KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Mantas Lenza

E. parašo taikymas autentifikavimui ir šifravimui video paskaitų sistemoje

Magistro darbas

Darbo vadovas
prof. dr. E. Sakalauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Mantas Lenza

E. parašo taikymas autentifikavimui ir šifravimui video paskaitų sistemoje

Magistro darbas

Recenzentas
doc. dr. Jonas Čeponis
2010-05-

Vadovas
prof. dr. E. Sakalauskas
2010-05-

Atliko
IFN-8/3 gr. stud.
Mantas Lenza
2010-05-26

Kaunas, 2010

TURINYS

ĮVADAS

Nuotolinis mokymas šiandien laikomas vienu pažangiausių, perspektyviausių mokymo ir mokymosi būdų. Nuotolinio mokymo ištakomis laikomi 1728 m., kai Kalebas Filipsas (Calebs Phillips) Bostone ėmėsi organizuoti stenografijos mokymus, užduotis savo studentams siųsdamas paštu. Toks mokymosi būdas pasirodė labai priimtinas ir patrauklus, kadangi mokymuisi neliko tokių kliūčių kaip atstumas, laikas, pinigai ir t.t. Būtent tai nulėmė nuotolinio mokymo išlikimą ir netgi sparčią evoliuciją.

Šiuolaikinio nuotolinio mokymo tėvu laikomas Čarlis Vedermėjeris (Charles Wedermeyer) dirbęs Viskonsino universitete (JAV). Jo idėjas apie nuotolinį mokymą panaudojo britai ir 1960 m. įkūrė Britų Nuotolinio mokymo universitetą (British Open University). Čia jau buvo panaudotos tokios technologijos, kaip radijas ir televizija. Vystantis technologijoms, atsiradus kompiuteriams ir sparčiam internetiniam ryšiui ėmė sparčiai steigtis valstybinės ir nevalstybinės nuotolinio mokymo įstaigos, kurios naudodamos pažangiausias technologijas, suteikia galimybę jaustis pilnaverčiu studentu ir lengvai bei patogiai gauti pateikiamą informaciją.

Nuotoliniam mokymui naudojamas technologijas galima suskirstyti į *sinchronines* ir *asinchronines.*

Sinchroninės – telefonai, video konferencijos, internetinės konferencijos. *Asinchroninės* – audio įrašai, el. paštas, forumai, balso paštas, vaizdo įrašai. Žinoma, pažangiausios yra sinchroninės technologijos, kurioms skiriamas didžiausias dėmesys ir susidomėjimas. Be visa ko, siekiant išnaudoti visas šiuolaikinio interneto teikiamas galimybes skatinama nuotolinio mokymo sistemų evoliucija.

Egzistuoja įvairių nuotolinio mokymo sistemų, tačiau nedaugelis jų suteikia galimybę organizuoti realaus laiko paskaitų transliacijas. Video paskaitų sistemos *Elluminate Live* ir *ViPS* leidžia realiu laiku transliuoti vykstančias paskaitas, konferencijas ir kitus renginius, peržiūrėti vaizdo įrašus. Deja, pastarosios sistemos nėra visiškai tobulos, jų pagrindinis trūkumas – nepakankamas pateikiamos informacijos saugumo lygis. Šis trūkumas labiausiai aktualus specialiose mokymo įstaigose, kur pateikiama informacija gali būti su tam tikromis informacijos saugumo žymėmis. Šios problemos sprendimas – naudoti pažangius autentifikavimo ir šifravimo mechanizmus. Dar vienas pastebimas sistemų trūkumas – studentams pateikiama tik tekstinio tipo informacija, dėstytojas neturi galimybės studentams vaizdžiai paaiškinti ar pateikti dėstomos teorinės medžiagos pavyzdžių.

Minėtų problemų sprendimui buvo pasiūlytas ir realizuotas modelis, kuriame sistemos dalyviai prisijungimui naudoja e. parašą, o jų siunčiamos žinutės yra šifruojamos naudojant pažangius kriptografinius algoritmus. Pasiūlytame modelyje dėstytojams

suteikiama galimybė studentams pateikti informaciją ne tik tekstinio tipo, tačiau pateikti dėstomos teorinės medžiagos pavyzdžių. Siūlomas modelis buvo sėkmingai pritaikytas „Audio-Video nuotolinio mokymo ir egzaminavimo sistemoje“ (toliau darbe minima kaip video paskaitų sistema), kurią realizavo magistrantas Paulius Lazauskas.

Bendra sistemos realizacija buvo pristatyta 2010 m. gegužės 4 d. vykusioje Universiteto mokslininkų darbų parodoje-konkurse „Technorama 2010“, kurioje pristatytam darbui skirta pirmoji vieta (žr. priedą Nr. 1).

1

Video paskaitų sistemų autentifikavimo ir informacijos apsaugos problemos analizė

Šiame skyriuje bus nagrinėjamos esamos nuotolinio mokymo bei internetinių konferencijų sistemos, kurios gali būti pritaikomos video paskaitų organizavimui. Pirmiausiai trumpai aptarsime kas yra nuotolinis mokymas ir internetinė konferencija.

Nuotolinis (distancinis) mokymas – žinių (informacijos) pateikimo technologija, kuriai yra būdingas ryšio priemonių naudojimas ir atvirumas vietos, laiko, spartos atžvilgiu. Nuotolinės studijos nėra tapačios įprastinei neakivaizdinei mokymo(si) formai. Jos aprėpia visas mokymo ir mokymosi formas, kai studijuojama neatvykstant į studijų instituciją, o dėstytojo ir studentų bendravimas vyksta ryšio priemonių pagalba. Nuotolinio mokymo būdas gali būti taikomas ir įprastinėse (stacionarinėse arba dieninėse) studijose. Nuotolinis mokymas yra moderni studijų komponentė, nors studijos iš esmės gali vykti tik nuotoliniu būdu.

Internetinė konferencija. Tai patogus būdas pateikti kompiuterinio formato medžiagą keletui ar keliasdešimčiai žmonių. Dažnai tam naudojama telefoninė ar vaizdo konferencija, nors vis dažniau pradedama naudoti internetinę telefoniją. Interneto konferencijai reikalingas kompiuteris ir interneto ryšys. Kompiuterio ekrane rodoma konferencijos metu aptariama informacija. Paprastai vienas iš konferencijos dalyvių turi išskirtinę teisę keisti turinį, jį redaguoti ar pašalinti, tačiau jis tokią teisę gali suteikti, bet kuriam konferencijos dalyviui. Toks konferencijos būdas ypač efektyvus nuotoliniuose mokymuose.[15]

1.1 Egzistuojančios video paskaitų sistemos

Egzistuojančios nuotolinio mokymo sistemos dažniausiai apsiriboja informacijos pateikimu tik standartinėmis tekstinio tipo laikmenomis, vartotojų autentifikavimui dažniausiai naudojamas primityviausias metodas – slaptažodis, o pateikiamos informacijos apsaugai praktiškai nėra taikomi jokie metodai. Šiame skyrelyje trumpai panagrinėsiu keletą nuotolinio mokymo sistemų, kurios savyje turi realizuotą video paskaitų funkciją. Pagrindinį dėmesį analizuojant panašias sistemas skirsiu šiems kriterijams: *naudojimo patogumui*, *paplitimo galimybei*, *vartotojų autentifikavimo*, *informacijos apsaugos užtikrinimui* bei pateikiamos *ekrano vaizdo transliavimui*.

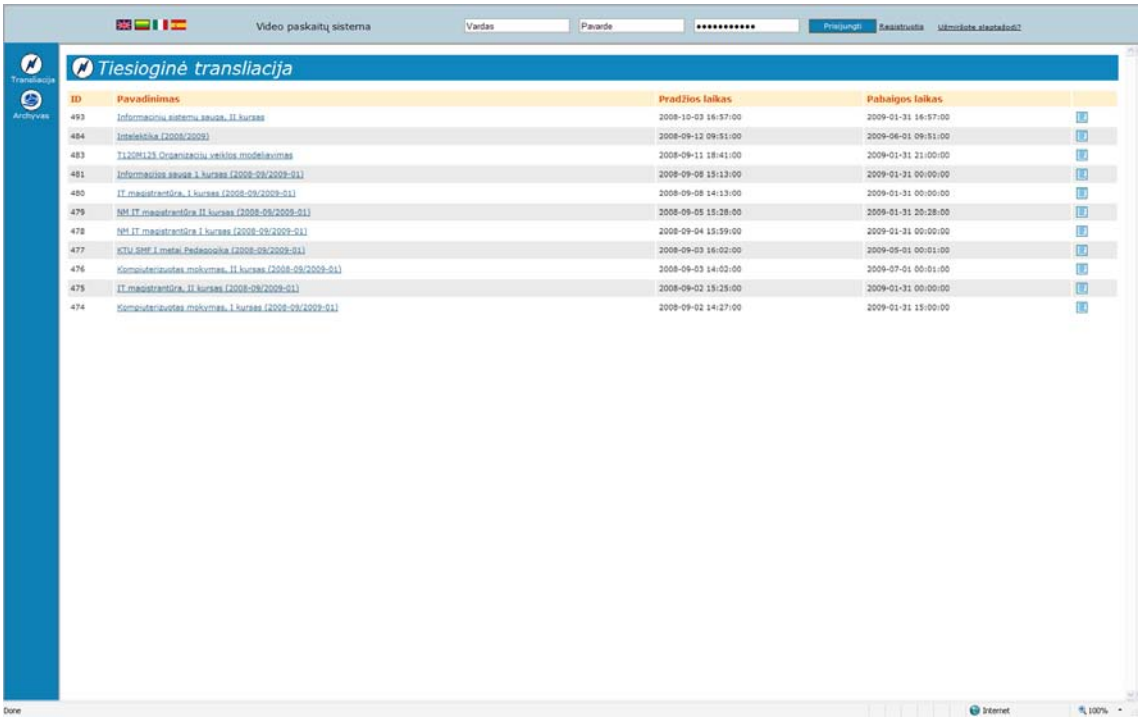
1.1.1 KTU video paskaitų sistema ViPS

KTU Distancinio mokymosi centro (DMC) specialistų sukurta video paskaitų sistema (*ViPS*) (1 pav.) leidžia transliuoti pranešimus ir paskaitas neribotam interneto

vartotojų skaičiui. *ViPS* pagalba dėstytojai skaito paskaitas ne tik KTU, bet ir kitų universitetų studentams.

Pranešėjas, naudodamasis *ViPS* sistemos galimybėmis, gali organizuoti momentines auditorijos apklausas, o pranešimus savo kompiuterio ekrane stebintys interneto vartotojai klausimus gali pateikti žinučių principu. Visi video pranešimai yra įrašomi ir vėliau pasiekiami iš archyvo, o įrašai gali būti redaguojami, koreguojant bei papildant juose demonstruotą vaizdinę medžiagą. Tokios *ViPS* sistemos galimybės išpopuliarino ją universitete, be šios paslaugos jau nebeapsieinama ne tik KTU, bet ir kitų institucijų organizuojamuose renginiuose. Distancinio mokymo centro specialistai nuolat talkina renginių organizatoriams teikdami filmavimo bei transliavimo paslaugas. [3]

Video paskaitų sistemos vienas pagrindinių trūkumų – nepakankamas universalumas, kuris pasireiškia tuo, jog norint peržiūrėti video medžiagą turi būti naudojama Internet Explorer (IE) naršyklė, taip sukeliama daug nepatogumų Linux, Mac OS, Sun OS ir kt. operacinių sistemų vartotojams, kadangi IE naršyklė palaiko tik MS Windows operacinę sistemą. Dėl šios priežasties paplitimo galimybės yra ribojamos. Kitas šios sistemos trūkumas, jog vartotojų autentifikavimas paremtas primityviausiu metodu – slaptažodžiu. Vartotojams pateikiamos informacijos apsauga šioje sistemoje nėra numatyta, todėl galima teigti, jog pateikiama/prieinama informacija gali būti klastojama. Nepaisant tokių trūkumų, video paskaitų sistema patogu naudotis. Joje pateikiama informacija klasifikuojama, o tai palengvina paiešką. *ViPS* nėra realizuota ekrano vaizdo perdavimo galimybė.



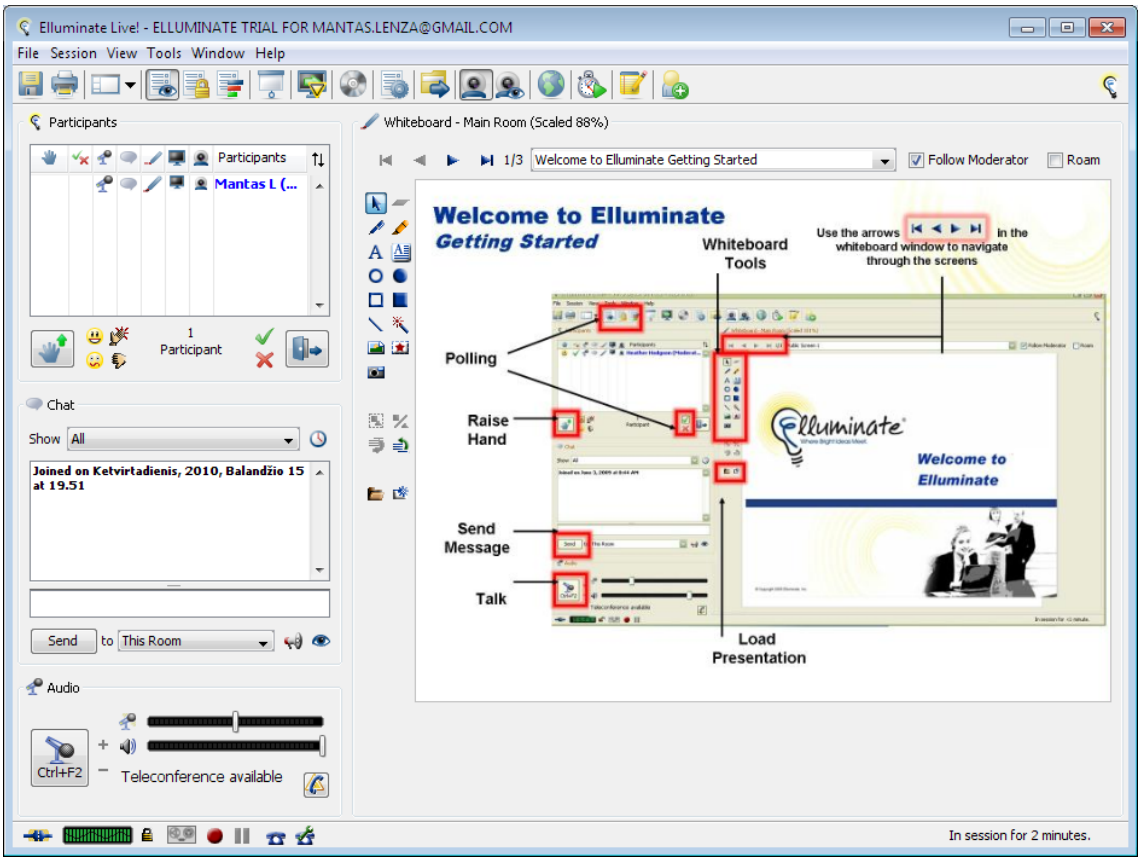
1 pav. Video paskaitų sistemos (ViPS) vartotojo sąsaja

1.1.2 Elluminate Live

Live programinė įranga (2 pav.), sukurta *Elluminate* kompanijos, yra sinchroninio mokymo sprendimas. Savyje šis produktas turi realizuotas tokias savybes:

- tiesioginis susirašinėjimas;
- realaus laiko video transliavimas, kuris žymiai pagerina mokymo kokybę.

Live programinio paketo vienas iš trūkumų, jog reikalingas diegimas į kompiuterį. Nors produkto kūrėjai tikina, jog tai pilnai suderinama su daugeliu operacinių sistemų ir taip dalinai išsprendžia naudojimo paplitimo problemą, tačiau sukeliama papildomų nepatogumų dėl minėto būtino įdiegimo į kompiuterį. Ši sistema pranašesnė už Video paskaitų sistemą tuo, jog pateikiamos informacijos apsaugai gali būti naudojamas SSL protokolas. [4] Vartotojų autentifikavimo problema *Live* išsprendžiama tokiu principu, jog norėdamas rengti konferencijas ar pokalbius, dalyviams reikia išsiųsti atitinkamą nuorodą, kurią jie gauna el. paštu ir atsidarę gautą nuorodą prisijungia prie pokalbio. Vertinant vartotojo pusės valdymą galima sakyti, jog ja naudotis nėra sudėtinga, kadangi visos reikalingiausios funkcijos pasiekiamos iš pagrindinio programos lango. Kaip ir *ViPS*, ši sistema neturi ekrano vaizdo perdavimo galimybės.



2 pav. Elluminate kompanijos Live produktas

1.1.3 See&Share

Tandberg kompanijos sukurto internetinių konferencijų produkto *See&Share* privalumai tokie, jog yra numatyta galimybė keistis kompiuterio ekrano informacija. Vartotojai jungiasi prie serverio, į kurį yra perduodamas vaizdas iš informacijos skleidėjo kompiuterio, arba tiesiogiai prie kompiuterio iš kurio yra pateikiama informacija. *See&Share* sprendimas naudoja 80 prievadą, kurio dėka yra išvengiama užkardų problemų.

