį moduliu m
   1. e’=d (mod m);
   2. ed=1 (mod m)
6. Viešas raktas: (e, n)
7. Privatus raktas: (d, n)

Užšifravimas ir iššifravimas:

- Užšifravimas (atlieka siuntėjas): $c=t^e \pmod n$
- Iššifravimas (atlieka gavėjas): $t=c^d \pmod n$

3.4 ElGamal asimetrinė kriptosistema

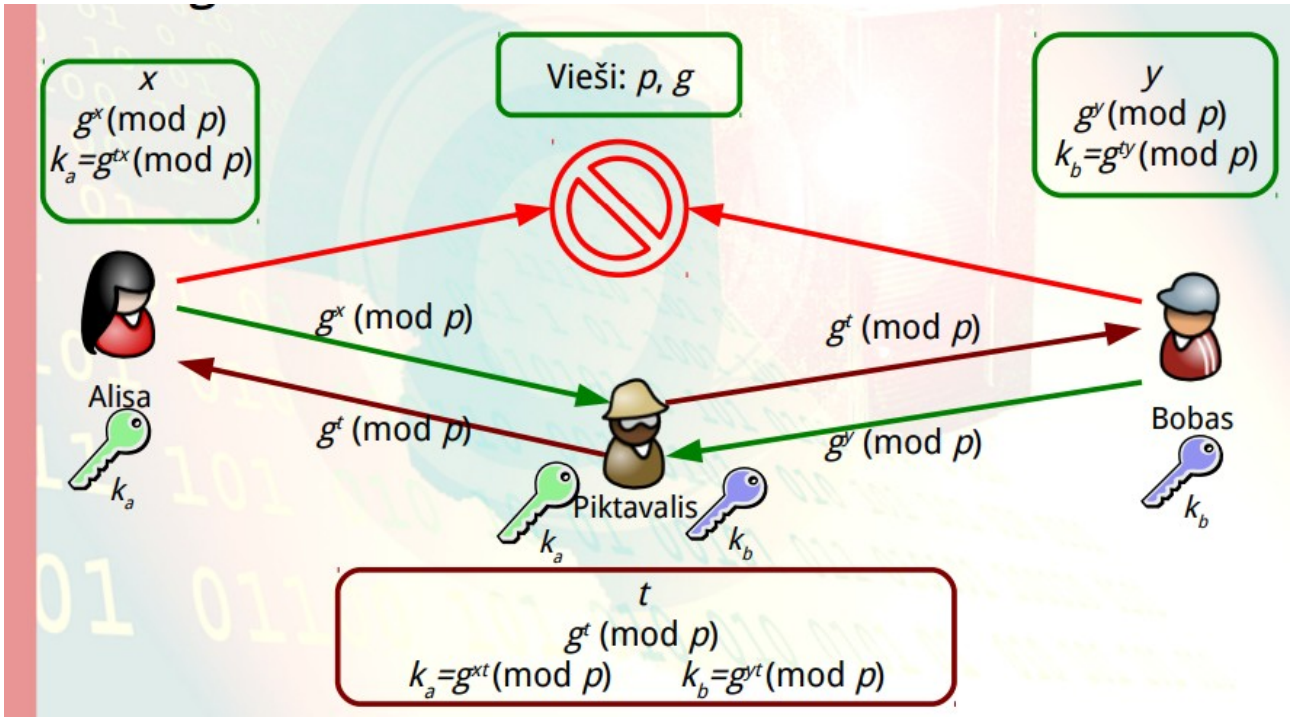
Raktų generavimas:

- Imkime didelį pirminį sksaičių p
- Pasirinkime kitą specifinį skaičių g
- Pasirinkime atsitiktinį skaičių x
- Apskaičiuokime a: $a=g^x \pmod p$ 0<a<p
- Viešasis raktas: a, privatusis raktas: x

3.5 Diffe Hellman raktų apsikeitimo protokolas

1. Alisa (A) ir Bobas (B) susitaria naudoti:
    1. Didelį pirminį skaičių p
    2. Generatorių g
2. Alisa pasirenka slaptą skaičių x, Bobas pasirenka slaptą skaičių y
3. Alisa apskaičiuoja $V_a=g^x \pmod p$ ir nusisunčia jį B, Bobas apskaičiuoja $V_b=g^y \pmod p$
4. Alisa apskaičiuoja $k=(V_b)^x \pmod p$, Bobas apskaičiuoja $k=(V_a)^y \pmod p$
5. Abu raktai k vienodi, nes: $k=(g^x)^y=(g^y)^x$

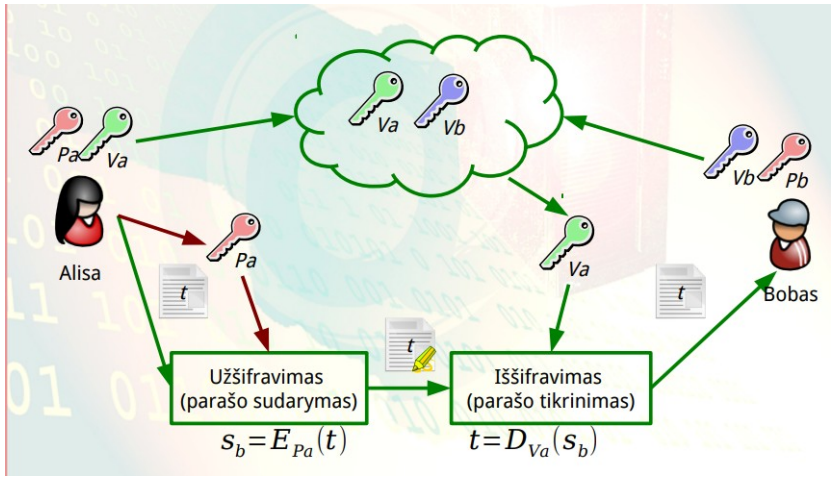
3.6 Ataka ,,žmogus viduryje”