Nors programinė įranga prieinama daugeliui operacinių sistemų vartotojų, pagrindinis šio sprendimo trūkumas - būtinas programinės įrangos diegimas į vartotojų kompiuterius, o tai turi įtakos naudojimo paplitimui. Vartotojai autentifikuojami tokiu pat principu kaip ir daugelyje kitų sistemų, t.y. slaptažodžiais, tik šiuo atveju vartotojai dar papildomai turi žinoti tikslų konferenciją transliuojančio serverio adresą. Analizuojant šį produktą nepavyko aptikti kaip apsaugoma informacija jos perdavimo metu. [18]

1.1.4 Egzistuojančių video paskaitų sistemų palyginimas

Šiame skyrelyje aptarsiu, nagrinėtas jau egzistuojančias video paskaitų sistemas pradžioje pasirinktais kriterijais:

- *Patogumas* – vartotojams paprastas ir patogus sistemos valdymas. Patogumas netiesiogiai susijęs su paplitimu.
- *Paplitimas* – sistemos populiarumo vartotojų tarpe matas, kuris priklauso nuo sistemos naudojimui keliamų specifinių reikalavimų: operacinė sistema, papildoma programinė įranga ir kt.
- *Autentifikavimas* – šiuo kriterijumi nurodoma kokie autentifikavimo metodai taikomi arba ką vartotojas turi žinoti iš anksto.
- *Informacijos sauga* – šiuo kriterijumi nurodoma kokia sistemoje įdiegta informacijos, pateikiamos vartotojams, apsauga.
- *Kompiuterio ekrano transliavimas* – sistemos galimybė pateikti ne tik tekstinio tipo informaciją, tačiau realiu laiku koreguoti pateikiamos medžiagos turinį pagal savo poreikius.

1 lentelė. Video paskaitų sistemų palyginimas

Kriterijus	Video paskaitų sistema		
	ViPS	*Elluminate Live*	*See&Share*
Patogumas	Didelis	Vidutinis	Vidutinis
Paplitimas	Didelis	Vidutinis	Vidutinis
Autentifikavimas	Minimalus	Vidutinis	Vidutinis
Informacijos apsauga	Nėra	Vidutinė	Nėra
Kompiuterio ekrano transliavimas	Nėra	Nėra	Yra

Iš pateiktos informacijos 1 lentelėje matome, jog sistemos paplitimui įtakos turi jos naudojimo patogumas ir tai, kokie specifiniai reikalavimai keliami jos vartotojams. *ViPS* sistema pranašesnė *patogumo* ir *paplitimo* kriterijų atžvilgiu už Elluminate Live ir See&Share tuo, kad pakanka standartinės operacinės sistemos konfigūracijos norint ja naudotis, o vienintelis trūkumas – ji nėra universali operacinių sistemų atžvilgiu. Nors Elluminate Live ir See&Share sistemos pritaikytos daugeliui operacinių sistemų, tačiau jų naudojimui būtinas papildomos programinės įrangos diegimas į vartotojo kompiuterį. Visas tris sistemas lyginant pagal *autentifikavimo* kriterijų galima teigti, jog žymiai pranašesnės sistemos nėra. Visų jų autentifikavimas paremtas vartotojų prisijungimo vardo ir slaptažodžio reikalavimu. Šiek tiek tobulesnė sistema yra See&Share, kadangi jos vartotojai turi žinoti ne tik minėtus duomenis, bet papildomai turi žinoti kur jungtis norint dalyvauti tam tikroje konferencijoje. Sistemas nagrinėjant *informacijos apsaugos* kriterijumi, vienareikšmiškai galima išskirti Elluminate Live sistemą, kadangi joje numatyta duomenų apsauga naudojant SSL protokolą. Informacijos apsauga See&Share ir *ViPS* sistemose nenumatyta. Iš nagrinėjus sistemas *kompiuterio ekrano perdavimo* kriterijumi, pastebėjau, kad vienintelė turinti šią savybę yra See&Share sistema, kitose nagrinėjamose sistemose tokios funkcijos nėra.

1.2 Autentifikavimo naudojimas informacijos apsaugai

Autentifikavimas vienas iš svarbiausių informacijos apsaugos būdų. Egzistuoja įvairių autentifikavimo apibūdinimų, apibendrinus keletą iš jų galima teigti, jog:

Autentifikavimas – metodas, leidžiantis identifikuoti tikrąjį informacijos šaltinį. Garantuojama, jog bendravimas bei informacijos mainai vyksta tikrai tarp tų subjektų, kuriais jie save prisistato.

Autentifikavimas realizuojamas įvairiais metodais. Jo pasirinkimą lemia tokie faktoriai kaip saugomos informacijos svarba, naudojimo paprastumas, įsibrovimo sudėtingumas ir kt. Paprasčiausias ir seniausiai egzistuojantis autentifikavimo metodas –

vartotojo vardas ir slaptažodis, vieni iš saugiausių autentifikavimo būdų – biometriniai duomenys ir kriptografiniai metodai (pvz. elektroninis parašas).

1.2.1 Elektroninis parašas

Elektroninio parašo panaudojimas apima ne tik autentifikavimą, bet ir informacijos, pateikiamos su tokiu parašu, autentiškumą bei vientisumą. Technologiniu požiūriu elektroninis parašas tai koduota informacija, kurios dėka elektroninės sistemos vartotojas gali patvirtinti savo tapatybę bet kuriam kitam tos sistemos vartotojui. E. parašo dėka užtikrinamos tokios pateikiamos informacijos ar duomenų savybės, kaip:

- Vientisumas;
- Autentiškumas;
- Nepaneigiamumas;

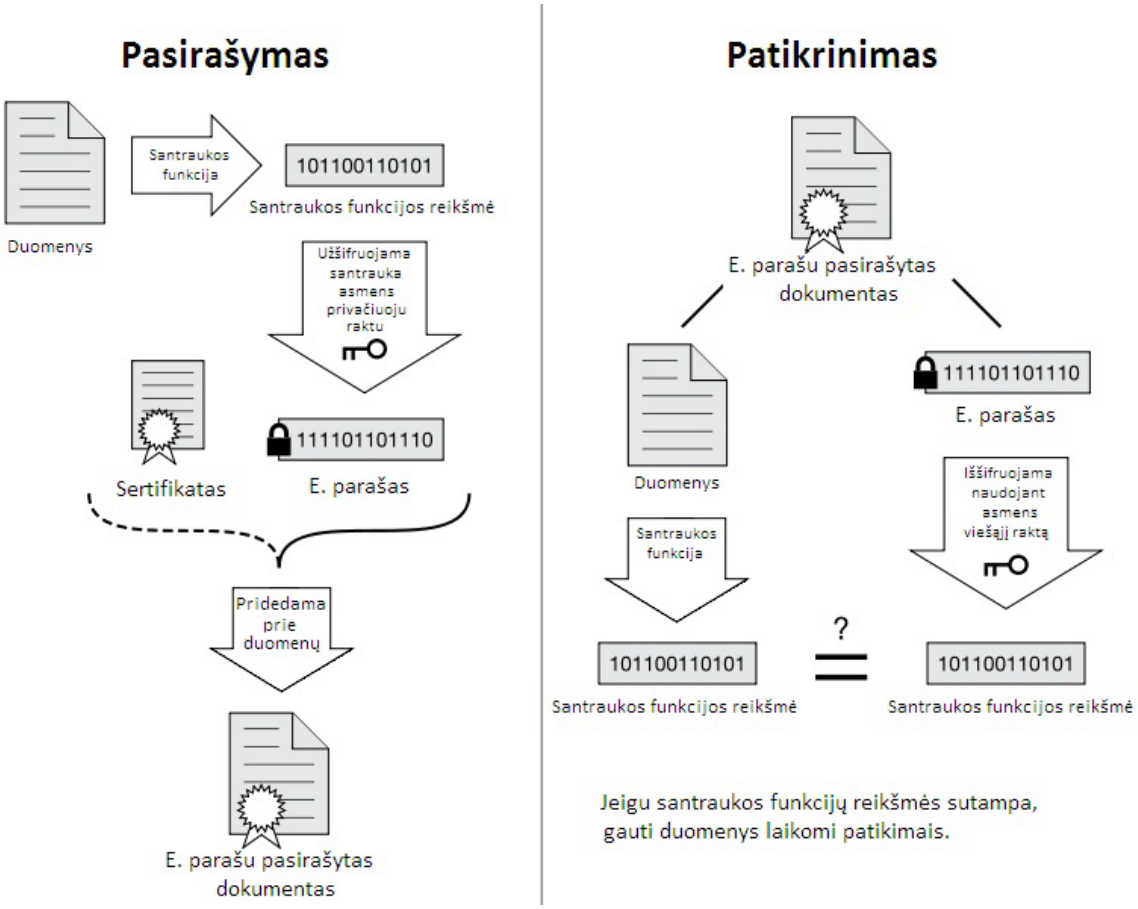
E. parašas yra tradicinio parašo atitikmuo, kuriuo pasirašomi elektroniniai dokumentai. Jo realizavimas remiasi asimetrine kriptografija, panaudojant viešųjų raktų infrastruktūrą. Duomenų vientisumui užtikrinti dažniausiai naudojama santraukos funkcija, autentiškumą garantuoja atitinkamas pasirašiusio asmens viešasis raktas, kuriuo galima patikrinti e. parašą. Pasirašęs asmuo negali išsiginti savo parašo, kadangi jam sudaryti naudojamas privatusis raktas, o tai vadinama - nepaneigiamumo savybe. [11, 13]

E. parašai naudojami duomenų autentiškumui ir vientisumui apsaugoti.

E. parašas – tai reikšmė, apskaičiuota kriptografiniu algoritmu ir pridėta prie duomenų objekto taip, kad kiekvienas norintis galėtų patikrinti duomenų autentiškumą. Pasitelkus atitinkamą viešąjį raktą ir nurodytą algoritmą, galima patikrinti, ar e. parašas galioja, t. y. ar duomenys nebuvo pakeisti. Skiriamos dvi pagrindinės e. parašo klasės:

- *E. parašai su priedais*: e. parašo duomenys pridedami prie duomenų bloko (pranešimo). Šie e. parašai aprašyti ISO/IEC 14888 standarte.
- *E. parašai su pranešimo atkūrimu*: šiuo atveju duomenų blokas kriptografiškai transformuojamas taip, kad jame atsiranda ir pasirašomi duomenys, ir e. parašas. Duomenys atkuriami tik patvirtinus e. parašą. Šie e. parašai aprašyti ISO/IEC 9796 standarte.

E. parašą su pranešimo atkūrimu galima naudoti kaip parašą su priedais. Tokiu atveju reikėtų pasirašyti ne patį pranešimą, o jo santrauką, ir tikrinant būtų lyginamos gauto pranešimo ir atkurta santraukos. E. parašui naudoti turi būti apibrėžti trys algoritmai: viešojo ir privačiojo raktų generavimo, e. parašo formavimo ir parašo tikrinimo (pranešimo atkūrimo) (3 pav.).



3 pav. Pasirašymas naudojant e. parašą ir parašo tikrinimas

Pranešimas t pasirašomas privačiuoju pasirašančiojo raktu PR ir sudaromas e. parašas s. Naudojant e. parašą su priedais, s pridedamas prie pranešimo t. Naudojant e. parašą su pranešimo atkūrimu, siunčiamas tik s. Gautas parašas tikrinamas pasitelkus pasirašiusio asmens viešąjį raktą VR. Jei pranešimas ir (ar) e. parašas nebuvo pakeisti, tikrinimo funkcijos rezultatas bus teigiamas, t. y. pranešimas autentiškas, arba bus gautas pradinis pranešimas t, atsižvelgiant į parašo tipą. [10, 11, 14, 16]

E. parašo naudojimas primena asimetrinį šifravimą, tik čia pranešimas arba jo santrauka užšifruojami privačiuoju raktu, o parašas iššifruojamas (tikrinamas) viešuoju. Kenkėjas, nežinodamas privačiojo rakto, negali sudaryti pranešimo ir jo e. parašo, kuris tenkintų tikrinimo procedūrą. Tokiu būdu taip pat užtikrinamas ir e. parašo nepaneigiamumas (neišsiginamumas). Tinkamą e. parašą galima sudaryti tik žinant privatųjį pasirašančiojo raktą, o jo slaptumą turi laiduoti pats pasirašantis asmuo.

Dokumento pasirašymą ir jo patikrinimą naudojant elektroninį parašą galima suskirstyti į tokius etapus:

1. *Raktų generavimas.* Šiame etape sudaromi du unikalūs matematiškai susiję raktai: privatusis (PR) ir viešasis (VR). Šie raktai gali būti naudojami daug kartų tiek tikrinant (VR), tiek pasirašant (PR).

2. *E. pasirašymas.* Pasirašantis asmuo savo privačiuoju raktu PR apibrėžtu algoritmu pasirašo dokumentą ar pranešimą ir suformuoja e. parašą.
3. *E. parašo tikrinimas.* Tikrintojas su pasirašiusiojo viešuoju raktu VR arba patvirtina e. parašą, arba atkuria iš jo dokumentą ar pranešimą.

Saugus e. parašas:

- Yra vienareikšmiškai susijęs su pasirašančiu asmeniu. E. parašą galima patikrinti tik to asmens viešuoju raktu.
- Leidžia identifikuoti pasirašantį asmenį. Prie e. parašo paprastai pridedamas viešojo rakto sertifikatas. Šis sertifikatas yra patikimas tiek, kiek patikimas jį pasirašęs sertifikavimo centras.
- Yra sukurtas priemonėmis, kurias pasirašantis asmuo gali tvarkyti savo valia. Pasirašantis asmuo turi būti garantuotas, kad pasirašo tikrai tai, ką mato. Pavyzdžiui, kenkėjas gali mėginti pakeisti programinę įrangą, kad būtų pasirašoma ir e. parašas tikrinamas tik su dokumento dalimi, o likusi dalis galėtų būti laisvai keičiama, nedarant įtakos e. parašo reikšmei.
- Yra susijęs su pasirašytais duomenimis, kad bet koks šių duomenų pakeitimas būtų pastebėtas. Naudojant kriptografines transformacijas, privačiuoju raktu pasirašomi arba patys duomenys, arba jų santrauka. Pakeitus bent vieną duomenų bitą, e. parašo tikrinimo algoritmas turėtų pranešti, kad parašas negalioja.

E. parašo teisinį statusą reglamentuoja ir Lietuvos Respublikos teisės aktai. LR elektroninio parašo įstatyme elektroninis parašas apibrėžiamas taip: „*Tai duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti*“. Teisinę galią turinčiam e. parašui užtikrinti e. dokumentų valdymo sistemoje turi būti:

- Priemonės, kuriomis galima įdiegti e. parašo technologiją: viešųjų raktų infrastruktūra, pasirašymo ir tikrinimo algoritmai, e. parašo formavimo programinė įranga.
- E. parašo tikrinimo priemonės: programinė įranga, leidžianti pasirašiusio asmens viešuoju raktu patikrinti e. parašą.
- E. parašo ir su jo naudojimu susijusios informacijos ilgalaikio saugojimo priemonės: dokumentų naudojimo ir saugojimo taisyklės, techninės priemonės.

RSA E. parašo schema

RSA e. parašo sistemoje raktų pora generuojama analogiškai kaip ir asimetrinio šifravimo sistemose. Raktų generavimo algoritmui pateikiamas saugumo parametras, kurį atitinka RSA modulio ilgis bitais. Algoritmo rezultatas yra raktų pora.

Raktų generavimą sudaro du žingsniai:

- Atsitiktinai generuojami du maždaug vienodo dydžio pirminiai skaičiai p ir q[4]. Apskaičiuojamas RSA modulis $n = p \cdot q$ (jo ilgį apibrėžia saugumo parametras) ir $\varphi = (p - 1)(q - 1)$. Šiuo metu rekomenduojama naudoti bent 2048 bitų ilgio RSA modulį, t. y. skaičių, kurį sudaro apytiksliai 600 skaitmenų. Todėl generuojami pirminiai skaičiai turėtų būti bent 2048 bitų ilgio.
- Atsitiktinai pasirenkamas toks e, $1 < e < \varphi$, kad e ir φ bendrasis didžiausias daliklis būtų lygus 1, ir randamas toks d, kad $e \cdot d = 1 \pmod{\varphi}$, t. y. e ir d sandaugos, padalytos iš φ, liekana yra lygi 1[5].

Remiantis gautais parametrais, viešasis raktas VR = (n, e), privatusis PR = d.

Parašui formuoti RSA sistemoje pranešimas atvaizduojamas į sveikąjį skaičių. Todėl norint naudoti e. parašo sistemą su pranešimo atkūrimu, pranešimai turi būti pakankamai trumpi. E. parašo sistemoje su priedais naudojamos santraukos funkcijos, o jų rezultatai atvaizduojami į sveikuosius skaičius. Pagrindinė RSA e. parašo idėja – pranešimo t kėlimas laipsniu privačiuoju raktu moduliu n (sistema su pranešimo atkūrimu):

$$s = t^d \pmod{n}.$$

Šis algoritmas yra paprastas ir efektyvus, jį vykdant tik keliama laipsniu moduliu n. E. parašo sistemoje su priedais numatyti du žingsniai:

- Apskaičiuojama dokumento santraukos funkcija H(t) ir H(t) atvaizduojama į sveikąjį skaičių, kuris yra maždaug modulio n eilės.
- Apskaičiuojamas parašas

$$s = \mathrm{H}(t)^d \pmod{n}.$$

Santraukos atvaizdavimo į sveikąjį skaičių algoritmai yra pateikti PKCS #1 standarte. Taip pat galima naudoti ir kitus algoritmus, kurių vienas paprasčiausių – prie gautos santraukos iš dešinės pridėti tiek 0, kad jos eilė atitiktų n.

Parašo tikrinimas sistemoje su priedais:

- Pasitelkus viešąjį raktą, apskaičiuojamas $t' = s^e \pmod{n}$.
- Gautas rezultatas palyginamas arba su pranešimu t, arba su jo santrauka H(t). Parašas galioja tada ir tik tada, kai $t' = t$ arba $t' = H(t)$6.

Sistemoje su pranešimo atkūrimu parašo tikrinimo algoritmas arba atkuria pranešimą, arba pateikia pranešimą, kad gautas parašas s negalioja su duotais (n, e). Pranešimo atkūrimo algoritmą sudaro du žingsniai:

- Pasitelkus viešąjį raktą, apskaičiuojamas $t = s^e \pmod{n}$.
- Nustatoma, ar gautas pranešimas t yra tinkamas. Jei taip, grąžinamas pranešimas t, priešingu atveju pranešama, kad parašas negalioja.

Antrasis žingsnis yra labai svarbus, mat bet kuris derinys gali būti tinkamas pranešimas. Tokiu atveju kenkėjui išlieka galimybė trivialiai parinkti suklastotą parašą, siekiant gauti norimą pranešimą ($t = s^e \pmod{n}$). Dėl šios priežasties paprastai nerekomenduojama naudoti RSA e. parašo sistemos su pranešimo atkūrimu. Ją vis dėlto pasirinkus, būtina imtis papildomų saugumo priemonių, kurios užtikrintų, kad tikimybė, jog atsitiktinai parinktas pranešimas bus prasmingas, būtų nedidelė. Vienas iš būdų tai padaryti – fiksuoti tam tikrą pranešimo struktūrą. [10, 11, 14, 16]

1.2.2 Biometriniai duomenys

Biometriniai duomenys vienu metu ir identifikuoja, ir autentifikuoja žmogų, kitaip tariant padeda atsakyti į klausimą „*kas aš esu*“. Biometrinių duomenų naudojimas nėra labai paplitęs, kadangi jo įdiegimas į bet kurią informacinę sistemą pakankamai brangus bei vartotojams sukelia nepatogumų naudojantis. Nepaisant šių „trūkumų“, ateityje informacinėse sistemose jų diegimas bus vis didesnis. Biometrinės priemonės leidžia atsisakyti: [16]

- **slaptažodžių** – *nereikia jų atsiminti*;
- **leidimų** – *nereikia nešiotis su savimi arba laikyti saugioje vietoje*.

Šiuo metu egzistuojančios biometrinės sistemos gali atpažinti pagal tokias fiziologines charakteristikas: [2, 20]

- pirštų atspaudai;
- delnų atspaudai;
- delno ir rankos plaštakos geometrija;
- akies tinklainės nuskaitymas;
- akies rainelės nuskaitymas;
- parašo dinamiškumo nustatymas;
- teksto rinkimo klaviatūra dinamiškumo nustatymas;
- balso atpažinimas;
- DNR testas.

Visas šias technologijas galima palyginti pagal tokius kriterijus:

- *Tikslumas*. Vienas svarbiausių kriterijų lyginant biometrinių technologijų priemones. Juo pažiūrima kiek sistema suklysta tikrojo vartotojo atveju, jo neįsileisdama, ir kokia tikimybė patekti į sistemą, neesant jos vartotoju.
- *Patogumas naudoti*. Lyginant biometrinių priemonių naudojimą pagal šį kriterijų didelis dėmesys atkreipiamas kaip greitai ją įsisavina vartotojas. Pavyzdžiui, akies tinklainės nuskaitymo priemonė vartotojui be papildomų apmokymų gali būti „neįveikiama“ kliūtis nors jis ir bus tikrasis vartotojas. Kita vertus veido, pirštų, rankos ar delno geometrijos nuskaitymo metodus vartotojams naudoti nesukelia papildomų sunkumų.
- *Kaina*. Šiuo atveju turima omenyje prietaiso, kurio dėka tikrinama, kaina.
- *Kiti veiksniai*.

2 lentelė. Biometrinių duomenų palyginimas

Biometrinė priemonė		Tikslumas	Patogumas naudoti	Kaina
FIZINĖS	Veido geometrija	Vidutinis	Vidutinis	Maža
	Pirštų antspaudas	Aukštas	Aukštas	Maža
	Delno ir rankos geometrija	Vidutinis	Aukštas	Vidutinė
	Akies rainelės nuskaitymas	Aukštas	Vidutinis	Didelė
	Akies tinklainės nuskaitymas	Aukštas	Žemas	Didelė
	DNR testas	Aukštas	Žemas	Didelė
ELGESIO	Klaviatūrinis parašas	Labai žemas	Aukštas	Maža
	Parašas	Žemas	Aukštas	Vidutinė
	Balso atpažinimas	Žemas	Aukštas	Maža

Nagrinėjant biometrines priemones aktualiausias yra patogumo kriterijus, kadangi nuo jo priklauso ir pačios technologijos paplitimas. Tuo pačiu reikia ypatingai svarbų dėmesį skirti ir biometrinės priemonės tikslumui. Pagal tai kokia informacija prieinama sistemoje turi būti parenkamas ir biometrinės priemonės tikslumas. Kaina aktuali priklausomai nuo to kaip plačiai bus naudojama ta biometrinė priemonė.

Panagrinėjus pateiktą 2 lentelę galima sakyti, jog iš biometrinių priemonių priimtiniausia yra pirštų antspaudo biometrinė priemonė, kadangi yra aukštas naudojimo patogumas, kuris pasireiškia tuo, jog vartotojui nereikia specialių žinių norint juo naudotis. Be to, didžiojoje dalyje vidutinės klasės nešiojamų kompiuterių yra standartiškai įmontuotas pirštų antspaudo skaitytuvas. Kitas svarbus šios biometrinės priemonės pranašumas, jog aukštas tikslumo lygis suteikiamas už priimtiną kainą.

1.2.3 Autentifikavimo e. parašu ir biometriniais duomenimis palyginimas

Šiuolaikinėse sistemose pagrindinis dėmesys skiriamas informacijos apsaugai, kuri susideda iš jos šifravimo ir sistemos vartotojų apsaugos. Sistemos vartotojų apsauga nepakankamai užtikrinama naudojant vartotojų vardus ir slaptažodžius. Minėto metodo trūkumui šalinti galima pasirinkti e. parašo ar biometrinių duomenų autentifikavimo metodus. Jie sparčiai diegiami kuriamose ir jau veikiančiose sistemose, kadangi informacijos nutekėjimas verslo sektoriuje finansine prasme gali turėti labai skaudžių pasekmių. Išskirti vieno ar kito autentifikavimo metodo pranašumą yra pakankamai sudėtinga. Biometrinių duomenų privalumas – duomenų atsparumas vagystei, lyginant su e. parašu, kurį būtina saugoti laikmenoje. Verta atkreipti dėmesį į tai, jog e. parašas visada veikia užtikrintai ko negalima pasakyti apie kai kurių tipų biometrinius duomenis. Dažniausiai sutinkamas biometrinių duomenų naudojimas fizinėje apsaugoje, tuo tarpu e. parašas taikomas – programinės įrangos apsaugai.

1.3 Šifravimo naudojimas informacijos apsaugai

Norint apsaugoti ypatingai svarbius duomenis ar informaciją vien vartotojų autentifikavimo nepakanka, tam papildomai sistemose naudojami įvairūs kriptografiniai algoritmai, kurių dėka informacija perdavimo metu yra šifruojama. Pagal naudojamų raktų skaičių šifrai skirstomi į (3 lentelė):

- *Simetrinius*. Duomenų šifravimui ir iššifravimui naudojamas slaptasis raktas. Šiam tipui priskiriami blokiniai ir srautiniai šifrai. Blokinis šifras nuo srautinio skiriasi tuo, jog pastarasis informacijos užšifravimui dar papildomai naudoja vidines būsenas. Blokiniais šifrais užšifruojami dideli fiksuoto ilgio duomenų blokai, o srautiniais – dažniausiai vieno bito ar vieno baito dydžio blokai.
- *Asimetrinius,* kitaip dar vadinamus *viešojo rakto*. Šio tipo šifrai duomenų užšifravimui naudoja viešąjį raktą, o iššifravimui – slaptą privatųjį raktą.

3 lentelė. Simetrinių ir asimetrinių šifravimo sistemų palyginimas

	Privalumai	Trūkumai
	1	2
Simetrinės sistemos	• Simetrinio šifravimo algoritmai veikia itin sparčiai. Tam tikrais atvejais šifravimo sparta gali siekti šimtus megabitų per sekundę. • Naudojami raktai yra 4–5 kartus trumpesni nei asimetrinėse sistemose • Simetrinio šifravimo algoritmo pagrindu gali būti sudaromi kriptografiniai algoritmai	• Simetrinis raktas turi likti slaptas. Jį turi žinoti tik bendraujančios šalys • Egzistuoja raktų apsikeitimo ir saugojimo problema • Dideliame tinkle reikia saugoti daug raktų porų. Raktų skaičius priklauso nuo šalių skaičiaus kvadrato • Kriptografinė praktika rodo, jog raktas tarp dviejų šalių turi būti dažnai keičiamas, galbūt net kiekvieno ryšio seanso metu
Asimetrinės sistemos	• Tik privatusis raktas turi būti slaptas, tačiau turi būti užtikrintas viešojo rakto autentiškumas • Tinkle administruojant raktus, turi dalyvauti patikima trečioji šalis. Ji turi būti sąžininga visų vartotojų atžvilgiu, tačiau negali turėti prieigos nei prie vartotojų slaptųjų raktų, nei prie slaptos informacijos • Atsižvelgiant į naudojimo būdą, viešojo ir privačiojo raktų pora gali būti nekeičiama pakankamai ilgai, t. y. raktų pora skirta daugkartiniam naudojimui • Daugelis viešojo rakto algoritmų tinka efektyviems e. parašo algoritmams sudaryti • Kai kurie asimetriniai algoritmai (pvz., RSA) pasižymi viena savybe: vienas iš dviejų raktų gali būti naudojamas užšifruoti, kitas – iššifruoti	• Populiariausių viešojo rakto algoritmų šifravimo sparta yra kelis šimtus kartų mažesnė nei labiausiai paplitusių simetrinio rakto sistemų • Raktų ilgis yra gerokai didesnis nei simetrinio šifravimo sistemose, siekiant užtikrinti tokį pat saugumo lygį

Patikima trečioji šalis (angl. trusted third party) atlieka raktų generavimo ir paskirstymo funkcijas, taip išsprendžiama raktų paskirstymo problema, tačiau jai yra žinomi visų subjektų slaptieji raktai ir tuo pačiu ji turi prieigą prie slaptos informacijos. Dėl šios priežasties tokia sistema reikalauja besąlygiško pasitikėjimo ja. [8, 9, 17]

Apibendrinant 3 lentelėje pateiktą informaciją apie asimetrines ir simetrines kriptografines sistemas galima sakyti, jog vienokios ar kitokios kriptografines sistemos naudojimas priklauso kam ji bus naudojama. Kuomet reikalingas greitas informacijos šifravimas vienareikšmiškai turi būti naudojama simetrinė kriptografinė sistema. Asimetrinės kriptografinės sistemos pagrindinis privalumas, jog informacija šifruojama vienu raktu kuris laikomas paslaptyje, o iššifruojama su kitu raktu kuris prieinamas visiems.

1.3.1 AES simetrinis šifravimo algoritmas

Pats populiariausias ir dažniausiai naudojamas simetrinio šifravimo algoritmas AES (angl. Advanced Encryption Standard - Pažangus šifravimo standartas). Tai JAV vyriausybės priimtas šifravimo standartas. Šis algoritmas greitas tiek programinės, tiek techninės įrangos atžvilgiu, gana lengvai įgyvendinamas ir reikalauja nedaug atminties. Standartas siūlo tris blokinius šifrus: AES-128, AES-192 ir AES-256. Kiekvieną AES šifro bloko dydį sudaro 128 bitai, su raktais, kurie gali būti 128, 192 ir 256 bitų. Darant prielaidą, kad vienas baitas lygus 8 bitai, fiksuoto bloko dydis 128 bitai yra $128 \div 8 = 16$ baitų. AES veikia 4×4 baitų matrica, vadinama būsena. Dauguma AES skaičiavimų atliekami specialioje galutinėje srityje. [10, 14, 17]

AES šifre nurodytas pertvarkos pakartojimų raundų skaičius, kurio reikia norint paversti paprastą įvesties tekstą į galutinį šifruotą tekstą. Kiekvienas raundas sudarytas iš keleto pertvarkymo veiksmų, įskaitant tokį, kuris priklauso nuo šifravimo rakto. Atvirkštiniai raundų veiksmai yra taikomi norint konvertuoti šifruotą tekstą atgal į originalų paprastą tekstą. [5, 6]

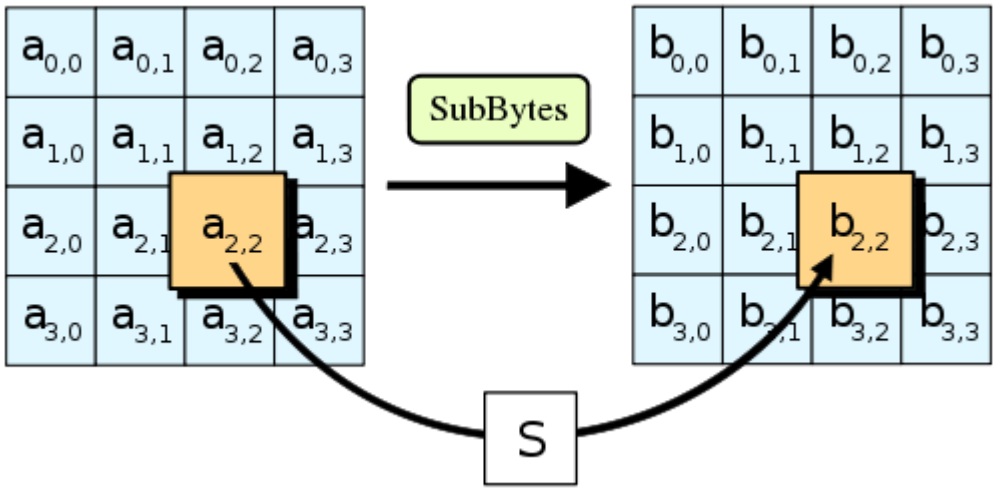
AES veikimo algoritmą bendrai galime aprašyti tokiais žingsniais:

1. Pradiniame raunde atliekama *AddRoundKey()* funkcija
2. Kituose raunduose atliekamos šios funkcijos:
    - *SubBytes()* – būsenos baitai pakeičiami pagal duotą sukeitimo lentelę (4 pav.)
    - *ShiftRows()* – būsenos eilutės paslenkamos kairėn skirtingais poslinkiais (5 pav.)
    - *MixColumns()* – kiekvieno stulpelio duomenys sumaišomi atsižvelgiant į būseną (6 pav.)

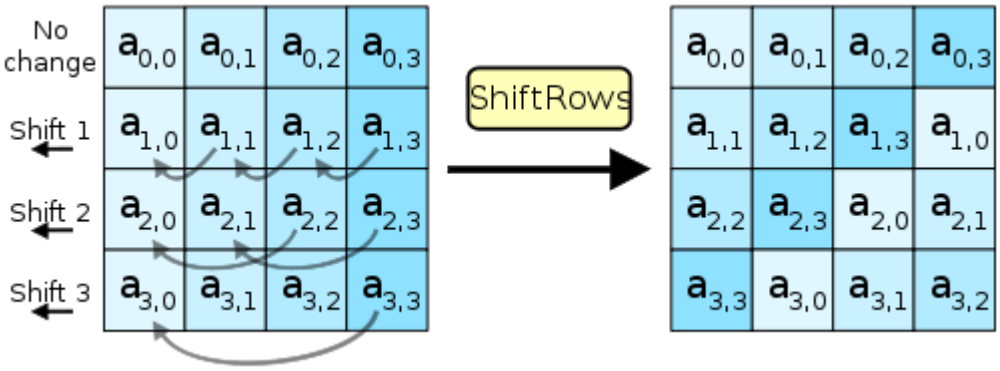
- *AddRoundKey()* - raundo raktas pridedamas prie būsenos. Šioje vietoje ir panaudojami slaptasis (simetrinis) raktas bei iš jo gautas raktų sąrašas. (7 pav.)