4 El. parašas

4.1 Elektroniio parašo schema, raktai

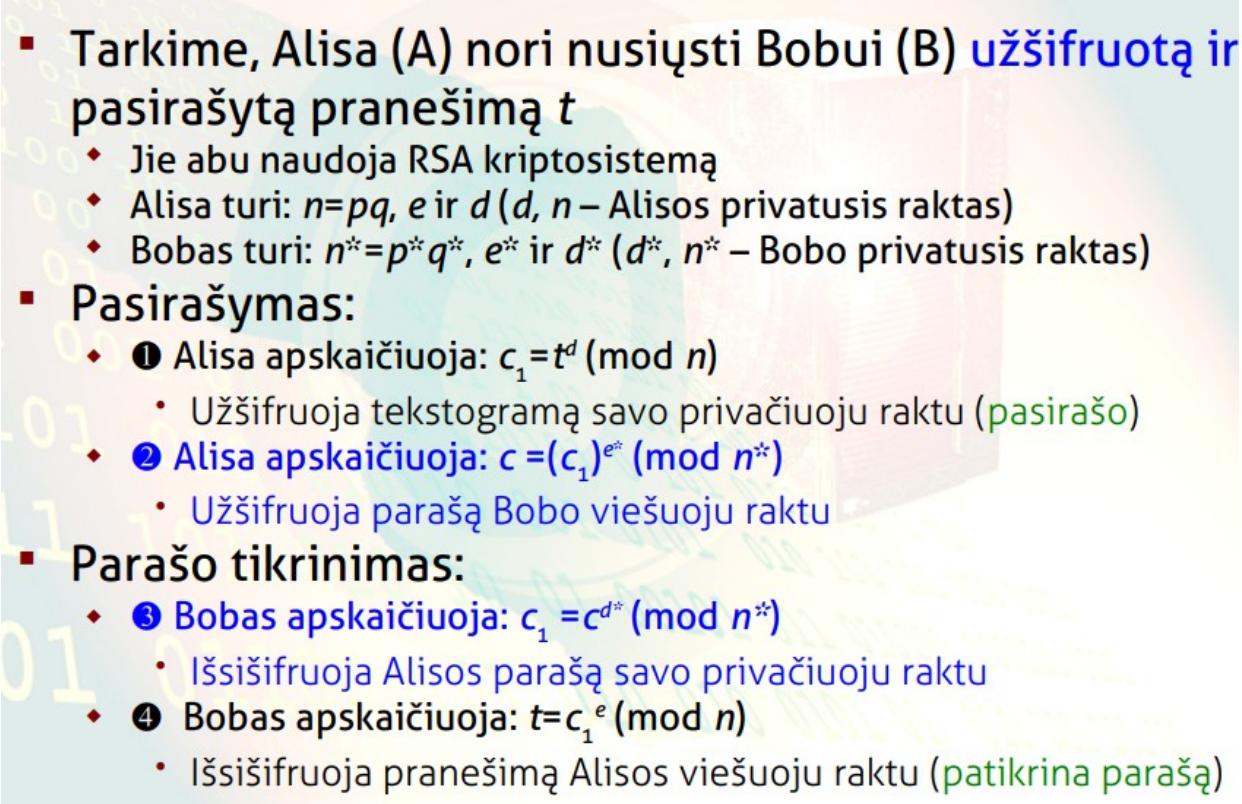
Schema:



Raktai:

- El. parašas užtikrina neišsiginamumo principą
- Pagal funkcionalumą atitinka įprastą žmogaus parašą dokumento pabaigoje
- turi identifikuoti tą kas pasirašo
- jį turi sugebėti sudaryti tik pati pasirašanti šalis
- gavėjas turi turėti galimybę patikrinti ar siuntėjas pasirašė būtent gautą dokumentą
- kai gauname mūsų viešuoju raktu užšifruotą pranešimą, mes nežinome kas jį pasiuntė

4.2 RSA skaitmeninio parašo apskaičiavimas



4.3 ElGamal ir DSA skaitmeninis parašas (tik bendri principai)

ElGamal skaitmeninis parašas:

- Pasirašymo algoritmas skiriasi nuo šifravimo
- Skirtingos išraiškos pasirašymui ir parašo tikrinimui
- Pasirašoma naudojant privatųjį raktą
- Parašas tikrinamas naudojant viešąjį raktą

DSA skaitmeninis parašas:

- tik pasirašymo metodas
- naudoja modifikuotą ElGamal kriptosistemos pasirašymo algoritmą

- NIST standartas numato tik 1024 bitų modulio naudojimą
- Naudojamas SSH protokole vartotojo autentifikavimui

4.4 ASM naudojimas ir veikimo principai

ASM (Aparatinis saugos modulis) naudojimas ir veikimo principai:

- Greitai veikia
- Labai brangus
- Neleidžia eksportuoti privataus rakto

4.5 Asimetrinių kriptosistemų trūkumai

Trūkumai:

- Reikalauja daug daugiau skaičiavimo išteklių:
  - bendru atveju net iki 1000 kartų daugiau
  - RSA 1000 kartų lėtesnė už DES, jei realizuojama techninėje įrangoje
- Neatsparios parinktos tekstogramos atakoms

4.6 Hibridinės kriptosistemos, sesijos raktas

Hibridinės kriptosistemos:

1. Bobas pasiunčia Alisai savo viešąjį raktą
2. Alisa sugeneruoja reikiamo ilgio atsitiktinį skaičių k – sesijos raktą. Jį užšifruoja Bobo viešuoju raktu ir pasiunčia Bobui
3. Bobas išsišifruoja sesijos raktą k savo privačiuoju raktu
4. Toliau savo bendravimą jie abu šifruoja simetriniu šifru naudodami sesijos raktą k

- Nelieka simetrinio rakto problemų
- Labai mažai naudojama asimetrinė kriptosistema, dėl to:
  - Veikia greitai
  - Šifruojama labai mažai duomenų, sunku atlikti atakas
- Neturi forward secrecy savybės
- Autentifikavosi tik viena šalis (Bobas nežino su kuo bendrauja)
- Sesijos raktą turėtų diktuoti abi šalys

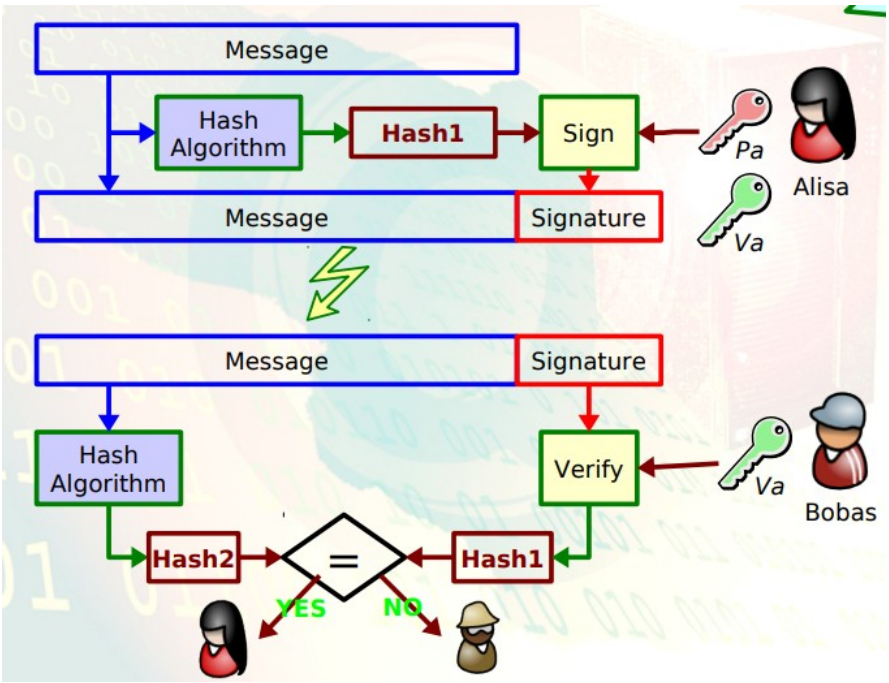
5 Maišos funkcijos ir jų taikymai. El. Vokas

5.1 Kriptografinės maišos funkcijos savybės, kolizijos, maišos rezultatai ir santraukos

Maišos funkcijos savybės:

- iš bet kokio ilgio pranešimo t suformuoja fiksuoto ilgio duomenų bloką H(t), kuris vadinamas:
  - santrauka
  - maišos rezultatu
- suspaudžiantis atvaizdis
- spartus santraukos skaičiavimas
- itin sudėtingas pranešimo atkūrimas iš santraukos (dėl menkiausių duomenų pakitimų turi visiškai pakisti ir maišos rezultatas)
- atspraios kolizijai (piktavalis neturi galimybės parinkti kitą pranešimą turintį tą pačią santrauką)
- santraukos funkcijos gali būti:
  - Nepriklausančios nuo slapto parametro
  - Priklausančios nuo slapto parametro (HMAC)
- Santrauka – lyg pranešimo pirštų antspaudas

5.2 Santraukų naudojimas vientisumui užtikrinti



5.3 MD5, SHA-1, SHA-2 ir SHA-3 maišos funkcijų savybės ir saugumas

MD5:

- Išėjo 1992 m.
- Naudoja 512b blokus
- Santrauka 128 bitų ilgio
- Buvo rasti keli silpnumai (dabar naudoti nerekomenduojama)
- Šiuo metu sugeneruoti koliziją galima per kelias sekundes

SHA-1:

- 1995 m. pasiūlė NIST
- Santrauka 160 bitų ilgio
- Veikimas panašus į MD5
- Pranešimas papildomas iki 512b kartotinio
- Dirba su 512b blokais, kiekvienas blokas dalinamas į 16 žodžių (po 32b)
- Kiekvienas žodis apdorojamas per 80 žingsnių
- Nesaugus

SHA2:

- SHA-256 ir SHA-52 yra naujos maišos funkcijos:
    - Naudoja 32 arba 64 bitų žodžius
    - Algoritmas panašus, tik naudojamas skirtingos konstantos, raundų kiekis ir pan.
    - Skirtingi ilgiai reikalingi patogiam darbui kartu su šifravimo metodais (AES, 2k3DES, 3DES ir pan.)

SHA3:

- Nepanašus į SHA ir MD
- 2012 metais

5.4 Maiša naudojant blokinius šifravimo metodus

- Jei šifravimo metodas saugus, tai ir maišos funkcija bus saugi
- Galima paimti blokinį šifrą ir naudoti CBC režime
- Parinkti fiksuotą, visiems žinomą raktą ir IV
- Santraukos reikšmė gali būti paskutinis šifrogramos blokas
- Dažniausiai naudojamas DES (3DES)
- Geriau kaip raktą naudoti tekstogramos bloką ir šifruoti prieš tai gautą režultatą
- 64b maišos rezultatas yra per trumpas

5.5 Pranešimų autentifikavimo kodai (MAC ir HMAC), HMAC apskaičiavimo principas

MAC:

- Nuo slapto parametro priklausančios santraukos vadinamos pranešimo autentifikavimo kodais (MAC):
  - MAC užtikrina ir duomenų vientisumą ir neišsiginamumą (autentiškumą)
  - Kadangi MAC sudaryme naudojamas ir slaptasis raktas, tai pranešimo vientisumą gali patikrinti tik gavėjas turintis tą patį slaptąjį raktą
- Turi tas pačias savybes kaip ir paprastos santraukos

HMAC – skaičiuojant pranešimo santrauką naudoja kokią nors maišos funkciją ir slaptajį raktą:

- dažnai naudojamos populiariausios kriptografiškai saugios maišos funkcijos SHA-1, MD5, SHA-256
- atitinkamai HMAC metodai vadinami: HMAC-SHA1, HMAC-MD5, HMAC-SHA256

5.6 Maišos funkcijų taikymas pasirašant didelius dokumentus

1. Alisa apskaičiuoja dokumento santrauką
2. Alisa užšifruoja santrauką savo privačiuoju raktu, taip ją pasirašydama
3. Alisa siunčia dokumentą ir pasirašytą santrauką Bobui
4. Bobas naudoja tą pačią maišos funkciją ir apskaičiuoja gauto dokumento santrauką
5. Alisos viešuoju raktu išsišifruoja gautą santrauką
6. Sulygina abi satraukas
7. Jei jos sutampa – parašas galioja

5.7 Maišos funkcijų taikymas saugant slaptažodžius

Serveris Bobas saugo vartotojų sąrašą ir jų slaptažodžių maišos rezultatus

1. Alisa nusiaunčia Bobui savo slaptažodį
2. Bosas apskaičiuoja maišos rezultatą
3. Bobas patikrina ar gautas maišos rezultatas sutampa su saugomu

Piktavaliui įsilaužus į serverį ir pasisavinus slaptažodžių sąrašą, jis negali juo pasinaudoti ir prisijungti prie serverio

Tačiau slaptažodžiai saugomi kaip maišos rezultatai yra nepakankamai saugūs:

- Galima s ukurti DB visų potencialiai galimų slaptažodžių ir išsisaugoti
- Dviejų vartotojų vienodi slaptažodžiai atrodys vienodai

Dėl to reiktų naudoti ,,druską”:

- druska – atsitiktinė eilutė, kuri pridedama prie slaptažodžio prieš skaičiuojant jo maišos rezultatą
- Po to ši eilutė atvirai išsaugoma kartu su maišos rezultatu
- Tokiu būdu neįmanoma iš anksto pasigaminti lentelių

5.8 Skaitmeninis vokas

- Skaitmeninis vokas sudarytas iš pranešimo užšifruoto naudojant kokią nors simetrinę kriptosistemą ir slaptojo rakto užšifruoto naudojant kitą raktą:
    - Dažniausiai slaptojo rakto užšifravimui naudojama viešojo rakto kriptosistema
    - Galima panaudoti vietoj DH protokolo slapto sesijos rakto susigeneravimui ir perdavimui
    - Galima panaudoti didelių dokumentų efektyviam šifravimui
- Privalumai:
    - Nereikia saugoti slaptojo rakto, galima perduoti kitai šaliai
    - Daug didesnis našumas nei asimetrinės kriptosistemos

6 Saugos metodų taikymai programavime

6.1 JCA architekrūra, kriptografinių paslaugų tiekėjai

JCA architekūra – Java platformos dalis aprašanti kriptografinių paslaugų tiekėjų (Provider) architektūrą ir API rinkinį skirtą dirbti su:

- Skaitmeniniais parašais
- Maišos funkcijomis ir pranešimų santraukomis
- Sertifikatais, sertifikatų tikrinimu
- Simetrinių, asimetrinių, blokinių, srautinių kriptosistemų funkcijomis
- Raktų generavimo ir valdymo funkcijomis
- Raktų apsikeitimo protokolais
- Nepriklausomumas nuo įgyvendinimo (programa nerealizuoja jokių saugos metodų, juos realizuoja nepriklausomi tiekėjai)
- Realizavimo nepriklausomumas (saugos paslaugų tiekėjai yra nepriklausomi nuo programos, programa neturėtų būti susieta su konkrečiu tiekėju)

6.2 Kaip veikia MessageDigest.getInstance(“MD5”, “ProviderC”) ir panašūs metodai

- Norėdama pasinaudoti JCA, programa paprašo specialaus tipo objekto egzemplioriaus, nurodydama algoritmą ar paslaugą (šio atveju „MD5“):
  - SHA1 arba MD5
  - Gauna vieno iš įdiegtų tiekėjų klasės egzempliorių pagal prioritetą
- Programa gali nurodyti, jog nori specifinio tiekėjo klasės (Šio atveju „ProviderC“)
- Programa kreipiasi į getinstance() factory metodą, kuris paprašo JCA surasti pagal duotus parametrus Provider klasės egzempliorių. Sukuriamas tos klasės egzempliorius, jis enkapsuliuojamas ir grąžinamas programai

6.3 Kuo iš esmės skiriasi objektai Key ir KeySpec

- Klasė Cipher reikalauja Key tipo objekto
- Norint išsaugoti ar perduoti raktų duomenis naudojamsa KeySpec
- Tiekėjai gali išplėsti KeySpec interfeisą savo specifiniais interfeisais