3. Paskutiniame raunde atliekamos šios funkcijos:
   - *SubBytes()*
   - *ShiftRows()*
   - *AddRoundKey()*

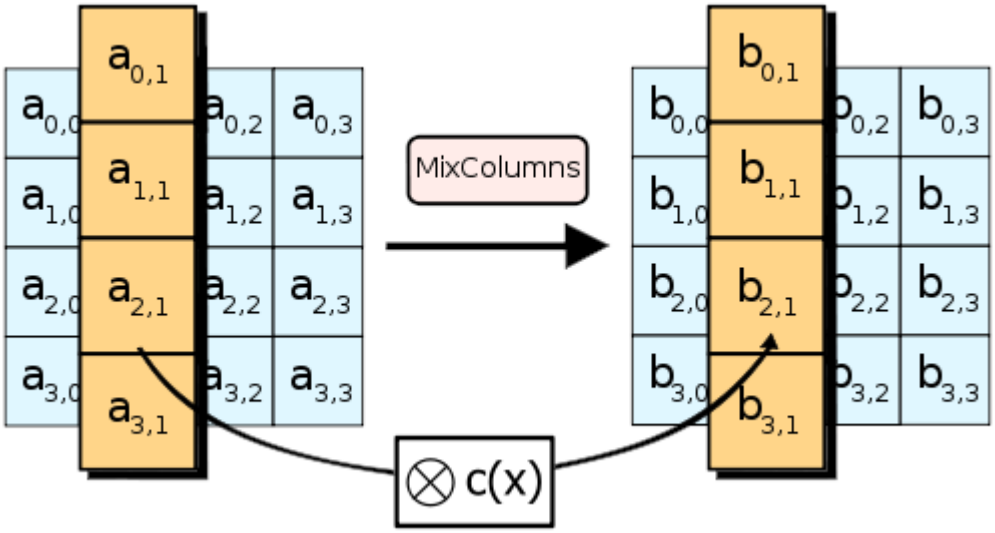
Algoritmo raudų skaičius 10, 12 arba 14 priklauso nuo naudojamo rakto ilgio.



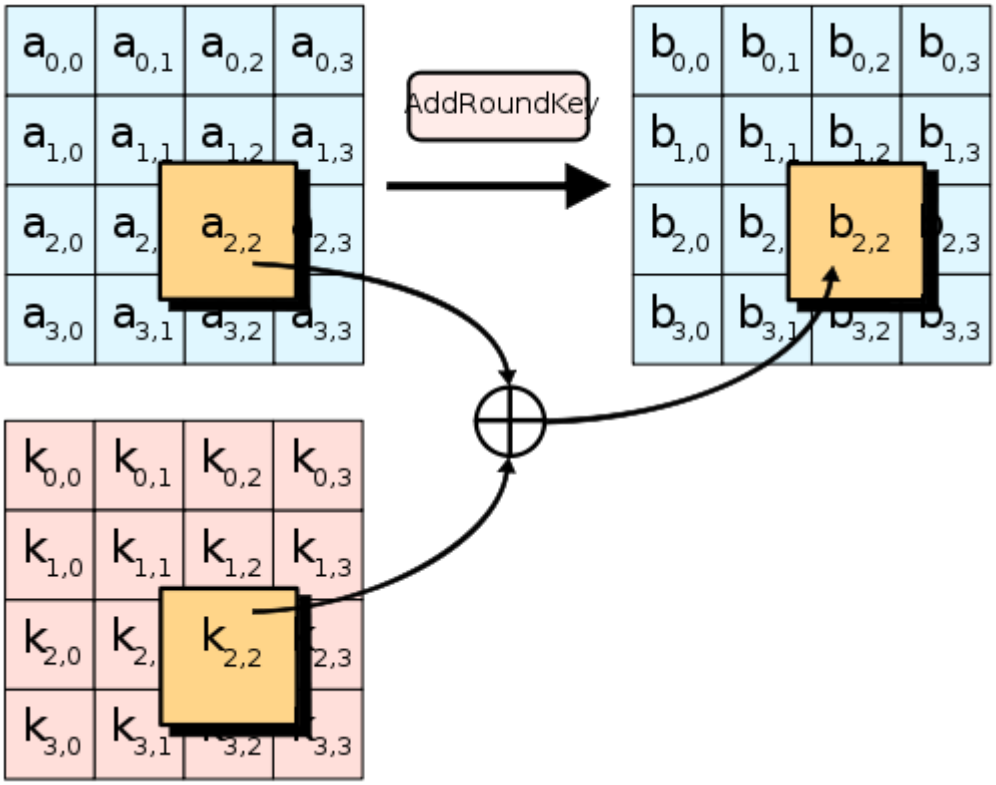
4 pav. Būsenos baitai pakeičiami pagal duotą sukeitimo lentelę



5 pav. Būsenos eilutės paslenkamos kairėn skirtingais poslinkiais



6 pav. Kiekvieno stulpelio duomenys sumaišomi atsižvelgiant į būseną



7 pav. Raundo raktas pridedamas prie būsenos

Įvykdyta ataka prieš AES

Nuo 2006 metų vienintelė sėkmingai įvykdyta ataka side-channel prieš AES šifravimo algoritmą. AES algoritmas pakankamą saugumą užtikrina su visais raktų ilgiais (128, 192, 256 bitų). Tačiau norint apsaugoti ypatingai svarbią informaciją būtina naudoti 192 arba 256 bitų raktus. AES vykdomas su 128 bitų raktu 10 raundų, 192 bitų raktu – 12, o su 256 bitų raktu – 14. 2006 m. žinomiausios atakos buvo 128 bitų raktu 7 raunde, 192 bitų raktu

– 8, o 256 bitų raktu – 9. Greičiausias kriptografinis nulaužimas yra galimų variantų paieška. Taigi, XSL (eXtended Sparse Linearization) ataka, kuri yra kriptoanalizės metodas skirtas blokiniams šiframs, vykdoma prieš AES 128 bitų raktą reikalauja 2100 operacijų (palyginimui 2128 galimų raktų skaičius) tam, kad būtų įvykdytas nulaužimas. Skirtingai nuo daugelio kitų blokinių šifrų, AES yra paprastai ir aiškiai aprašytas. 2002 m. Nicolas Courtois ir Josef Pieprzyk paskelbė teorinę ataką, pavadinimu „XSL ataka“, kurioje buvo siekiama parodyti AES algoritmo silpnumą dėl jo paprasto aprašymo. Nuo tada, kiti dokumentai pateikia, jog ataka nėra galima kaip iš pradžių buvo teigiama. [11]

Side-channel ataka įveikia AES šifro mechanizmą, tačiau ne dėl AES algoritmo saugumo spragų, bet dėl prasto AES šifro realizavimo sistemoje, kurioje galimas duomenų nutekėjimas ir jų analizė.

1.3.2 Raktų apsikeitimo protokolai

1.3.2.1 Diffie-Hellman raktų apsikeitimo protokolas

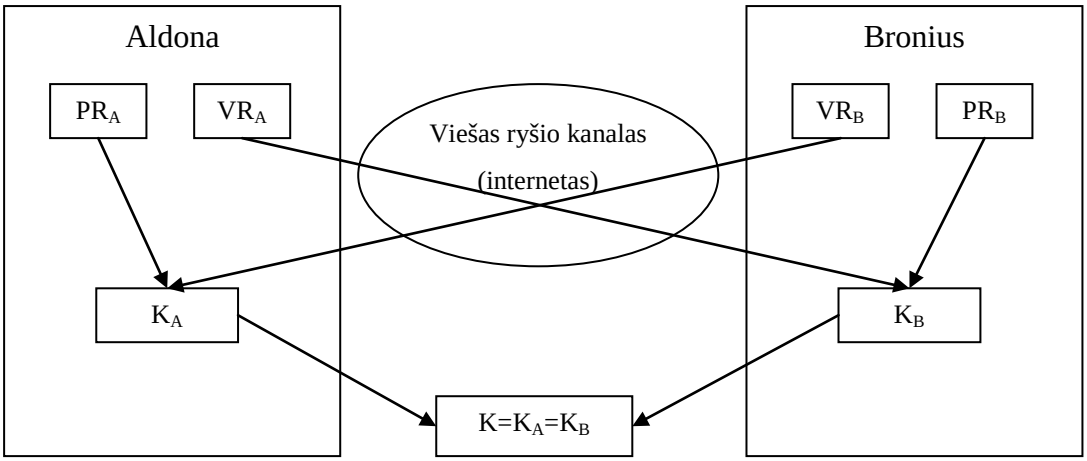
Diffie-Hellman (DH) raktų apsikeitimo protokolas buvo sukurtas 1976 metais. Jo dėka du vartotojai gali sukurti bendrąjį slaptą raktą viešame ryšio kanale, o iš vartotojų siunčiamos informacijos nebus galima nustatyti jų sukurto bendrojo slapto rakto. DH algoritmas realizuotas taip, jog vartotojai naudodami skirtingus įvesties duomenis, gautų vienodus rezultatus. DH rakto apsikeitimo protokolo reikšmė panaudojama seanso raktui sukurti. [11, 19]

DH raktų apsikeitimo protokolo veikimo mechanizmas

DH raktų apsikeitimo protokolo veikimas:

- Aušra ir Bernardas pirmiausiai viešai susitaria dėl didelio pirminio skaičiaus p ir grupės Z_p^* generatoriaus g.
- Aušra atsitiktinai pasirenka savo slaptąjį raktą $PR_A = x$, tada suskaičiuoja savo viešąjį raktą $VR_A = a = g^x \bmod p$ ir viešąjį raktą siunčia Bernardui.
- Bernardas atsitiktinai pasirenka savo slaptąjį raktą $PR_B = y$, tada suskaičiuoja savo viešąjį raktą $VR_B = b = g^y \bmod p$ ir viešąjį raktą siunčia Aušrai.
- Aušra, turėdama savo slaptąjį raktą $PR_A = x$ ir Broniaus viešąjį raktą $VR_B = g^y \bmod p$, apskaičiuoja bendrą raktą $K_A = (VR_B)^x \bmod p = g^{xy} \bmod p$.
- Bernardas, turėdamas savo slaptąjį raktą $PR_B = y$ ir Aušros viešąjį raktą $VR_A = g^x \bmod p$, apskaičiuoja bendrą raktą $K_B = (VR_A)^y \bmod p = g^{yx} \bmod p$.

Tokiu būdu Aušra ir Bernardas apsiskaičiuoja bendrą slaptą raktą K, kadangi $K = g^{xy} \bmod p = g^{yx} \bmod p$ (8 pav.). [11]



8 pav. DH raktų apsikeitimo protokolo veikimo schema

Dabar pateiksime DH raktų apsikeitimo protokolo pavyzdį (4 lentelė):

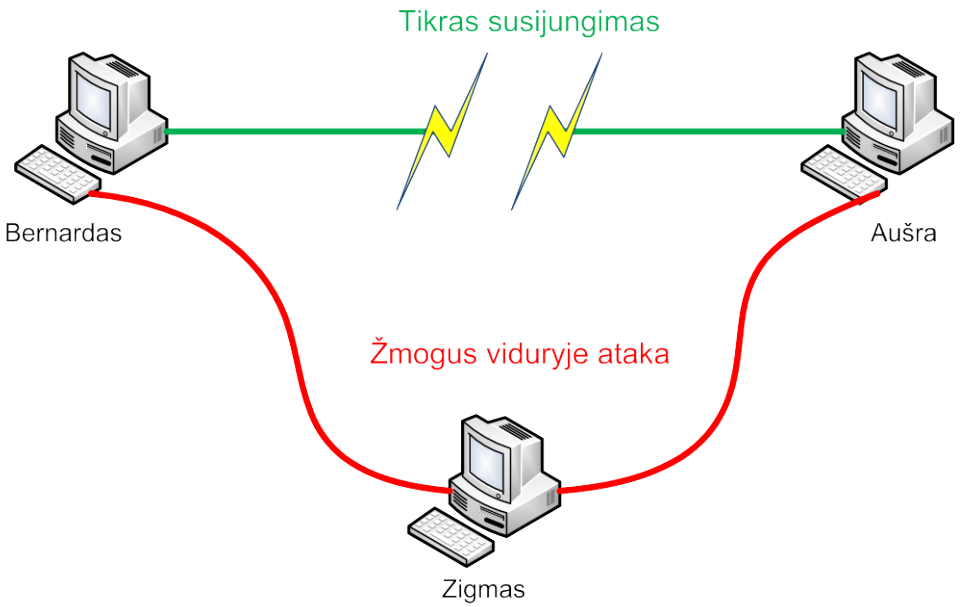
4 lentelė. DH protokolo veikimas pažingsniui

Aušra				**Bernardas**		
Seka		Skaičiuoja		Skaičiuoja		Seka
	p, g				**p, g**	
a						**b**
		$\mathbf{g}^{\mathbf{a}}$ mod p	$\rightarrow$		...	
	…		$\leftarrow$	$\mathbf{g}^{\mathbf{b}}$ mod p		
	$(\mathbf{g}^{\mathbf{b}}$ mod p$)^{\mathbf{a}}$ mod p		=		$(\mathbf{g}^{\mathbf{a}}$ mod p$)^{\mathbf{b}}$ mod p	

Kaip matome abu vartotojai gavo tokį patį rezultatą, kadangi g^{ab} ***mod*** p ir g^{ba} ***mod*** p yra lygūs. Paslaptyje laikomi tik atsitikinai pasirinkti skaičiai *a, b* ir apskaičiuotos reikšmės g^{ab} ***mod*** p, g^{ba} ***mod*** p. Visos kitos reikšmės: p, g, g^{a} ***mod*** p, ir g^{b} ***mod*** p yra žinomos. Kai Aušra ir Bernardas apskaičiuoja bendrą slaptąjį raktą, kurį toliau gali naudoti kaip šifravimo raktą siųsdami žinutes per viešą ryšio kanalą (internetą). Jis bus žinomas tik abiems vartotojams.

Ataka „žmogus viduryje“

Pagrindinė DH raktų apsikeitimo protokolo saugumo problema iškyla tada, kai atsiranda „aktyvus“ kenkėjas Zigmas. Nors Zigmas žino viešuosius Aušros ir Broniaus raktus bei mato jų siunčiamus pranešimus, tačiau tokių pat veiksmų kaip jie atlikti negali. Iš turimų viešųjų raktų ji negali apskaičiuoti bendro slaptojo rakto K, kadangi tam reikia išspręsti Diffie – Hellman problemą. Zigmas norėdamas apskaičiuoti bendrą slaptąjį raktą K, turi žinoti nors vieną privatųjį raktą.



9 pav. Ataka „Žmogus viduryje”

Jei Zigmas turi galimybę ne tik stebėti pranešimus, tačiau juos pakeisti ir siųsti, tuomet gali būti įvykdyta ataka „žmogus viduryje“ (9 pav.) (angl. *Man in the middle*).

Tuo metu kai vykdoma „žmogaus viduryje“ ataka DH raktų apsikeitimo protokolo veikimas būtų:

- Aušra ir Bernardas pirmiausiai viešai susitaria dėl didelio pirminio skaičiaus p ir grupės Z_p^* generatoriaus g. Kadangi informacija yra vieša apie tai sužino ir Zigmas.
- Aušra atsitiktinai pasirenka savo slaptąjį raktą $PR_A = x$, tada suskaičiuoja savo viešąjį raktą $VR_A = a = g^x \bmod p$ ir viešąjį raktą siunčia Bernardui. Kadangi Zigmas yra aktyvus kenkėjas ir turi galimybę ne tik stebėti siunčiamus pranešimus, tačiau ir pati juos siųsti, tai ji perima Aušros siunčiamą pranešimą, jį modifikuoja ir išsiunčia Bernardui savo viešąjį raktą $VR_Z = u = g^z \ mod \ p$. Naudodama savo privatų raktą $PR_Z = z$ Zigmas apskaičiuoja bendrą slaptą raktą su Aušra $K_{AZ} = (VR_A)^z \bmod p = g^{xz} \bmod p$
- Bernardas atsitiktinai pasirenka savo slaptąjį raktą $PR_B = y$, tada suskaičiuoja savo viešąjį raktą $VR_B = b = g^y \bmod p$ ir viešąjį raktą siunčia Aušrai. Zigmas perima Broniaus siunčiamą pranešimą, jį modifikuoja ir išsiunčia Aušrai savo viešąjį raktą $VR_Z = u = g^z \ mod \ p$. Naudodamas savo privatų raktą $PR_Z = z$ Zigmas apskaičiuoja bendrą slaptą raktą su Bernardu $K_{BZ} = (VR_B)^z \bmod p = g^{yz} \bmod p$
- Aušra, turėdama savo slaptąjį raktą $PR_A = x$ ir Zigmo suklastotą Bernardo viešąjį raktą $VR_B = g^y \bmod p$, apskaičiuoja bendrą raktą $K_{AZ} = (VR_Z)^x \bmod p = g^{xz} \bmod p$.

- Bernardas, turėdamas savo slaptąjį raktą PR_B = y ir Zigmo suklastotą Aušros viešąjį raktą $VR_A = g^x \bmod p$, apskaičiuoja bendrą raktą $K_{BZ} = (VR_Z)^y \bmod p = g^{yz} \bmod p$.

Taigi slaptasis bendras raktas K yra ne tiesiogiai tarp Aušros ir Bernardo, tačiau tarp Aušros ir Zigmo bei Zigmo ir Bernardo. Sėkmingai tai įgyvendinus Zigmas gali skaityti pranešimus bei juos klastoti.

DH raktų apsikeitimo protokolas nėra veiksmingas aktyvaus kenkėjo atveju, nes neįmanoma užfiksuoti fakto kada jis atsiranda, o tai neužtikrina konfidencialumo. Norint išvengti tokio tipo atakos, naudojamas autentifikuotas DH raktų apsikeitimo protokolas. [9, 11, 19]

1.3.2.2 Autentifikuotas Diffie-Hellman raktų apsikeitimo protokolas

Autentifikuotas DH raktų apsikeitimo protokolas vykdomas taip:

- Aušra ir Bernardas viešai susitaria dėl bendrų sistemos parametrų – didelio pirminio skaičiaus p ir grupės Z_p^* generatoriaus g.
- Aušra pasirenka atsitiktinį skaičių x, apskaičiuoja $k_x = g_x \bmod p$, gautą reikšmę pasirašo $s_x = S(k_x, PR_A)$ ir siunčia Bernardui porą (k_x, s_x).
- Bernardas pasirenka atsitiktinį skaičių y, apskaičiuoja $k_y = g_y \bmod p$, gautą reikšmę pasirašo $s_y = S(k_y, PR_B)$ ir siunčia Aušrai porą (k_y, s_y).
- Aušra, gavusi porą (k_y, s_y), pirmiausia patikrina B e. parašą. Jei parašas tikras, apskaičiuoja bendrą raktą $K_A = (k_y)^x \bmod p = g^{yx} \bmod p$.
- Bernardas, gavęs porą (k_x, s_x), pirmiausia patikrina A e. parašą. Jei parašas tikras, apskaičiuoja bendrą raktą $K_B = (k_x)^y \bmod p = g^{xy} \bmod p$.

Tokiu atveju vartotojo autentifikavimas užtikrinamas e. parašu, kuris pagal apibrėžimą yra atsparus klastojimui. Be to, e. parašas taip pat užtikrina duomenų vientisumą. Taigi, jei kenkėjas poroje (k_x, s_x) modifikuos k_x, e. parašo patikra bus atmesta. Jei pakeis visą porą į (k_z, s_Z), parašas bus tikras. Tačiau patikrinęs e. parašo sertifikatą, gavėjas nustatys, kad siuntėjas netikras, ir nutrauks tolesnį protokolo vykdymą. [12]

1.3.2.3 Išvados

Simetriniame šifravime būtinas saugus raktų apsikeitimas tarp bendraujančių šalių. Vienu saugiausių rakto apsikeitimo protokolų yra laikomas šiame skyriuje aptartas Diffie-Hellman raktų apsikeitimo protokolas. Ataka prieš šį raktų apsikeitimo protokolą buvo sėkmingai įvykdyta ne dėl algoritmo silpnumo, o dėl galimo informacijos perėmimo jos perdavimo momentu. Norint išvengti minėtos atakos reikia naudoti autentifikuotą Diffie-Hellman raktų apsikeitimo protokolą.

1.3.3 Saugaus ryšio kanalo naudojimas informacijos apsaugai

SSL (*Secure Sockets Layer*) – kriptografinis algoritmas, kuris yra naudojamas informacijai, perduodamai viešuoju ryšio kanalu, šifruoti. SSL perduodamos informacijos šifravimui naudojama simetrinė ir asimetrinė kriptografija. Asimetrinė kriptografija naudojama saugiam raktų apsikeitimui, o simetrinė kriptografija dėl didelio šifravimo greičio naudojama informacijos šifravimui. SSL protokolą sukūrę kompanija Netscape. [13, 14]

TLS (*Transport Layer Security*) – tai SSL protokolo atmaina, kurią remiantis SSL 3.0 protokolo sukūrė IETF (*The Internet Engineering Task Force*). Protokolas naudojamas kliento-serverio programose, kadangi leidžia tinkle siunčiamus pranešimus apsaugoti nuo klastojimo. TLS protokole realizuotas autentifikacijos ir konfidencialumo internete mechanizmas panaudojant kriptografiją.

TLS protokolo dėka galimi du autentifikavimo atvejai:

- Autentifikuojamas tik serveris
- Autentifikuojamas serveris ir vartotojas

Autentifikuoto serverio atveju, klientas jungdamasis prie serverio įsitikina jo tikrumu, tačiau pats klientas lieka nežinomas.

Kuomet abi bendraujančios pusės autentifikuojamos, būtinas ne tik serverio sertifikatas, tačiau ir klientas turi turėti sertifikatą, kuriuo patvirtintų savo tapatybę.

TLS sudaro trys pagrindinės fazės:

- Bendraujančių pusių susitarimas dėl naudojamo algoritmo
- Raktų apsikeitimas ir autentifikavimas
- Simetrinių šifravimas ir žinučių autentifikavimas

Standartiniai algoritmai naudojami TLS protokole:

- Raktų apsikeitimui: RSA, Diffie-Hellman, ECDH, SRP, PSK
- Autentifikavimui: RSA, DSA, ECDSA
- Simetriniai šifrai: RC 4, Triple DES, AES, IDEA, DES, Camellia.
- Kriptografinės santraukos funkcijos: HMAC-MD5 arba HMAC-SHA (***TLS***), MD5 ir SHA (***SSL***) [13, 14]

1.3.3.1 TLS „rankų paspaudimo“ algoritmas

„Rankų paspaudimo“ (angl. *handshaking*) metu klientas susitaria su serveriu dėl naudojamų parametrų, siekiant užtikrinti saugų susijungimą.

- „Rankų paspaudimas“ prasideda tuomet, kai klientas jungiasi prie serverio, turinčio aktyvų TLS protokolo palaikymą, prašydamas saugaus susijungimo ir pateikdamas sąrašą palaikomų šifrų bei santraukos funkcijų (angl. hash functions).

- Iš šio sąrašo serveris išrenką „stipriausią“ šifrą ir santraukos funkciją, kurią jis irgi palaiko ir informuoja klientą apie pasirinkimą.
- Serveris siunčia savo identifikavimo duomenis sertifikato forma. Sertifikatą sudaro serverio vardas, patikimas sertifikatų centras ir serverio viešasis raktas.

Klientas gali susisiekti su serveriu, kuris išdavė sertifikatą ir paprašyti patvirtinti, jog sertifikatas yra tikras, prieš toliau vykdydamas veiksmus.

- Tam kad būtų galima sugeneruoti susijungimo sesijos raktus, naudojamus saugiam susijungimui, klientas turi užšifruoti savo sugalvotą atsitiktinį skaičių su serverio viešuoju raktu (VR_S) ir gautą rezultatą nusiųsti serveriui. Tik serveris galės iššifruoti jį (su savo privačiuoju raktu (PR_S). Tokiu būdu raktas yra paslepiamas nuo galimų atakuotųjų. Klientas žino serverio viešąjį raktą ir savo sugalvotą skaičių, o serveris žino savo privatų raktą ir ,po to kai iššifruoja kliento žinutę, kliento sugalvotą skaičių. Galimas atakuotojas žino tik serverio viešąjį raktą, nebent serverio privatus raktas buvo išaiškintas.
- Iš atsitiktinai sugalvoto skaičiaus, serveris ir vartotojas sugeneruoja raktą kurį naudos šifravimui ir iššifravimui

„Rankų paspaudimas“ baigiasi ir pradedamas saugus susijungimas, kurio metu siunčiami duomenys šifruojami ir iššifruojami su sugeneruotu raktu. Tai vyksta tol kol susijungimas nutraukiamas. [13, 14]

Jei bet kuriame žingsnyje įvyksta klaida, TLS „raktų paspaudimas“ ir susijungimas neįvyksta.

1.3.3.2 Paprastas TLS „rankų paspaudimas“

Paprastas TLS „rankų paspaudimas“ apibrėžia serverio autentifikavimą.

1. Susitarimo etapas:
    - Klientas siunčia *ClientHello* žinutę, kurioje nurodo:
        - kokią TLS protokolo versiją jis gali naudoti
        - sugeneruotą atsitiktinį skaičių
        - siūlomų naudoti šifrų ir suspaudimo metodų sąrašą
    - Serveris atsako su *ServerHello* žinute, kurioje yra informacija:
        - pasirinkto protokolo versija
        - sugeneruotas skaičius
        - pasirinktas (iš kliento pasiūlytų) šifro algoritmas ir suspaudimo metodas

        - taip pat *session id* kaip žinutės dalis, kuri nurodo, jog tęsiamas „rankų paspaudimas“
    - Serveris siunčia *Certificate* žinutę
    - Serveris siunčia *ServerHelloDone* žinutę, kuria nurodomas „rankų paspaudimo“ baigimas šiame etape.
    - Klientas atsako su *ClientKeyExchange* žinute, kurioje gali nieko nebūti arba viešasis raktas, priklausomai nuo naudojamo šifro.
    - Klientas ir serveris naudodamas atsitiktinį skaičių ir pagalbinį pagrindinį raktą apskaičiuoja pagrindinį raktą.
2. Klientas siunčia *ChangeChiperSpec* įrašą, informuodamas serverį, jog viskas kas bus siunčiama bus autentifikuota (ir šifruota, jei šifravimo parametrai nustatyti serveryje).
    - Galiausiai klientas siunčia autentifikuotą ir šifruotą *Finished* žinutę
    - Jei serverio patikrinime įvyksta klaida susijungimas nutraukiamas
3. Serveris siunčia *ChangeChiperSpec* žinutę, informuodamas klientą, jog viskas kas bus siunčiama bus autentifikuota (ir šifruota serverio privačiu raktu, kuris yra susijęs su sertifikuotu viešuoju raktu, jei šifravimas reikalingas).
    - Serveris siunčia autentifikuotą ir šifruotą *Finished* žinutę
    - Klientas atlieka iššifravimo ir patikrinimo veiksmus, jei įvyksta klaida susijungimas nutraukiamas.
4. Programos fazė

1.3.3.3 Autentifikuoto kliento TLS „rankų paspaudimas“

Paprastas TLS „rankų paspaudimas“ apibrėžia serverio autentifikavimą.

1. Susitarimo etapas:
    - Klientas siunčia *ClientHello* žinutę, kurioje nurodo:
        - kokią TLS protokolo versiją jis gali naudoti
        - sugeneruotą atsitiktinį skaičių
        - siūlomų naudoti šifrų ir suspaudimo metodų sąrašą
    - Serveris atsako su *ServerHello* žinute, kurioje yra informacija:
        - pasirinkto protokolo versija
        - sugeneruotas skaičius
        - pasirinktas (iš kliento pasiūlytų) šifro algoritmas ir suspaudimo metodas
        - taip pat *session id* kaip žinutės dalis, kuri nurodo, jog tęsiamas „rankų paspaudimas“

- Serveris siunčia *Certificate* žinutę
- Serveris reikalauja kliento sertifikato siųsdamas *CertificateRequest* žinutę
- Serveris siunčia *ServerHelloDone* žinutę, kuria nurodomas „rankų paspaudimo“ baigimas šiame etape.
- Klientas atsiunčia savo sertifikatą su *Certificate* žinute
- Klientas atsako su *ClientKeyExchange* žinute, kurioje gali nieko nebūti arba viešasis raktas, priklausomai nuo naudojamo šifro.
- Klientas siunčia *CertificateVerify* žinutę
- Klientas ir serveris naudodamas atsitiktinį skaičių ir pagalbinį pagrindinį raktą apskaičiuoja pagrindinį raktą.

2. Klientas siunčia *ChangeChiperSpec* įrašą, informuodamas serverį, jog viskas kas bus siunčiama bus autentifikuota (ir šifruota, jei šifravimo parametrai nustatyti serveryje).
    - Galiausiai klientas siunčia autentifikuotą ir šifruotą *Finished* žinutę
    - Jei serverio patikrinime įvyksta klaida susijungimas nutraukiamas
3. Serveris siunčia *ChangeChiperSpec* žinutę, informuodamas klientą, jog viskas kas bus siunčiama bus autentifikuota (ir šifruota serverio privačiu raktu, kuris yra susijęs su sertifikuotu viešuoju raktu, jei šifravimas reikalingas).
    - Serveris siunčia autentifikuotą ir šifruotą *Finished* žinutę
    - Klientas atlieka iššifravimo ir patikrinimo veiksmus, jei įvyksta klaida susijungimas nutraukiamas.
4. Programos fazė

1.4 Analizės dalies išvados

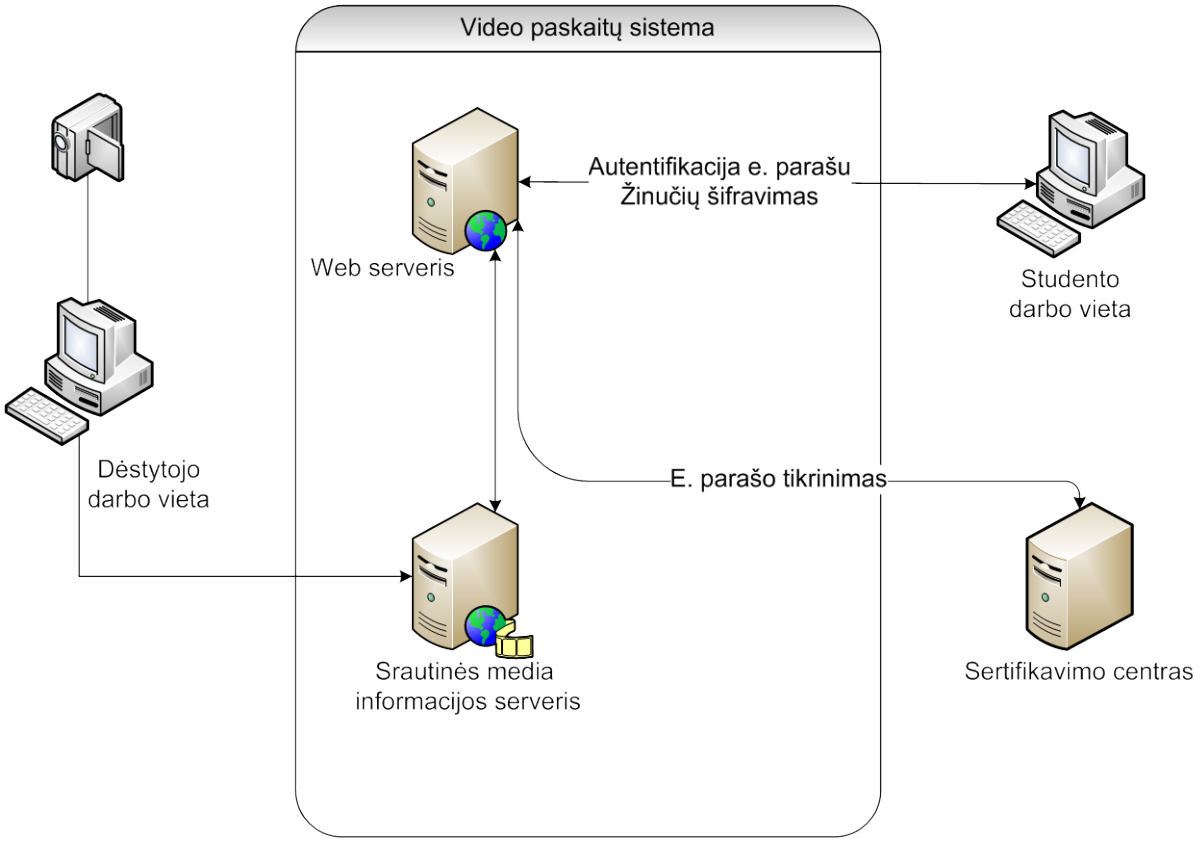
Atlikus egzistuojančių video paskaitų sistemų analizę, galima sakyti, jog patogiausia KTU sukurta *ViPS* video paskaitų sistema. Nors joje nėra realizuoto pateikiamos informacijos apsaugos mechanizmo, o esamas autentifikavimo mechanizmas yra primityvus, tačiau vartotojo aplinka pakankamai paprasta ir lengvai valdoma.

Kita analizės dalis apėmė kriptografinių algoritmų paiešką iškeltiems tikslams įgyvendinti. Pagrindinis tikslas sukurti video paskaitų sistemos autentifikavimo ir šifravimo mechanizmą paremtą e. parašu. Išanalizavus e. parašų veikimo principus ir galimus jų realizavimo būdus buvo pasirinkta RSA e. parašo schema. Keliamam būtinumui šifruoti video paskaitų sistemoje vartotojų siunčiamas žinutes buvo pasirinktas simetrinės kriptografijos šifravimo algoritmas – AES.