6.4 PKCS#5/#7 užpildai blokiniams šiframs

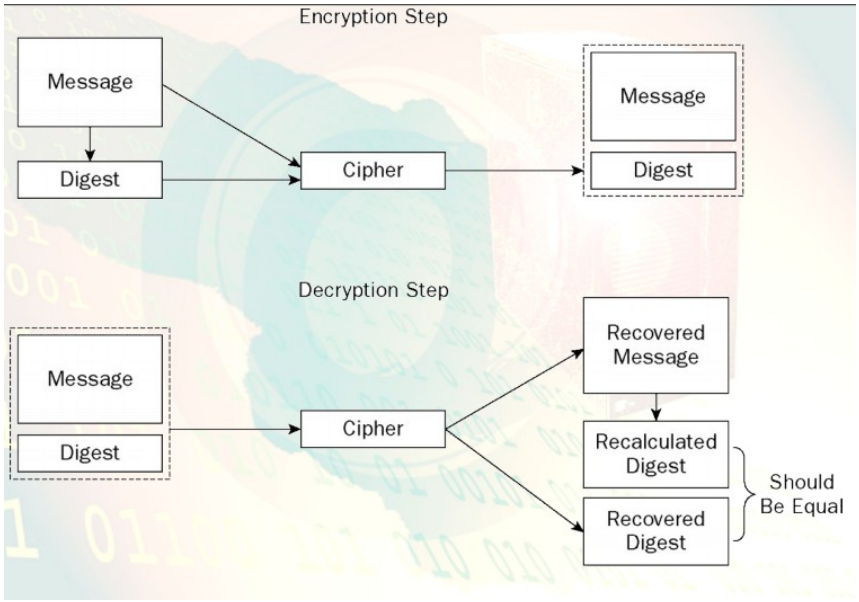
PCKS – užpildui naudojami skaičius kiek reikia baitų užpildyti iki pilno bloko

PKCS#5 – naudojamas 8 baitų blokams

PKCS#7 – naudojamas 255 baitų blokams

6.5 Srautinių šifrų vientisumo užtikrinimo problema. MAC būtinumas

Srautinio šifro vientisumo užtikrinimas:

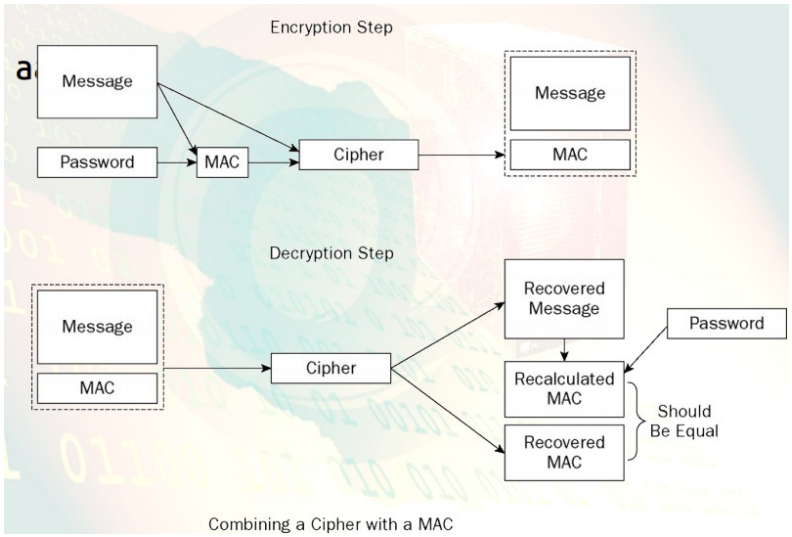


MAC būtinumas:

- Naudojant srautinį šifrą ir paprastą santrauką galima padaryti taip, kad pakeistas tekstas būtų „neaptinkamas“:
  - Tam rekia žinoti ir pradinį tekstą
  - Galima sukonstruoti korektišką užšifruotą pranešimą su santrauka net nežinant slaptažodžio
  - Pagrįstas sumos moduliu 2 savybėmis

6.6 Saugus santraukų palyginimas. Laiko ataka

Palyginimas:



Laiko ataka – jeigu einama per gautos santraukos kiekvieną skaičių ir lyginama su paskaičiuotu skaičiumi, tai stebint apskaičiavimo laiką galima gauti reikalingą santrauką.

Norint to išvengti reiktų eiti per visą paskaičiuotą santraukos baitas, jį sumuoti moduliu 2 ir tą suma tik tada lyginti su gautu. Tokio palyginimo laikas visada sutaps

6.7 RSA kriptosistemos naudojimo problemos. RSA užpildo būtinumas: PKCS#1 RSA užpildas, Kodėl RSA užpildas pridedamas į pradžią, o ne į galą?

RSA kriptosistemos naudojimo problemos:

- Tekstograma gali būti sugadinta, kai pridedamas užpildas į priekį jeigu nenaudojami ,,dideli" skaičiai

RSA užpildo būtinumas: PKCS#1 RSA užpildas:

- PKCS#1 standartas aprašo 3 galimus užpildų tipus:
  - Type 0 užpildui naudojami ,,0"
  - Type 1 naudojamas tada, kai šifruojama privačiuoju raktu (pasirašant)
  - Type 2 naudojamas tada, kai šifruojama viešuoju raktu (šifravimui)

Užpildas pridedamas į pradžia dėl to, kad būtų galima išvengti tekstogramos sugadinimo

7 IP tinklais perduodamų duomenų sauga

7.1 SMIME naudojami saugos algoritmai: pasirašytų ir užšifruotų laiškų pagrindinės sudėtinės dalys, pasirašymo ir šifravimo esminiai žingsniai

SMIME – yra standartas nusakantis kaip naudojant MIME perduoti užšifruotus ir/ar pasirašytus pranešimus

SMIME naudojami saugos algoritmai:

- Pranešimo santraukai:
  - Privalomas: SHA-256
  - Rekomenduojamas: SHA-1-, MD5-
- Skaitmeniniam parašui:
  - Privalomas: RSA su SHA-256
  - Rekomenduojamas: DSA su SHA-256, SHA-1-, MD5-
- Asimetriniam šifravimui (raktų šifravimui):
  - Privalomas: RSA
  - Rekomenduojamas: RSAES-OAEP+, DH
- Simetriniam šifravimui:

    - Privaloma: AES-128 CBC
    - Rekomenduojama: AES-192 CBC+, AES-256 CDB+, DES EDE3 CBC-

Laiškų sudėtinės dalys:

- Visada sudarytas iš dviejų MIME elementų:
    - Pirmasis MIME elementas – tai kas yra pasirašoma
    - Antrasis – parašas

Pasirašymo procesas:

- Pasirašoma dalis kanonizuojama
- Pasirašomai daliai suformuojamas SignedData MIME elementas naudojant pasirinktą saugos metodą:
    - apskaičiuojama santrauka
    - santrauka pasirašoma siuntėjo privačiuoju raktu
    - pridedamas siuntėjo sertifikatas
- Pasirašoma dalis įterpiama kaip pirmas sudėtinio MIME dokumento elementas
- Parašas užkoduojamas transporto koduote
- Parašas pridedamas kaip application/pkcs7-signature MIME elementas

Šifravimo procesas:

1. Saugomas MIME elementas (turinys) kanonizuojamas
2. MIME elementas ir kiti reikiami duomenys užšifruojami gaunant EnvelopedData elementą:
    1. Sugeneruojamas atsitiktinis simetrinis sesijos raktas. Jis užšifruojamas kiekvieno gavėjo viešuoju raktu
    2. Turinys užšifruojamas simetriniu sesijos raktu
    3. Užšifruotas turinys papildomas sesijos raktu
3. Į pranešima įtraukiamas tinkamai užkoduotas vienas MIME elementas