2 E. parašo taikymo autentifikavimui ir šifravimui video paskaitų sistemoje modelis

2.1 Konteksto schemos aprašymas

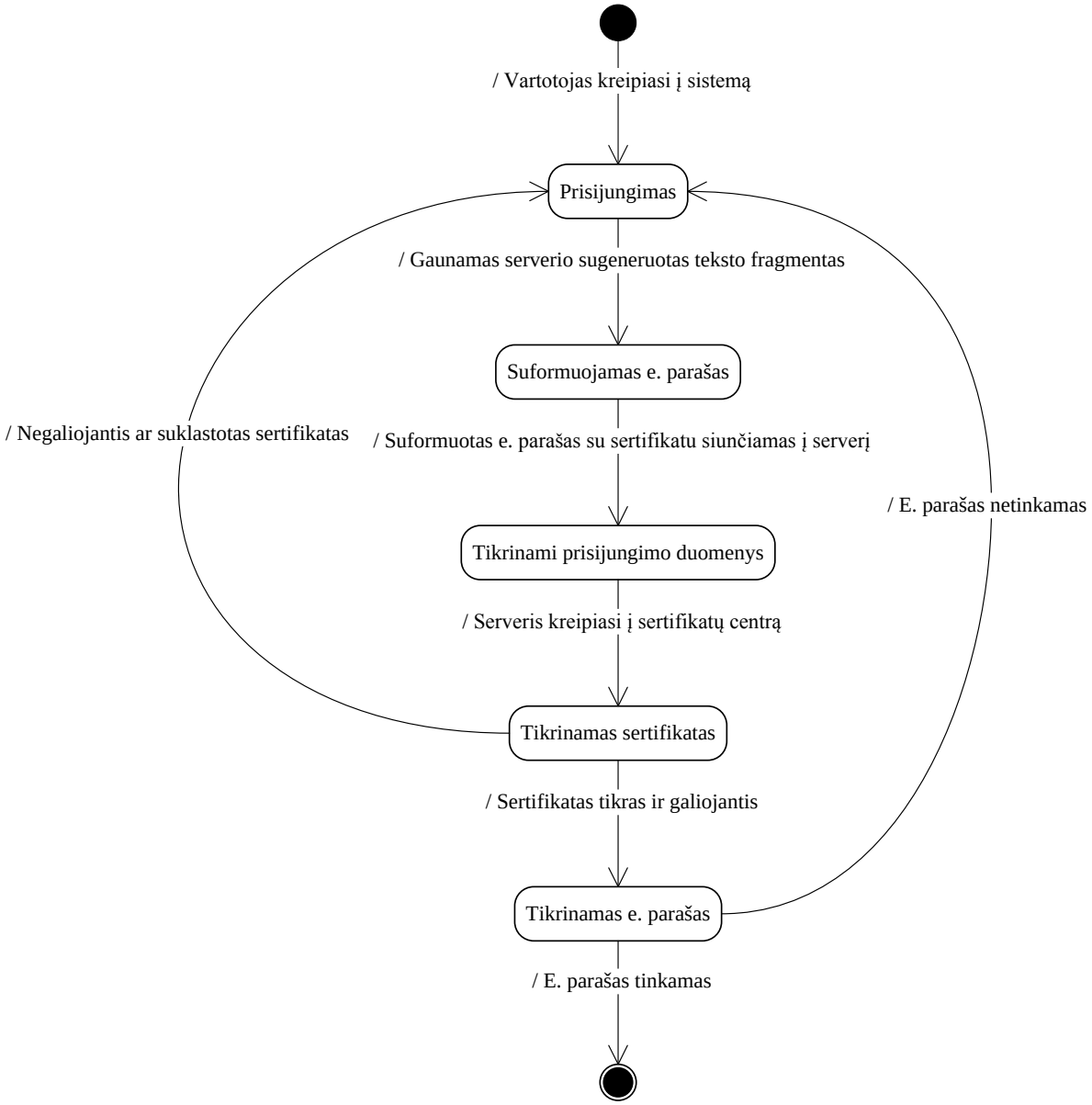
Kuriamas video paskaitų sistemos autentifikavimo ir informacijos šifravimo mechanizmas taikant elektroninį parašą (10 pav.) apima dvi saugumo požiūriu aktualias problemas, tai vartotojų autentifikavimą ir prieinamos informacijos patikimumą. Šiuo metu populiarus vartotojų autentifikavimas slaptažodžio principu nėra pakankamai saugus atsižvelgiant į tai, jog kuriamas sistemos modelis gali būti pritaikomas specialiose mokymo sferose, kuomet sistemos vartotojams pateikiama informacija su tam tikromis saugumo žymomis. Sistemos vartotojų autentifikavimui, naudojama RSA e. parašo schema. Informacijos patikimumo problemos sprendimui naudojamas informacijos, siunčiamos viešuoju ryšio tinklu, šifravimas. Šifravimui pasirinktas AES blokinio šifravimo algoritmas ir autentifikuotas Diffie–Hellman raktų apsikeitimo protokolas, dėl jų optimalaus veikimo greičio ir teikiamo saugumo lygio.



10 pav. Autentifikuotos video paskaitų sistemos komponentai

2.2 E. parašu pagrįstas prisijungimas prie sistemos

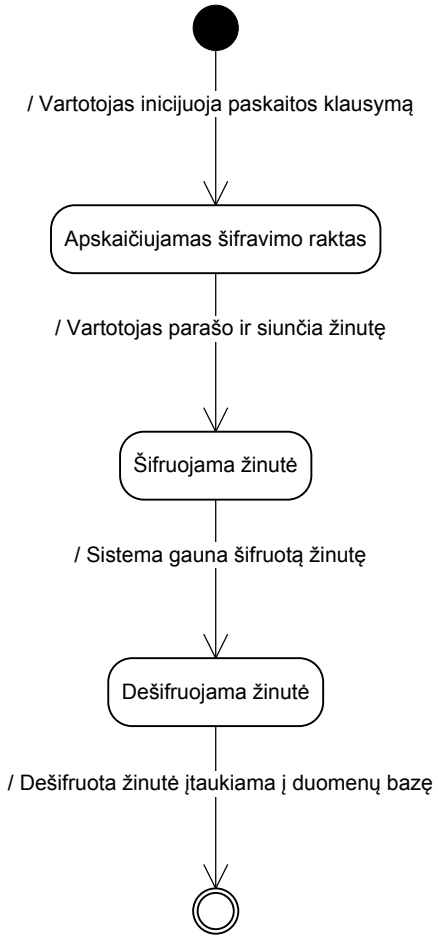
Siūlomas vartotojų autentifikavimas e. parašu kuriamoje sistemoje pateiktas 11 paveikslėlyje. Pirmiausiai vartotojas turi atsidaryti interneto naršyklę ir nurodyti sistemos adresą. Tuomet užkraunamas prisijungimo langas ir jam pateikiama atsitiktiniu būdu sistemos sugeneruota frazė, kurią vartotojas užšifruoja savo privačiuoju raktu taip suformuodamas e. parašą. Kartu su e. parašu sistemai siunčiamas sertifikatas. Tuomet sistema kreipdamasi į sertifikavimo centrą (SC) tikrina ar pateiktas vartotojo sertifikatas nėra suklastotas, ar galiojimo laikas nepasibaigęs. Jeigu pateiktas sertifikatas tikras ir galiojantis sistema identifikuoja asmenį ir pagal žinomą jo viešąjį raktą iššifruoja pateiktą žinutę, tokiu būdu patikrinamas e. parašas ir vartotojas prisijungia prie sistemos. Jeigu sertifikatas suklastotas ar negaliojantis arba pateikta pasirašyta žinutė neiššifruojama su to vartotojo viešuoju raktu, sistema neleidžia prisijungti ir prašo pakartoti anksčiau minėtus veiksmus.



11 pav. Vartotojų autentifikavimas e. parašu

2.3 Siunčiamų žinučių apsauga sistemoje

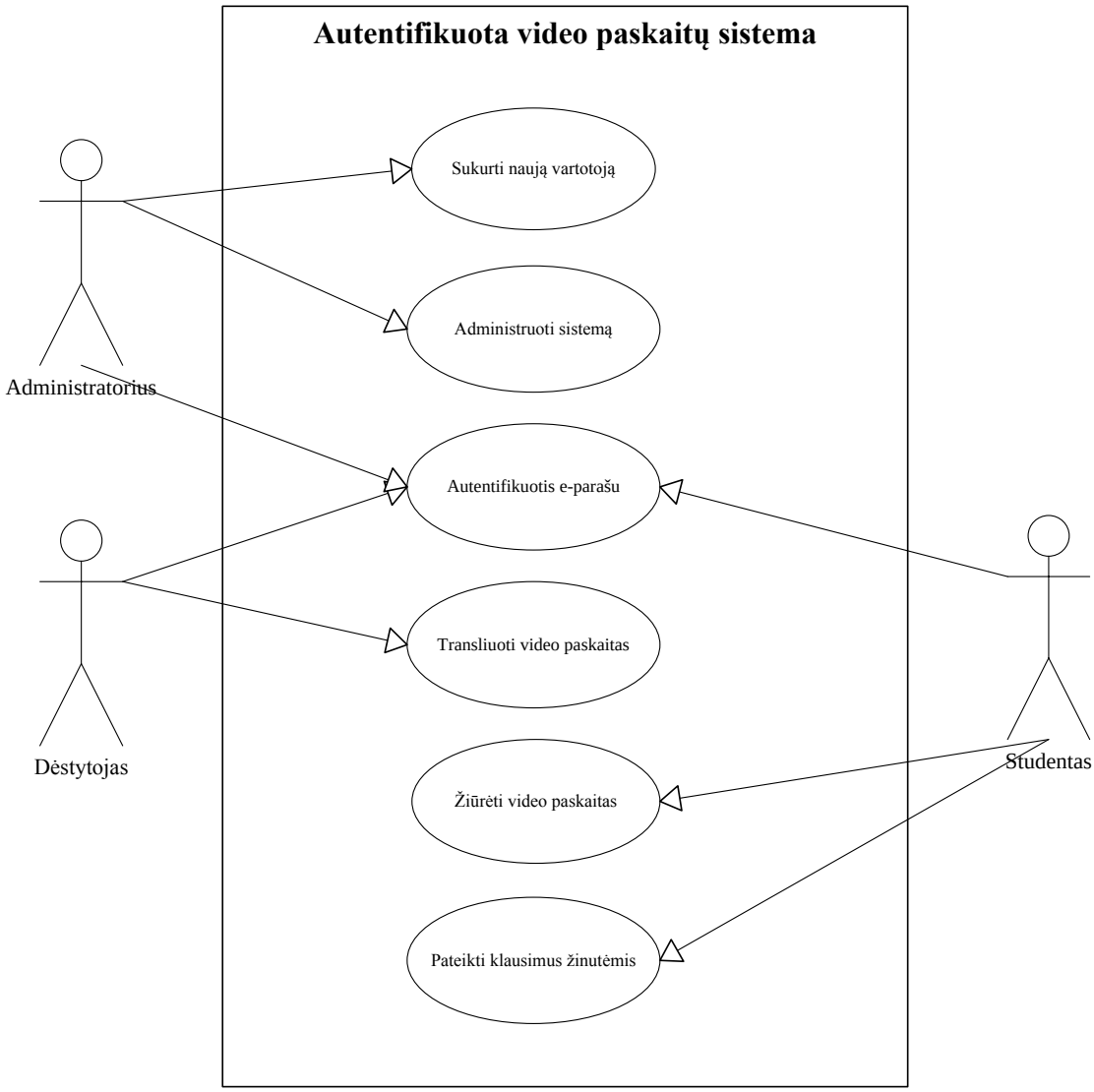
Siūlomame modelyje svarbus dėmesys skiriamas siunčiamų žinučių šifravimui. Sistema gali būti pritaikoma specifinėse mokymo srityse, kuriose pateikiama medžiaga su tam tikra saugumo žyme. Šiam tikslui įgyvendinti geriausias sprendimo būdas panaudoti e. parašą, autentifikuotą Diffie–Hellman raktų apsikeitimo protokolą ir AES šifravimo algoritmą. 12 paveikslėlyje pateiktas siūlomas apsaugos mechanizmas siunčiamų žinučių turinio apsaugai. Vartotojui prisijungus prie sistemos ir rengiantis klausyti paskaitos pradedamas šifravimo rakto sudarymas remiantis jau minėtu autentifikuotu Diffie–Hellman raktų apsikeitimo protokolu, kuriame panaudojamas e. parašas. Detalesnis šio protokolo aprašymas pateiktas analizės dalies 1.2 skyrelyje. Vartotojui siunčiant parašytą žinutę, ji užšifruojama, panaudojant apskaičiuotą šifravimo raktą ir AES šifravimo algoritmą, tada išsiunčiama į sistemą. Sistema gavusi šifruotą žinutę ją dešifruoja ir įtraukia į duomenų bazę.



12 pav. Siunčiamų žinučių šifravimas

2.4 Sistemos vartotojų grupės

Projektuojamoje sistemoje išskiriami trys vartotojų tipai: administratorius, dėstytojas, studentas. Kiekvienas iš jų sistemoje gali atlikinėti tam tikrus veiksmus, kaip tai parodyta 13 paveikslėlyje.



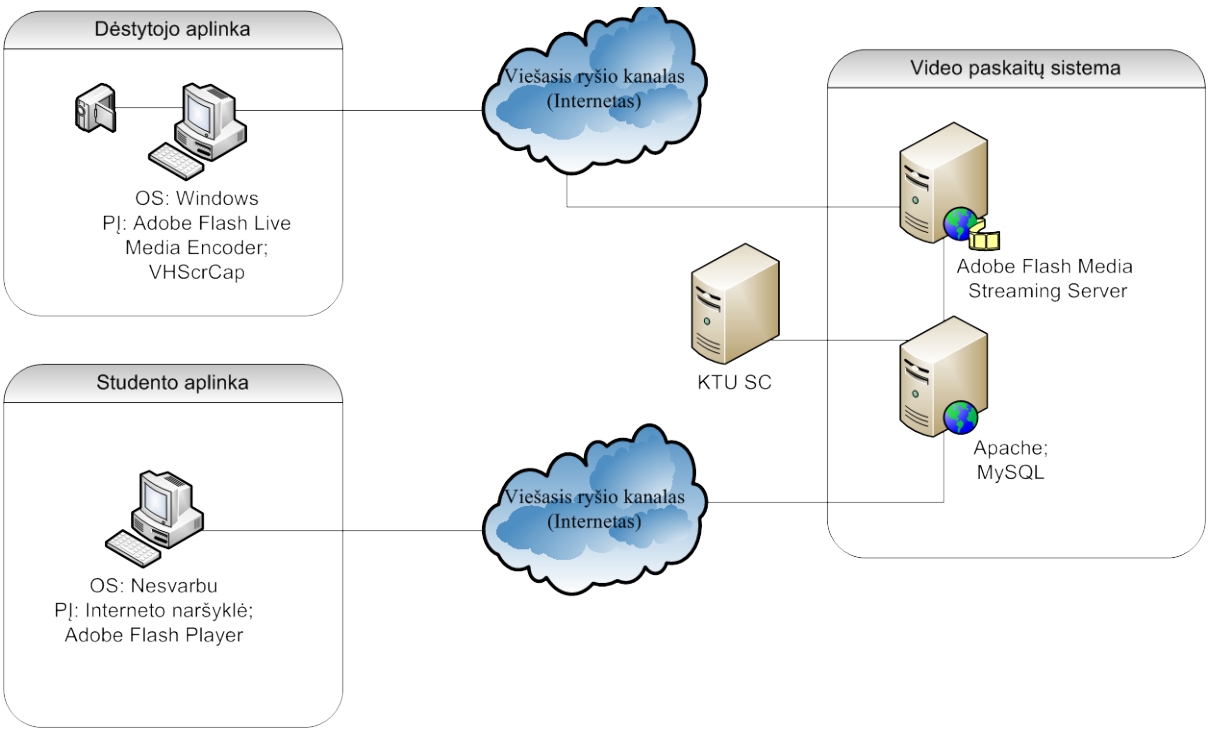
13 pav. Vartotojų veiksmai sistemoje

3 E. parašo taikymo autentifikavime ir šifravime video paskaitų sistemoje modelio realizacija

2 skyriuje pateikto projektuojamo sistemos modelio realizavimą galima būti suskirstyti į keletą dalių:

- dėstytojo aplinką
- video paskaitų sistemos branduolį
- studento aplinką

14 paveikslėlyje pateikiama visos sistemos konteksto schema. Šiame skyriuje detaliau aptarsime dėstytojo aplinką ir video paskaitų sistemos branduolį, pasakydami kuo jie svarbūs ir kokios technologijos naudojamos jų realizavime. Studento aplinka – tai internetinis puslapis, kuriame studentas gali stebėti transliuojamas video paskaitas



14 pav. Video paskaitų sistemos konteksto schema

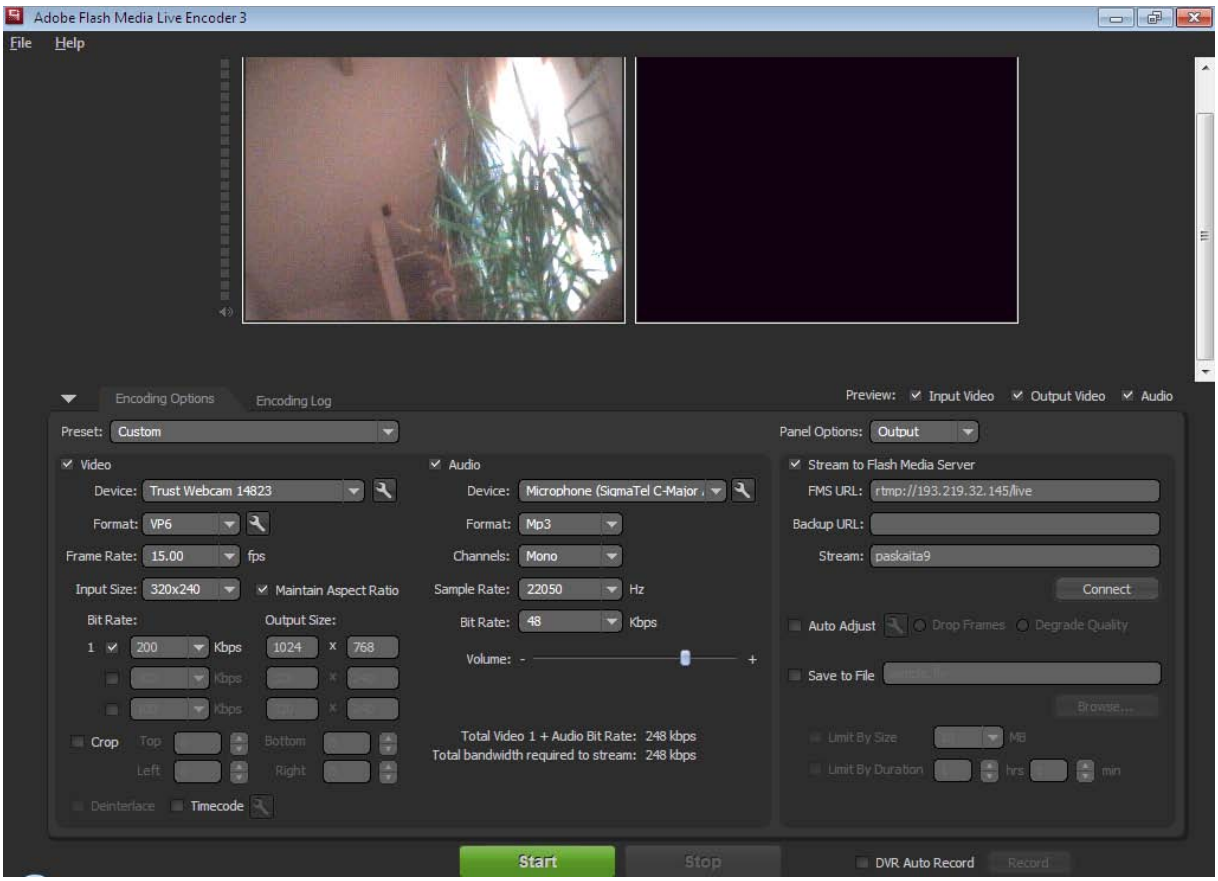
3.1 Dėstytojo aplinkos realizacija

Dėstytojo aplinkoje buvo sprendžiama viena iš pagrindinių esamų video paskaitų sistemų trūkumų – universalios mokomosios medžiagos pateikimas. Analizės dalyje nagrinėtose video paskaitų sistemose dėstytojas negali improvizuoti, pateikdamas studentams video, audio ar kitokio tipo pavyzdžių, kadangi minėtose sistemose dėstoma medžiaga pateikiama pateikčių arba kitokio tekstinio tipo formatu. Analizuotoje video paskaitų sistemoje *ViPS* dėstytojas pirmiausiai pateikia skaidres su mokomąja medžiaga

administratoriui, tik po to yra organizuojama video paskaita. Tačiau paskaitos metu iš anksto dėstytojo parinktas pavyzdys gali sukelti studentams papildomų klausimų. Šios problemos galima išvengti suteikiant dėstytojui galimybę realiu laiku keisti parengtos paskaitos informaciją.

Norint skaityti paskaitas realizuotoje video paskaitų sistemoje dėstytojui reikalingas kompiuteris su *Microsoft Windows* operacine sistema ir *Adobe Flash Media Live Encoder* (15 pav.) bei *VHScrCap* (16 pav.) programine įranga. *Adobe Flash Media Live Encoder* programinė įranga skirta transliuoti video ir audio signalą į Adobe Flash Streaming serverį, kuris yra video paskaitų sistemos sudedamoji dalis. *VHScrCap* (VH Screen Capture) – tai Splitmedialabs kompanijos programinis įrankis, kurio dėka video medžiagos šaltiniu laikomas kompiuterio ekrano vaizdas arba nurodyta jo dalis.

Dėstytojas, rengdamasis transliuoti paskaitą, pasiruošia medžiagą ir pasileidžia *Adobe Flash Media Live Encoder* programinę įrangą, tuomet nurodo transliuojamos video ir audio medžiagos kokybę, priklausomai nuo poreikių, ir pradeda transliaciją. Pasinaudojus *Adobe Flash* programavimo įrankiu specialiai dėstytojo aplinkai buvo sukurta programa, kuri informuoja paskaitą skaitantį dėstytoją apie studentų pateikiamus klausimus.



15 pav. Adobe Flash Media Live Encoder programinė įranga

16 pav. VH Screen Capture Driver programinė įranga

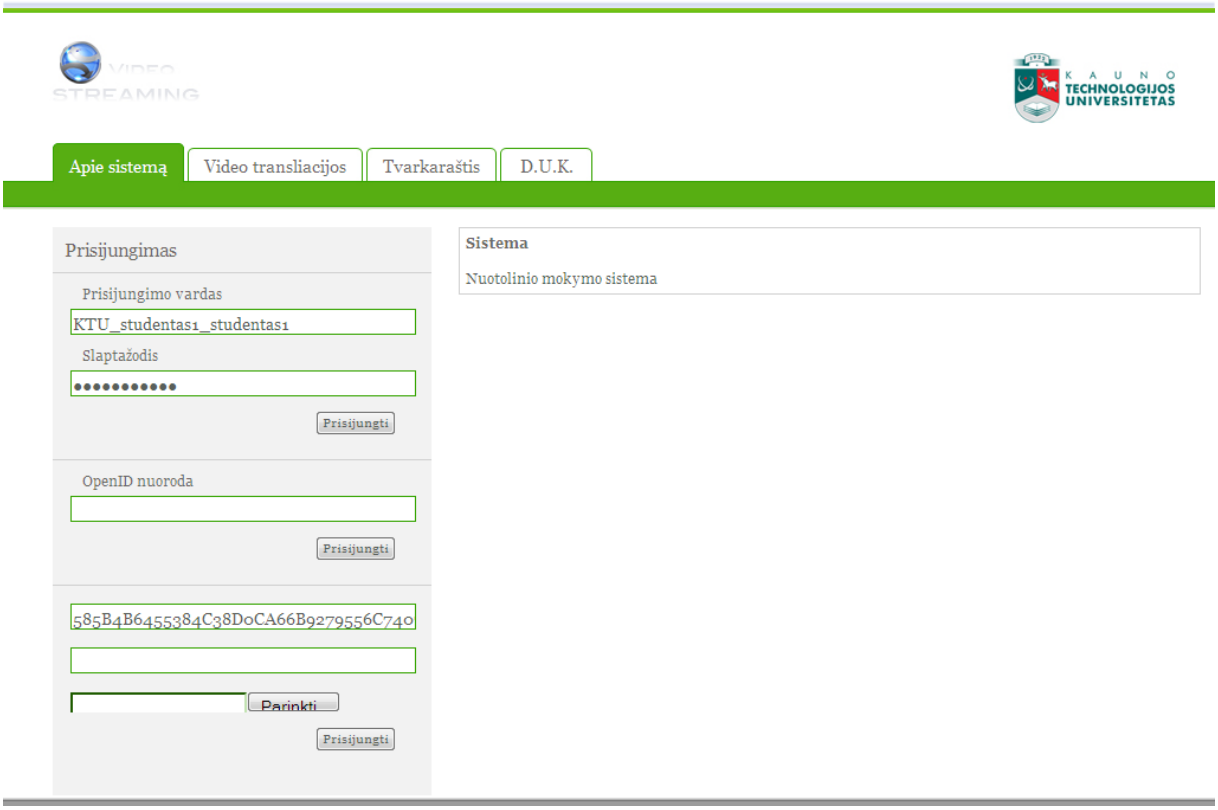
3.2 Video paskaitų sistemos realizacija

Projektuojamoje video paskaitų sistemoje svarbus dėmesys buvo skiriamas pateikiamos informacijos apsaugai šiais aspektais:

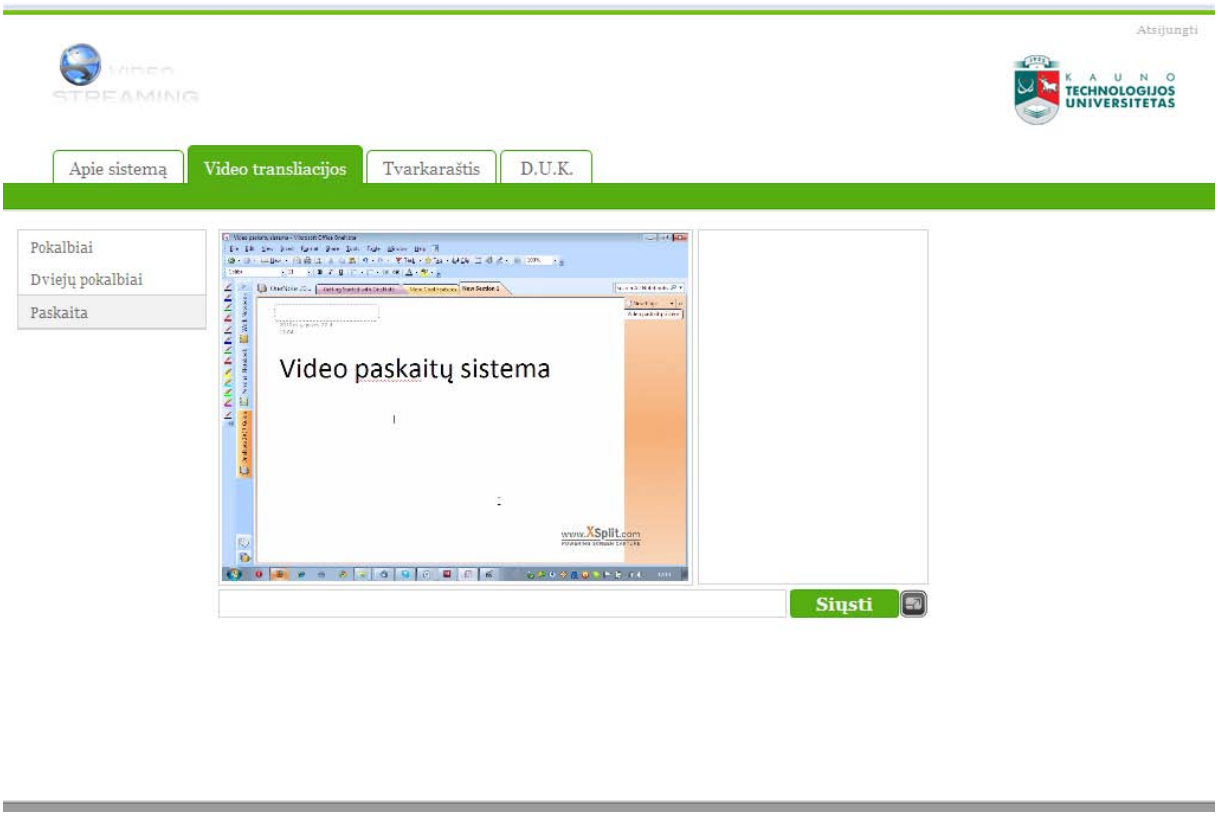
- Kiekvienas sistemos vartotojas autentifikuojamas e. parašu (17 pav.), kurio veikimo principas pateiktas 11 paveikslėlyje.
- Vartotojų siunčiamos žinutės per sistemą šifruojamos, panaudojant efektyviausius kriptografinius algoritmus.

Video paskaitų sistemos realizavimui buvo pasirinktas *Adobe Flash Media Streaming* serveris [1], leidžiantis perduoti aukštos kokybės video ir audio informaciją, ir klasikinis internetinis serveris, skirtas vartotojų sąsajos realizavimui. Aukštos kokybės video medžiagos naudojimas aktualus, kadangi dėstytojas gali transliuoti savo kompiuterio ekrano vaizdą (18 pav.). Atlikus panašių sistemų analizę buvo nuspręsta sistemą realizuoti internetinio puslapio principu. Tokia sistema ne tik patogi naudojimosi atžvilgiu, tačiau ir universali operacinių sistemų atžvilgiu.

Pagrindinis sistemos branduolys veikia internetiniame serveryje. Tekstinė informacija saugojama MySQL duomenų bazėje. Vartotojui autentifikuojantis e. parašu video paskaitų sistema kreipiasi į KTU sertifikavimo centrą, iš kurio gaunama informacija, pagal kurią patikrinamas vartotojo pateikto sertifikato galiojimas ir galimas suklastojimas.



17 pav. Prisijungimas e. parašu prie video paskaitų sistemos



18 pav. Realizuoto ekrano perdavimo pavyzdys

4 E. parašo taikymo video paskaitų sistemos autentifikavime ir šifravime eksperimentinis tyrimas

Sukurtoje video paskaitų sistemoje realizavus autentifikavimui skirtą e. parašo mechanizmą, svarbu nustatyti jo įtaką, prisijungimo prie sistemos laikui, lyginant su standartiniu vartotojo vardo ir slaptažodžio autentifikavimo mechanizmu. Minėtos charakteristikos tyrimas aptariamas pirmojoje eksperimentinio tyrimo dalyje. Kita aktuali sistemos funkcija - siunčiamų pranešimų šifravimas. Realizuota video paskaitų sistema nuolatos tobulinama, planuojama realizuoti perduodamos video medžiagos šifravimą. Video medžiagos ir siunčiamų pranešimų šifravimas II eksperimento dalyje palyginami matuojant algoritmų greičius.

4.1 Autentifikavimo e. parašu palyginimas su standartiniu prisijungimu

Siekiant nustatyti, kuris prisijungimo prie sistemos būdas yra greitesnis, buvo atliktas eksperimentinis tyrimas. Jo metu gauti prisijungimo prie sistemos laiko rezultatai, autentifikavimui naudojant e. parašą (20 pav) ir naudojant vartotojo vardą bei slaptažodį (19 pav.). Lentelėje Nr. 5 pateikiami 5 bandomųjų prisijungimų rezultatai.

5 lentelė. Prisijungimo prie sistemos laiko rezultatai

Autentifikavimo būdas	1 bandymas	2 bandymas	3 bandymas	4 bandymas	5 bandymas
	Laikas, sekundėmis				
Vartotojo vardas ir slaptažodis	0.00034	0.00038	0.00033	0.00037	0.00035
Autentifikavimas e. parašu	0.05762	0.01837	0.01573	0.03863	0.01807

Iš lentelėje pateiktų duomenų matosi, jog vartotojo prijungimo prie sistemos laikai skiriasi nuo 50 iki 150 kartų. Toks skirtumas susidaro dėl skirtingo atliekamų veiksmų skaičiaus norint autentifikuoti vartotoją.

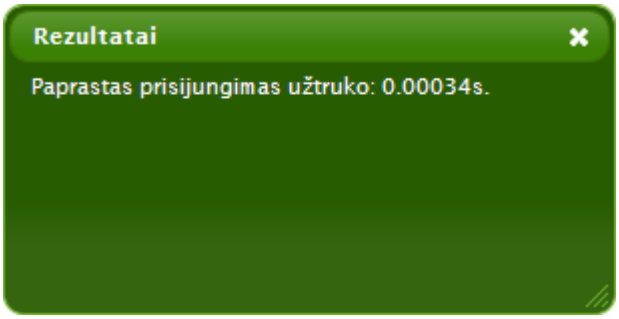
Autentifikuojant vartotojo vardu ir slaptažodžiu atliekami tokie veiksmai:

- Vartotojas nurodo savo vartotojo vardą bei slaptažodį ir spaudžia mygtuką prisijungti
- Sistema atlieką paiešką pagal pateiktą vartotojo vardą, jeigu netinkamas vartotojo prijungimas nutraukiamas
- Patikrinamas pateiktas slaptažodis su saugomu sistemos duomenų bazėje, jeigu netinkamas vartotojo prijungimas nutraukiamas
- Vartotojas prijungiamas prie sistemos

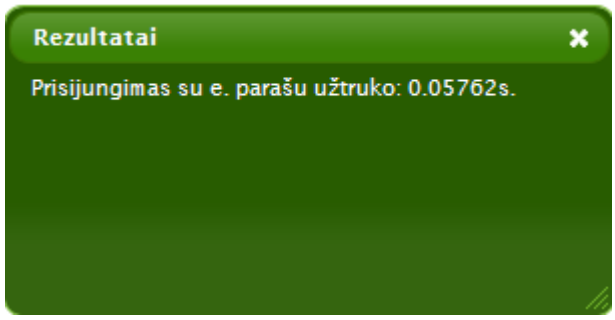
Autentifikuojant e. parašu atliekami tokie veiksmai:

- Sistema sugeneruoja frazę
- Vartotojas pasirašo pateiktą sistemos sugeneruotą frazę, prideda savo sertifikatą ir spaudžia prisijungimo mygtuką
- Sistema patikrina sertifikate esančią informaciją, pagal kurią vartotojas identifikuojamas
- Sistema kreipiasi į sertifikavimo centrą patikrinti ar vartotojo pateiktas sertifikatas nepanaikintas
- Sistema patikrina pasirašytą frazę
- Vartotojas prijungiamas prie sistemos, jei atlikti visi tikrinimo etapai

Gauti rezultatai parodė, jog autentifikavimas e. parašu yra žymiai lėtesnis nei autentifikavimas vartotojo vardu ir slaptažodžiu.