7.2 SSL/TLS protokole naudojami saugos algoritmai, simetrinių raktų generavimo metodai

RSA, DH, AES-128 CBC, SHA

7.3 SSL/TLS kliento ir serverio autentifikavimo būdai: ką reiškia užrašas TLS_RSA_WITH_AES_128_CBC_SHA naudojant SSL/TLS

Tai šifravimo rinkinys, kuris nurodo kokie algoritmai bus naudojami

7.4 Ipsec protokolai: AH (Authentication Header) ESP(Encapsulating Security Payload)

Ipsec:

- Apsaugo IP tinklais perduodamas datagramas tinklo lygyje (žemiau transporto lygio)
- Labai sudėtingas protokolas:
  - Sudarytas iš labai daug sudedamųjų dalių
  - Turi daug skirtingų nustatymų
  - Gali veikti net keturiais skirtingais režimais
- Užtikrina perduodamų duomenų autentiškumą, konfidencialumą ir vientisumą

Protokolai:

- AH (Authentication Header):
  - Autentifikuoja perduodamus duomenis
  - Užtikrina perduodamų duomenų vientisumą
- ESP (Encapsulating Security Payload):
  - Užtikrina duomenų konfidencialumą (šifruoja)
  - Autentifikuoja duomenis
  - Užtikrina duomenų vientisumą
- Dažniausiai naudojami atskirai ir nepriklausomai

7.5 Ipsec režimai: Tunelio ir Transporto

Ipsec režimai: Tunelio ir Transporto:

- Tunelio – pilnai apgubia IP datagramas (net ir adresus) sukurdamas virtualų saugų pilnų IP datagramų pernešimo tunelį
- Transporto – užtikrina saugų (AH arba ESP) duomenų perdavimą, nes apgaubia tik IP datagramų duomenis

8 Imonių vidinių tinklų saugos priemonės

8.1 Populiarausios įmonės IT infrastruktūros atakos: Dos, DDos, Sniffing, Phishing

Atakos:

- Dos (denial of service) – atakos metu serveris užtvindomas daugybe IP paketų, dėl padidėjusio užklausų kiekio serveriai tampa neprieinami, nes nespėja aptarnauti užklausų
- Ddos (paskirstytas paslaugos blokavimas) – paslaugos blokavimo ataka glai būti efektyvesnė, jei serverį atakuoja daugybė kompiuterių. Organizuojami tinklai panaudojant Trojos arklius ir kitas piktavališkas programas

- Sniffing – naudojant programinę įrangą atliekamas duomenų perduodamų tinklais stebėjimas ir analizė
- Phishing (slaptažodžių žvejojimas) – siekiame išgaauti prisijungimus prie sistemų ar kitus konfidencialius duomenis. Gali būti naudojama socialinė inžinerija

8.2 Imonės tinklo atakos ir rizikos zonos, ugniasienių tipai (strategijos)

Rizikos zonos:

- Įmonės vietinį tinklą prijungus prie Interneto visas vietinis tinklas tampa (potencialios) atakos objektu (rizikos zona)

Ugniasienių tipai – tai programinė ar techikinė sistema, skirta užkirsti kelią neautorizuotam priėjimui prie saugomo tinklo. Naudojamas strategijos:

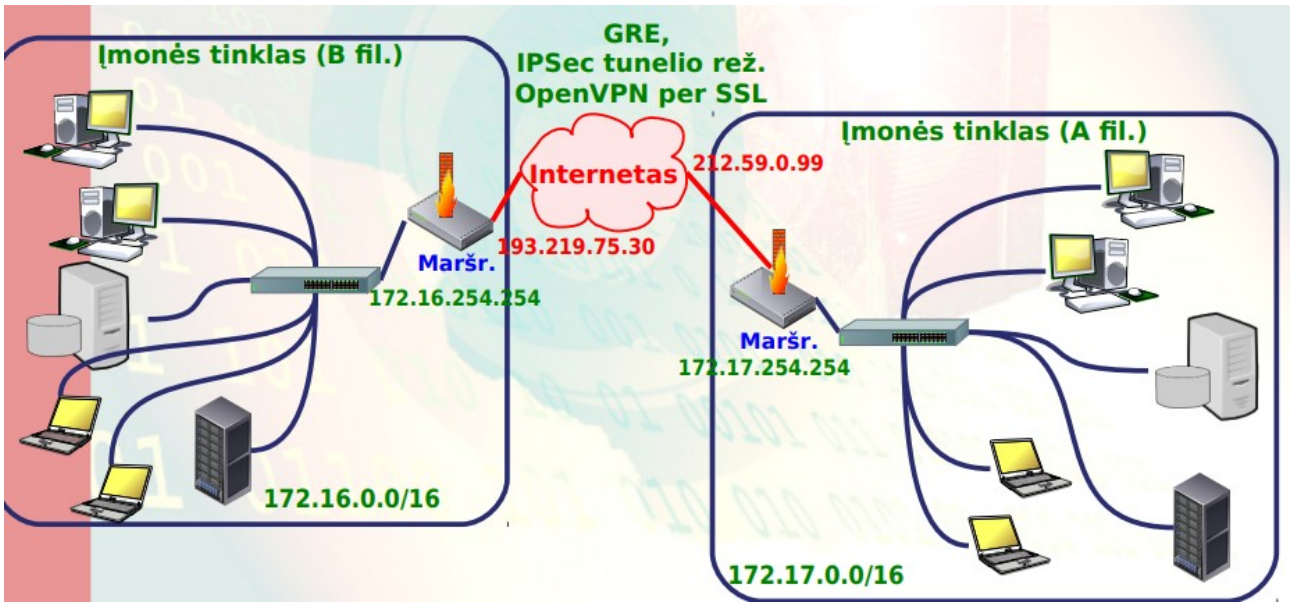
- Ribojanti – tai kas nėra deklaruota kaip lestina yra draudžiama (Deny All)
- Leidžianti – tai kas nėra deklaruota kaip draudžiama yra leistina (Allow All)

8.3 Imonės demilitarizuota zona, DMS poreikis ir vieta įmonės tinklo architektūroje

Demilitarizuota zona (DMZ) tai spec. įmonės vietinis tinklas prijungtas prie Interneto per mažai apsaugotą ugniasienės tinklo sąsają

DMZ poreikis – padeda apsaugoti vidines sistemas nuo nelegalių vartotojų, kurie gali bandyti prieiti prie vidinio tinklo iš demilitarizuotos zonos

8.4 Įmonės virtualūs privatūs tinklai



8.5 Įsilaužimų aptikimo ir išvengimo sistemos

- Pagrindinis tikslas – galimų incidentų aptikimas ir pagalba incidentų tyrimo metu:
  - atpažįsta potencialiai pavojingą veiklą
  - veda potencialiai pavojingų įvykių žurnalą
  - praneša apie įvykius
  - gali imtis atsakomųjų veiksmų
- Gali padėti įgyvendinti įmonės saugos politiką:
  - Sekti ar darbuotojai neatlieka uždrastų veiklų
- Įmonės saugos politikos spragų aptikimas
- Grėsmių dokumentavimas

8.6 Tinklinės įsilaužimų aptikimo sistemos, įsilaužimų įvykių atpažinimo tikslumas, IDS vieta įmonės tinklo struktūroje

Tinklinės įsilaužimų aptikimų sistemos – prijungtos prie vietinio tinklo nuolat analizuoja tinklo duomenų paketų turinį:

- TCP, UDP ir ICMP protokolų paketų lengvai susekami

8.7 SNORT architektūra ir pagrindinės funkcijos, SNORT taisyklių naudojimas ir galimybės

SNORT architektūra ir pagrindinės funkcijos:

- paketų dešifratorius – surenka paketus iš įvairių tinklo sąsajų ir paruošia apdorojimui
- preprocesorius – modifikuoja paketus prieš juos perduodant aptikimo moduliui
- aptikimo modulis – sprendžia ar paketas yra keliantis grėsmę
- žurnalų ir pranešimų sistema – daro įrašus žurnale ir generuoja pranešimus

SNORT taisyklių naudojimas ir galimybės:

- susidaro iš antraštės ir kūno
- gali nurodyti kas turi būti daroma su paketu jei jis pagaunamas
- gali nurodyti tiksliai kokius paketus gaudyti

9 Kompiuterių ir OS sauga

9.1 CIA – konfidencialumas, vientisumas, pasiekiamumas

Rizikos:

- Konfidencialių duomenų atskleidimas:
  - tyčinis pavogimas, raktų atskleidimas

    - darbuotojas netyčia pasiuntė el. Paštu, padėjo į DropBox
- Duomenų praradimas (vientisumo praradimas):
    - sugedo diskas
    - pavogė nešiojamąjį kompiuterį
- Neprieinamumas (sistemos neveikimas):
    - Dingo elektra
    - Sugedo maitimimo šaltinis, diskas, procesorius
    - Potvynis, gaisras

9.2 AAA – autentifikavimo, autorizavimo ir audito užtikrinimo priemonės šiuolaikinėse OS: pagal ką galima autentifikuoti vartotoją? Kas yra daugiafaktorinis autentifikavimas?; UNIX slaptažodžiai, *etc/*passwrd ir *etc/*group; Prieigos teisių valdymo modeliai DAC, mAC, RBAC; Prieigos teisių valdymas POSIX ir Windows; Auditas Windows ir Linux OS

Pagal ką galima autentifikuoti vartotoją?

- Tai ką vartotojas žino:
    - Slaptažodis
    - PIN kodas
- Tai ką vartotojas turi:
    - Išmaniąją kortelę
    - RSA token
    - Slaptažodžių kortelę
- Tai kas vartotojas yra:
    - Piršto antspaudas
    - Akies rainelė
    - Balsas

Daugiafaktorinis autentifikavimas:

- autentifikuojama naudojant kelias skirtingas klases
- bankomate, banko žiniatinklio sistemoje (Smart ID)

Šiuolaikinėse OS dažniausiai leidžia autentifikuoti pagal tai ką vartotojas žino

/etc/passwd – UID, GID, Vardas, Namų direktorija, Shell’as

/etc/group – Grupės slaptažodis, GID, vartotojų sąrašas

Prieigos teisių valdymo modeliai:

- DAC – kiekvienam ištekliui sukuriama ir palaikoma prieigos teisių lentelė
- RBAC (Role based access control) – teisės priklauso nuo vartotojo rolės (grupės)
- MAC (Mandatory Access Control) – subjektai ir objektai priklauso saugos kategorijoms. Naudojamas USA top secret, secret, confidential, unclassified. Subjektas nieko keisti negali

Auditas Windows:

- Audito žurnalus gali vesti tiek OS, tiek pati programa (Apache, DBVS ir pan.)
  - programa gali naudoti OS auditavimo funkcijas (syslogd)
  - arba kurti savo nepriklausomą žurnalą
- Windows naudoja paslaugą EventLog

Unix auditas:

- Naudoja standartinę OS paslaugą syslogd. Visi įvykiai saugomi tekstiniame faile
- Į syslogd galima siųsti duomenis ir iš nutolusio kompiuterio
- Paprastai audito failai saugomi /*var*/log auditorijoje

Prieigos teisių valdymas POSIX ir Windows:

- POSIX – numatė standartines OS savybes. Tame tarpe ir FS prieigos teisių valdymą

10 OS išteklių sauga

10.1 OS išteklių sauga: Atminties, procesų teisių, failų sistemų sauga; Žurnalinės failų sistemos, failų sistemų kvotos

OS išteklių sauga:

- Atminties:
  - atmintis suskirstoma į specialias struktūras (segmentus) kurioms suteikiami tam tikri atributai ir fizinių adresų ruožas. Pats procesorius seka, kad tai nebūtų pažeista
  - Įvykus pažeidimui, įvyksta pertraukimas, kurį apdoroja OS ir masi atitinkamų veiksmų
- Procesų teisių – procesorius seka, ar vykdomasis procesas turi pakamkamas privilegijas:
  - Atlikti privilegijuotas komandas
  - Atlikti įvedimo-išvedimo komandas
  - Kreptis į kitų procesų atminties segmentus
  - Iškviesti paprogrames tam tikrais adresais
  - Apsaugai naudojami apsaugos žiedai (0-3 lygiai)
- Failų sistemos:
  - daugiausia problemų kyla po trikių duomenų rašymo į diską metu

    - jei failo trinimo metu sistema sutrinka, diske lieka tam tikra vieta pažymėta kaip užimta, nors joks failas iš tikrųjų jos neužima. Norint tokias klaidas ištaisyti, reikia patikrinti viso disko turinį, kas labai ilgai užtrunka

Žurnalinės failų sistemos:

- Naudoja tranzakcijų mechanizmą
- Disko operacijos pirma įrašomos į žurnalą
- Po to tik daromi pakeitimai diske
- Jei viskas sėkmingai įvyksta, ištrinamas įrašas žurnale
- Jei sistema sutrinka, tai persikrovus OS galimi du atvejai:
    - Įrašas į žurnalą nebuvo padarytas iki galo. Tokiu atveju nieko nedaroma
    - Įrašas į žurnalą buvo padarytas, bet nebaigta rašyti į diską. Tokiu atveju pakartojamos visos disko operacijos

FS kvotos – disko naudojimo ribojimai:

- kai kurios FS leidžia apriboti vartotojams ir/ar jų grupėms prieinamą vietą diske
- quotecheck, edquota, setquota
- saugo nuo tyčinio ar netyčinio perpildymo
- labai lėtina FS darbą
- užtikriną diske įrašytų duomenų saugą tik tol kol veikia pati OS

10.2 Duomenų konfidencialumas „už OS ribų”

- Jei konfidencialumo reikia ir be OS, naudojamas duomenų šifravimas
- Disko skirsinio šifravimas
- Failų sistemos lygio šifravimas (visai FS vienas raktas)
- Failo šifravimas

10.3 Kerberos protokolas

- Kerberos – tinklinis autentifikavimo protokolas
- Skirtas užtikrinti vieningą prisijungimą ir prieigą prie skirtingų išteklių įmonės tinkle
- Naudoja simetrinę kriptografiją
- Nesaugiuose tinkluose:
    - Užtikrina serverio ir kliento abipusį autentifikavimą
    - Apsaugo nuo pakartojimo atakų, duomenų nutekėjimo

10.4 LDAP katalogo paslaugos

- Katalojo paslaugos teikia vartotojų autorizavimo paslaugą įmonės tinkle:

    - tai lyg DB kurioje galima centralizuotai užregistruoti visus objektus ir jų atributus
    - Vartotojus, tinklo išteklius

LDAP (Lightweuight Directory Access Protocol)

- protokolas kuris leidžia tinklu kreiptis ir pildyti x.500 standarto katalogą
- pats nesuteikia jokios saugos
- visi pasikeitimai duomenimis vyksta atviru kanalu
- klientų nereikalauja autentifikuotis

11 Fizinių bruožų atpažinimo tenchnologijos

11.1 Fiziologiniai ir elgsenos bruožai

Visos biometrinės technologijas galima suskirstyti į 2 klases:

- Fiziologinės, fizinės – pirštų atspaudų atpažinimas, rankos ir delno geometrijos atpažinimas, akies tinklainės ir akies rainelės nuskaitymas, veido geometrijos atpažinimas
- Elgsenos charakteristikų – apima asmens parašo atpažinimą, balso atpažinimą, klaviatūros naudojimo atpažinimą, eisenos atpažinimą

11.2 Asmens tapatumo patikrinimas ir asmens identifikavimas: jų tarpusavio skirtumai

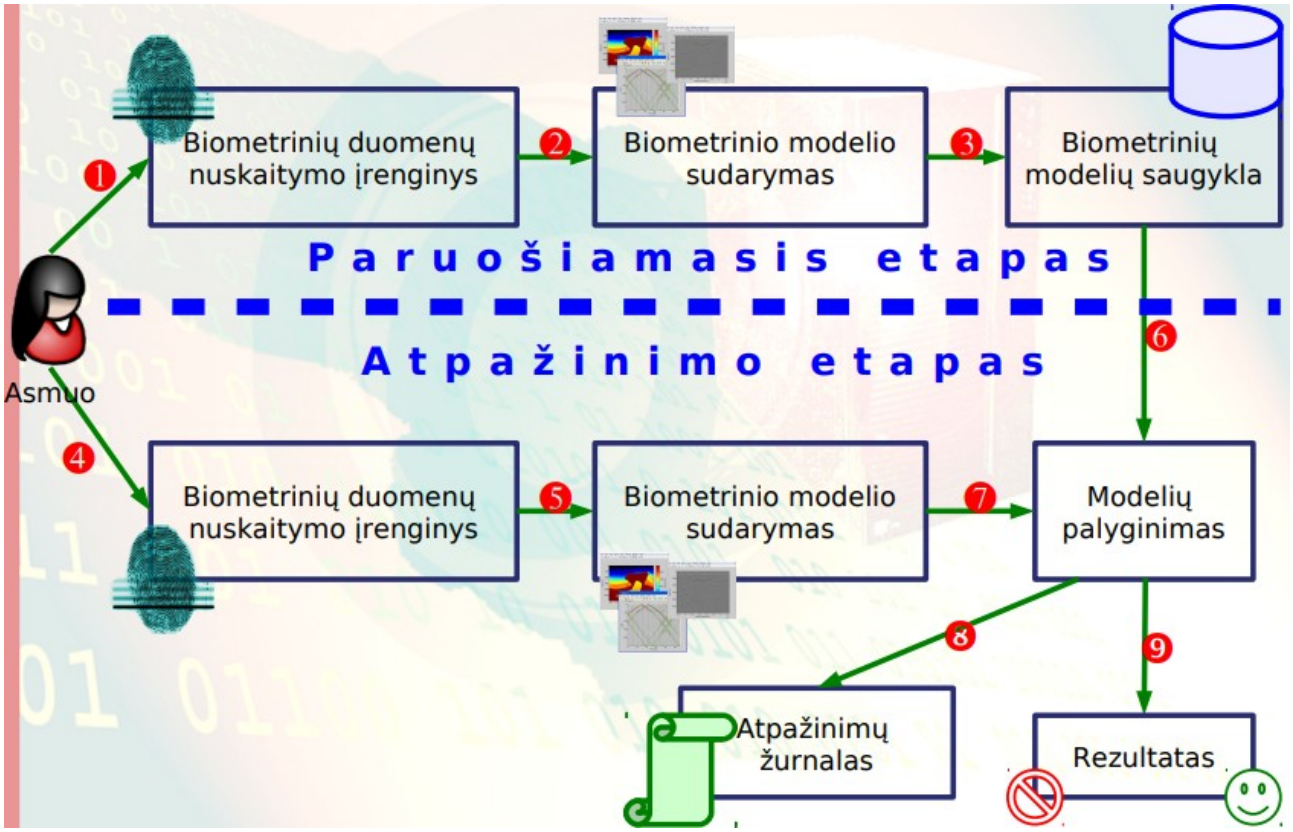
Asmens tapatumo patikrinimas:

- Asmuo deklaruoja savo tapatumą: tabelio nr., ID kodas, prisijungimo vardas
- Po to pateikia savo biometrinę charakteristiką
- Biometrinė sistema palygina dabartinę biometrinę charakteristiką su saugoma duomenų bazėje (atlieka vienas su vienu patikrinimą)

Asmens identifikavimas:

- Asmuo pateikia savo biometrinę charakteristiką
- Sistema patikrina visą aibę turimų kandidatų ir nusprendžia, ar vienas iš jų atitinka identifikuojama asmenį:
    - atlieka vienas su daug paieška
    - reikalauja daug apdorodimo resursų
    - biometrinis modelis turi būti mažas, bet labai tikslus

11.3 Apibendrintas fizinių bruožų atpažinimo procesas



1. Specialiu įrenginiu nuskaitomi biometriniai duomenys
2. Biometriniai duomenys apdorojami, iš jų sudaromas biometrinis modelis
3. naujai gautas biometrinis modelis palyginamas su anskčiau duomenų saugykloje išsaugotu modeliu
4. Apskaičiuojamas abiejų biometrinių modelių atitikimas vienas kitam
5. Žurnale išsaugomas įrašas apie atpažinimo arba neatpažinimo faktą
6. Proceso rezultatas:
    1. Patvirtinta (arba ne) tapatybė
    2. Atpažintas (arba ne) asmuo

11.4 Detales įvertinantys ir koreliaciniai biometriniai metodai

Pirštų atspaudų atpažinimo metodai gali būti suskirstyti į dvi kategorijas:

- detales įvertinantys metodai ant piršto ieško specialių taškų ir vertina jų santykinę padėtį:
    - nepatikimi, kai piršto antspaudas yra labai prastos kokybės
    - taikomi tada, jei nereikia ypatingai didelio tikslumo ir visada galima pakartoti antspaudo nuskaitymą, reikia greito atpažinimo
    - nesaugomas vaizdas, dėl to sunku padirbti antspaudą
- Koreliaciniai metodai lygina naujai gautą piršto atspaudo vaizdą su užregistruotų duomenų bazėje:

    - Tikslesnis, geriau tinka kai pirštų atspaudas nepilnas ar blogos kokybės
    - Mažiau saugūs, galima pavogti, panaudoti kitoje sistemoje

11.5 Biometrinės sistemos našumo rodikliai: FRR – klaidingo atmetimo rodiklis; FAR – klaidingo priėmimo rodiklis

- FRR – klaidingo atmetimo rodiklis. Asmenų, kurie turėtų būti sėkmingai atpažinti, atmetimo tikimybė:
    - Tikimybė neatpažinti teisingo objekto:
        - Nepavojinga saugos požiūriu
        - Sukelia nepatogumus vartotojams
    - Vartotojas privalo pakartotinai pateikti sistemai savo biometrines charakteristikas
- FAR – klaidingo priėmimo rodiklis. Apgaulingo priėmimo tikimybė:
    - Tikimybė neteisingai atpažinti:
        - Pavojinga saugos požiūriu
        - Labiau priimtina vartotojams

11.6 Pagrindinė biometrinių technologijų charakteristikos

- Atsparumas klastojimui – įvertina naudojamo fizinio bruožo atkartojimo (suklastojimo) galimybę
- Naudojimo paprastumas:
    - Žmonėms leidžia atsikratyti įprastinių raktų ryšulių ir būtinybės prisiminti dešimtis prisijungimo vardų bei slaptažodžių
    - Ar lengvai pasinaudoti?
    - Ar reikia išankstinio apmokymo? (Akies tinklainės nuskaitymas)
- Atgrasumas žmonėms:
    - dalis fizinių bruožų atpažinimo sistemų yra labiau atgrasios žmonėms nei kitos
    - pvz. Atpažįstant akies tinklainę, akys apšviečiamos ryškiu spinduliu, o tai žmogui sukelia nemalonių pojūčių
    - balso atpažinimas atrodo visiškai įprastas ir neatgrasus metodas
- Pritaikomumas – kai kurie žmonės gali fiziškai nesugebėti naudotis
- Atpažinimo laikas
- Biometrinio modelio dydis
- Stabilumas laiko požiūriu
- Technologijos užbaigtumas – kai kurios technologijos patikrintos praktiškai

12 Veiklos atnaujinimo programos

12.1 Atsarginių kopijų (backup) darymas: pilnos, papildančios, skirtumų

Atsarginės kopijos:

- Pilnos – visos sisteminės programinės įrangos, taikomųjų programų bei duomenų atsarginės kopijos turėtų būti daromos kas savaitę arba kas mėnesį
- papildančios – saugomi visi pakitimai po paskutinės kopijos
- skirtumų – visi duomenys pakitę po paskutinės pilnos kopijos

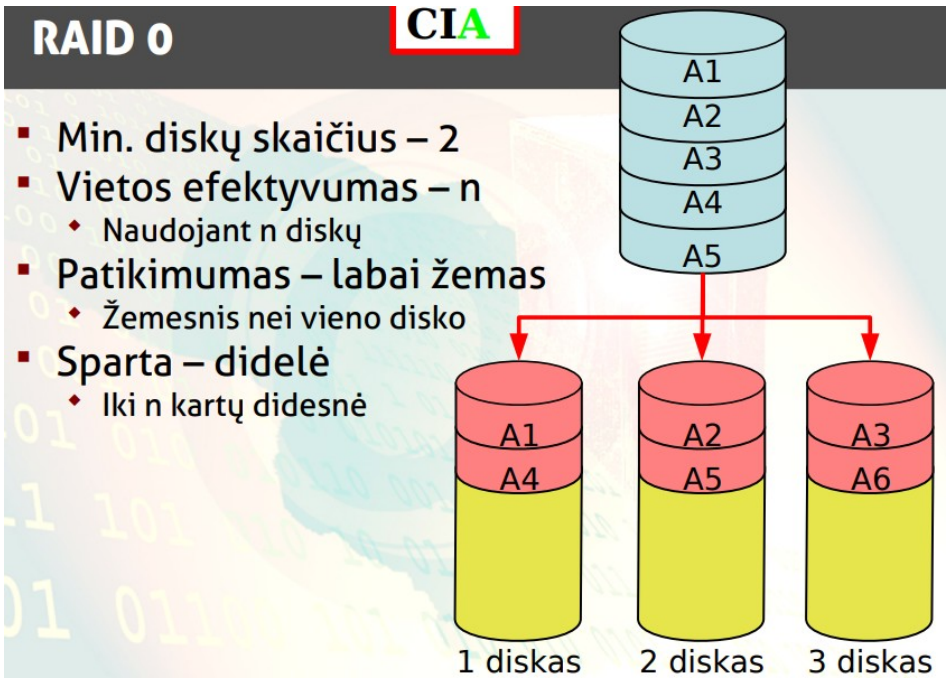
12.2 Alternatyvi įmonės informacijos apdorojimo infrastruktūra: Karšta infrastruktūra; šalta infrastruktūra

VAP (verslo atnaujinimo programa) turėtų numatyti alternatyvią informacijos apdorojimo infrastruktūra, į kurią, įvykus katastrofai, būtų galima perkelti pagrindinį informacijos apdorojimo centrą ir atkurti e. verslo paslaugų tiekimą

Karšta infrastruktūra – visiškai aprūpinta reikiama įranga (apšvietimu, elektros tiekimu, oro kondicionavimo sistema, kompiuterių technine ir programine įrange ir gali pradėti funkcionuoti greičiau nei per 24 valandas). Galima pradėti naudoti labai greitai. Kai stovi nenaudojama įmonei brangiai kainuoja.

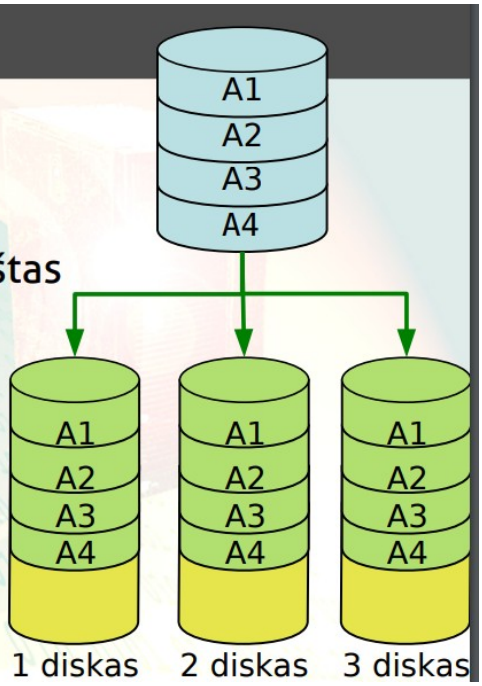
Šalta infrastruktūra – aprūpinta tik pagrindine įrange, būtina norint ekspoluoti informacijos apdorojimo sistemą (apšvietimas, elektra, tiekimo sistema). Jokia kompiuterinė įrange nėra iš anksto perkama. Gali pradėti veikti tik po savaitės arba net kelių.

12.3 RAID technologija



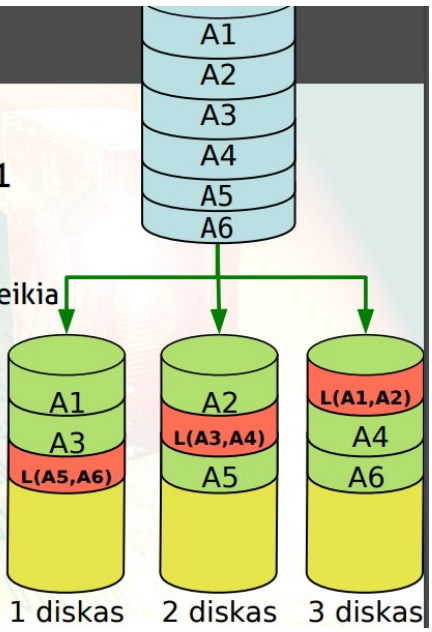
RAID 1

- Min. diskų skaičius – 2
- Vietos efektyvumas – 1
  - Naudojant n diskų
- Patikimumas – labai aukštas
  - Sutrikus n-1 diskui, masyvas veikia
- Sparta – vidutinė



RAID 5

- Min. diskų skaičius – 3
- Vietos efektyvumas – n-1
  - Naudojant n diskų
- Patikimumas – aukštas
  - Sutrikus 1 diskui, masyvas veikia
- Sparta – žema
  - Rašant duomenis reikia skaičiuoti lygiškumo duomenis
- „Karšti" pakaitiniai (Hot spare) diskai



RAID 6

- Min diskų skaičius – 4
- Vietos efektyvumas – n-2
  - Naudojant n diskų
- Patikimumas – aukštas
  - Sutrikus 2 diskams, masyvas veikia
- Sparta – žema
  - Rašant duomenis reikia skaičiuoti lygiškumo duomenis
  - Naudojami du skirtingi algoritmai (P ir Q)