19 pav. Prisijungimo prie sistemos laiko rezultatai, autentifikavimui naudojant vartotojo vardą ir slaptažodį



20 pav. Prisijungimo prie sistemos laiko rezultatai, autentifikavimui naudojant e. parašą

4.2 Video medžiagos ir siunčiamų pranešimų šifravimo algoritmų teorinis palyginimas

Darbo pradžioje buvo keliama problema pateikiamos informacijos apsaugai panaudojant šifravimą. Šią problemą pavyko įgyvendinti sėkmingai šifruojant siunčiamus pranešimus. Realizuotoje video paskaitų sistemoje informacija pateikiama realiu laiku, todėl labai svarbu tinkamai parinkti kriptografiškai saugius ir greitai veikiančius algoritmus, kad

sistemos vėlinimas būtų kuo mažesnis. Analizės dalyje nurodyta, jog informacijos šifravimui labiausiai tinkami simetrinės kriptografijos algoritmai. Šiuo metu vienu saugiausių yra laikomas AES algoritmas. Šis algoritmas pasirinktas siunčiamų pranešimų šifravimui. Tolimesniame sistemos plėtojime yra numatomas video medžiagos šifravimas, kuris ženkliai skiriasi nuo jau realizuoto siunčiamų pranešimų šifravimo. Galima išskirti keletą pagrindinių skirtumų tarp realiu laiku perduodamos video medžiagos ir siunčiamų pranešimų:

1. Esant paketų praradimams tinkle realaus laiko video medžiagos perdavime jie pakartotinai nesiunčiami, priešingai nei siunčiamų pranešimų atveju.
2. Realaus laiko video medžiaga yra jautresnė laiko vėlinimui nei siunčiami pranešimai.

Remiantis šiais skirtumais galima teigti, jog pranešimų šifravimui naudotas kriptografinis algoritmas nėra tinkamas naudoti video informacijos šifravimui. Realaus laiko video medžiagos šifravimui reikėtų pasirinkti iš simetrinės kriptografijos srautinių šifravimo algoritmų. Nuo 2004 iki 2008 metų buvo ieškoma naujų, saugių ir greitai veikiančių srautinių šifravimo algoritmų, šią veiklą vykdė eSTREAM projektas. Pasirinksime keletą projekte siūlomų srautinio šifravimo algoritmų ir juos palyginsime su AES. 6 lentelėje pateikiami Rabbit, Salsa20/12 ir AES šifravimo algoritmų veikimo sparta nustatyta eSTREAM atlikto tyrimo metu naudojant 128 bitų šifravimo raktus. Lentelėje pateikiamas algoritmų veikimo greitis šifruojant informacijos srautą. Tyrime buvo naudojami kompiuteriai su tokiais procesoriais:

- *Intel Pentium M (1700 MHz)*
- *AMD Athlon 64 X2 4200+ (2200 MHz)*

6 lentelė. Šifravimo algoritmų greičių palyginimas

Algoritmas	Cycles/byte		MB/s		Mbps	
	Intel	AMD	Intel	AMD	Intel	AMD
Rabbit	3,94	4,98	431,47	441,77	3451,78	3534,14
Salsa20/12	7,43	4,85	228,80	453,61	1830,42	3628,87
AES	15,97	13,39	106,45	164,30	851,60	1314,41

Atliktų matavimų duomenys buvo pateikiami dažniausiai kriptografijoje naudojamu matavimo vienetu *cycles/byte*. Norint paskaičiuoti kokį informacijos srautą megabitais per sekundę galima užšifruoti, pirmiausiai reikia pasiversti į srauto matavimo vienetus pagal šią formulę:

$$s = \frac{a}{b} * 8, kur \begin{cases} s - informacijos\ srautas\ Mbps \\ a - procesoriaus\ darbinis\ dažnis\ MHz \\ b - cycles/byte \end{cases}$$

Pagal šifravimo greitį vienareikšmiškai galima teigti, jog iš nagrinėtų algoritmų video šifravimui reikėtų naudoti *Rabbit* algoritmą. Jo šifravimo sparta praktiškai nepriklauso nuo kompiuteryje naudojamo procesoriaus tipo, ko negalima pasakyti apie *AES* ar *Salsa20/12* algoritmus.

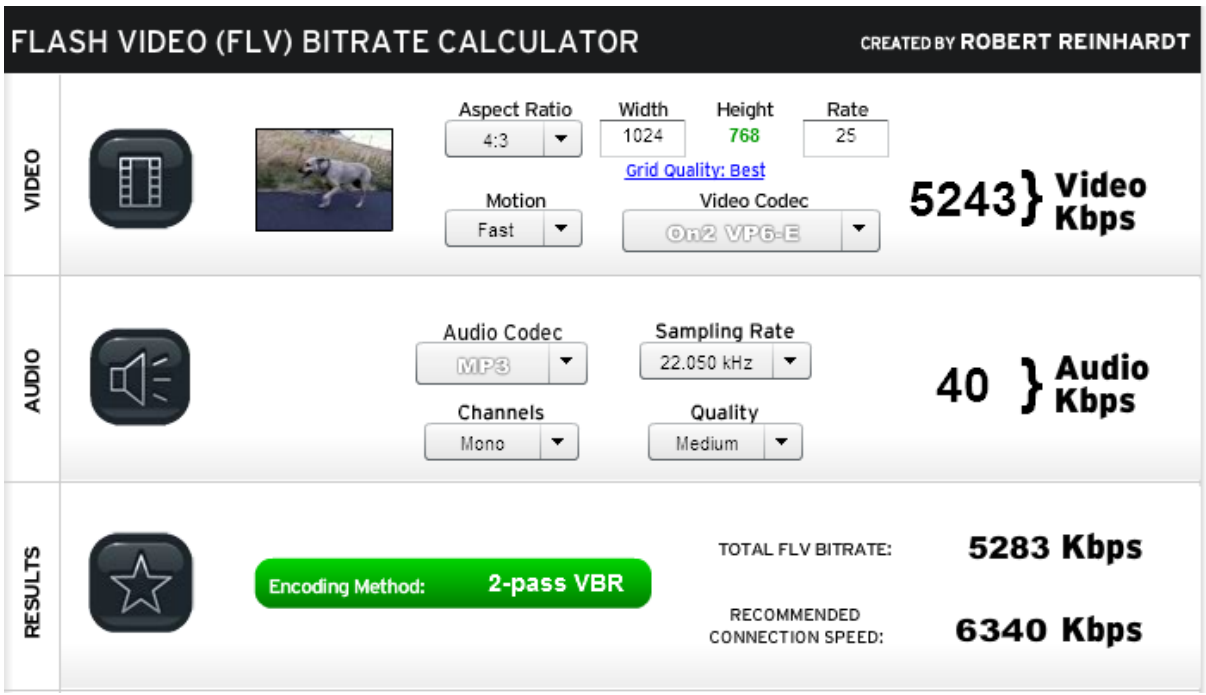
7 lentelėje pateikiami duomenys, kurie parodo koks reikalingas srautas video informacijos išsiuntimui pagal pasirinktas charakteristikas: *ekrano skiriamąją gebą* ir *transliuojamo vaizdo kitimo greitį*. *Kadrų kadrų skaičius per sekundę* ir *video kodekas* fiksuojami.

7 lentelė. Reikalingas srautas video medžiagos perdavimui

Ekrano skiriamoji geba	Kadrų skaičius per sekundę	Transliuojamo vaizdo kitimo greitis	Reikalingas minimalus srautas video išsiuntimui
640x480	25	Žemas	662 Kbps
		Vidutinis	1277 Kbps
		Aukštas	2506 Kbps
1024x768	25	Žemas	1621 Kbps
		Vidutinis	3193 Kbps
		Aukštas	6340 Kbps
1280x960	25	Žemas	2506 Kbps
		Vidutinis	4963 Kbps
		Aukštas	9878 Kbps
1920x1080	25	Žemas	4195 Kbps
		Vidutinis	8342 Kbps
		Aukštas	16637 Kbps

Atliktuose skaičiavimuose nėra įvertinamos video medžiagą transliuojančio serverio papildomos apkrovos, dėl ko aptarnaujamų klientų skaičius gali skirtis nuo apskaičiuoto. Skaičiavimams buvo naudojama speciali skaičiuoklė (21 pav.).

Šiuolaikiniai tinklai jau suteikia interneto greitaveiką iki 1 Gbps, o tai reiškia, jog pagal apskaičiuotus duomenis vienas video serveris galėtų aptarnauti nuo 60 (kuomet transliuojama 1920x1080 skiriamosios gebos su aukšta vaizdo kitimo sparta) iki 1500, (kuomet transliuojama 640x480 skiriamosios gebos su žema vaizdo kitimo sparta) vartotojų. Minėti skaičiavimai atlikti, kai video informacijos šifravimas neatliekamas. Pagal apskaičiuotus srautinio šifravimo algoritmų veikimo greičius jie turėtų įtakos aptarnaujamų klientų skaičiui tuo atveju, kai interneto linijų sparta sieks 10 Gbps. Nustatytas *Rabbit* veikimo greitis srauto šifravimo metu siekia 3,5 Gbps.



21 pav. Video medžiagos perdavimui reikalingo srauto skaičiuoklė

IŠVADOS

1. Atliekant egzistuojančių video paskaitų sistemų analizę nustatyti pagrindiniai jų trūkumai:
    - Analizuotose sistemose vartotojų autentifikavimas vykdomas remiantis vartotojo vardo ir slaptažodžio metodu, pateikiamos informacijos apsauga – nenumatyta.
    - Dėstytojams nenumatyta galimybė realiu laiku keisti dėstomos medžiagos turinį.
2. Autentifikavimo ir pateikiamos informacijos apsaugos problemoms spręsti buvo nagrinėjami kriptografiniai metodai, kurie geriausiai užtikrintų norimą saugumo lygį. Atlikta kriptografinių metodų analizė parodė, jog vartotojų autentifikavimui rekomenduojama naudoti e. parašą, o pateikiamos informacijos apsaugai – AES simetrinį šifravimo algoritmą. Darbe naudotas e. parašas gautas iš KTU sertifikatų centro
3. Realizavus siūlomą autentifikavimo metodą paremtą e. parašu buvo atliekamas tyrimas, kuriame lyginamas e. parašo autentifikavimo greitis su vartotojo vardo ir slaptažodžio autentifikavimo greičiu. Tyrimo metu nustatyta, kad vartotojo vardo ir slaptažodžio autentifikavimas greitesnis nuo 50 iki 150 kartų lyginant su e. parašu. Verta akcentuoti, kad vartotojo vardo ir slaptažodžio autentifikavimas saugumo prasme negali būti sulyginamas su autentifikavimu naudojant e. parašą.
4. Darbe sukurtas „E. parašo taikymo autentifikavimui ir šifravimui video paskaitų sistemoje“ modelis naudojamas „Audio – video nuotolinio mokymo ir egzaminavimo sistemoje“. Modelis kartu su sistema pristatytas universiteto jaunųjų mokslininkų darbų parodoje - konkurse KTU „Technorama 2010“ ir laimėjo I vietą (žiūrėti Priedą Nr.1).
5. Darbe buvo realizuotos tokios funkcijos:
    - Vartotojų autentifikacija e. parašu.
    - Vartotojų siunčiamų pranešimų šifravimas.
    - Galimybė transliuoti kompiuterio ekrano vaizdą, taip suteikiant dėstytojams galimybę realiu laiku vykdomos paskaitos medžiagą keisti pagal savo poreikius, pasitelkiant ir internetinius resursus.

Sukurtas e. parašo autentifikavimo ir šifravimo modelis gali būti tobulinamas. Rekomenduojami tobulinimai:

- Autentifikuota prieiga prie video medžiagos archyvų, apsaugant nuo neteisėto jos panaudojimo.
- Realiu laiku perduodamos video medžiagos šifravimas.

LITERATŪRA

1. Adobe Systems Incorporated. *Adobe® Flash® Media Server 3.5 Technical white paper* [interaktyvus] [žiūrėta 2009-12-14]. Prieiga per internetą: <http://www.adobe.com/products/flashmediaserver/pdfs/fms3_5_wp_ue.pdf>
2. Biometric Consortium, *Introduction to biometrics*, [interaktyvus] [žiūrėta 2009-05-12]. Prieiga per internetą: <http://www.biometrics.org/html/introduction.html>.
3. *Distancinio centro sukurta ViPS sistema populiari ne tik KTU* [interaktyvus] [žiūrėta 2008-11-12]. Prieiga per internetą: <http://www.ktu.lt/lt/apie_renginius/issamiau_.asp?page=&id=126>.
4. *Elluminate Live* [interaktyvus] [žiūrėta 2008-11-11] Prieiga per internetą: <http://www.elluminate.com/Resources/White_Papers/?id=95>
5. *Encryption Algorithms* [interaktyvus] [žiūrėta 2009-04-10] Prieiga per internetą: <http://www.jetico.com/bc8_web_help/html/02_basic_concepts/05_encryption_algorithms.htm>.
6. *Encryption Algorithms* [interaktyvus] [žiūrėta 2009-04-11] Prieiga per internetą: <http://www.mycrypto.net/encryption/crypto_algorithms.html>.
7. *Interneto konferencijos* [interaktyvus] [žiūrėta 2008-11-11]. Prieiga per internetą: <http://www.elipsis.lt/index.php?id=45>.
8. *Kriptografija* [interaktyvus] [žiūrėta 2009-01-10]. Prieiga per Internetą: <http://www.hakeriai.lt/articles.php?id=8203>.
9. MAO, W Modern Cryptography: Theory and Practice. New Jersey, 2003 ISBN: 0-13-066943-1
10. OPPLIGER, R *Contemporary Cryptography.* Norwood, 2005. ISBN 1-58053-642
11. SAKALAUSKAS, E. et al. *Kriptografinės sistemos*. Kaunas, 2008
12. SARR, Augustin P., et al. *A Secure and Efficient Authenticated Diffie–Hellman Protocol.* [interaktyvus] [žiūrėta 2009-04-25] Prieiga per internetą <http://eprint.iacr.org/2009/408.pdf>
13. ST DENIS, T ir JOHNSON, S. *Cryptography for developers.* Rockland, 2006 ISBN-13: 978-1-59749-104-4
14. STALLINGS, W. *Cryptography and Network Security Principles and Practices, 4th Edition.* 2005 Print ISBN-13: 978-0-13-187316-2
15. *Synchronous eLearning* [interaktyvus] [žiūrėta 2008-11-18]. Prieiga per internetą: <http://www.ecollege.com/Synchronous_eLearning.learn>.

16. TALBOT, J. ir WELSH, D. *Complexity and Cryptography – An Introduction*. Cambridge, 2006 ISBN-13: 9780521852319
17. *Techniques in Cryptography* [interaktyvus] [žiūrėta 2009-05-10] Prieiga per internetą: <http://www.rsa.com/rsalabs/node.asp?id=2212>.
18. *Web conferencing products and solutions* [interaktyvus] [žiūrėta 2008-11-17]. Prieiga per internetą: <http://www.tandberg.com/collateral/product_brochures/TANDBERG_web_conferencing.pdf>.
19. *What is Diffie-Hellman?* [žiūrėta 2009-04-15] Prieiga per internetą: <http://www.rsa.com/rsalabs/node.asp?id=2248>.
20. WOODWARD, J. et al. *Biometrics*. Berkeley, 2003 Prieiga per internetą: <http://books.google.lt>.

AUTHENTICATION AND ENCRYPTION USING DIGITAL SIGNATURE IN VIDEO LECTURE SYSTEM

SUMMARY

Distance learning is not a modern invention. It was started to be organized sufficiently a long time ago, using technology that existed at the time. When the technologies of communication were being developed the distance learning was being improved too. Modern communication technology allows you to organize video lectures and that's why the systems of video lectures are created. . After the analysis of existing video lectures systems, several issues have been raised:

- low security level of the proposed information;
- not given access to the teachers to modify the content of teaching materials in real time.

For the solution of the problems the model of the system is suggested which focuses on the authentication of the user by the e. signature and the encryption of the given information. These problems have been successfully solved by using popular and secure cryptographic algorithms. Designed system is successfully tested, and, after a pilot study was found that the functionality of the system is as good as the standard lectures.

1 PRIEDAS. KTU „Technorama 2010“ diplomas