KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACINIŲ SISTEMŲ INŽINERIJOS STUDIJŲ PROGRAMA

HENRIKAS LABANAUSKAS

DALINIO FAILŲ ŠIFRAVIMO PERNEŠAMOSE LAIKMENOSE GALIMYBIŲ TYRIMAS

Magistro darbas

Darbo vadovas
Dr. Armantas Ostreika

KAUNAS, 2014

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACINIŲ SISTEMŲ INŽINERIJOS STUDIJŲ PROGRAMA

HENRIKAS LABANAUSKAS

DALINIO FAILŲ ŠIFRAVIMO PERNEŠAMOSE LAIKMENOSE GALIMYBIŲ TYRIMAS

Magistro darbas

Darbo vadovas:
Dr. Armantas Ostreika
2014-05-

Recenzentas:
Dr. Šarūnas Packevičius
2014-05-

Atliko:
IFM-2/1 gr. studentas
Henrikas Labanauskas
2014-05-

KAUNAS, 2014

AUTORIŲ GARANTINIS RAŠTAS DĖL PATEIKIAMO KŪRINIO

2014 - 05 - 23 d.
Kaunas

Autoriai, Henrikas Labanauskas
patvirtina, kad Kauno technologijos universitetui pateiktas baigiamasis magistro (toliau vadinama - Kūrinys) Dalinio failų šifravimo pernešamose laikmenose galimybių tyrimas.

pagal Lietuvos Respublikos autorių ir gretutinių teisių įstatymą yra originalus ir užtikrina, kad

1) jį sukūrė ir parašė Kūrinyje įvardyti autoriai;
2) Kūrinys nėra ir nebus įteiktas kitoms institucijoms (universitetams) (tiek lietuvių, tiek užsienio kalba);
3) Kūrinyje nėra teiginių, neatitinkančių tikrovės, ar medžiagos, kuri galėtų pažeisti kito fizinio ar juridinio asmens intelektinės nuosavybės teises, leidėjų bei finansuotojų reikalavimus ir sąlygas;
4) visi Kūrinyje naudojami šaltiniai yra cituojami (su nuoroda į pirminį šaltinį ir autorių);
5) neprieštarauja dėl Kūrinio platinimo visomis oficialiomis sklaidos priemonėmis.
6) atlygins Kauno technologijos universitetui ir tretiesiems asmenims žalą ir nuostolius, atsiradusius dėl pažeidimų, susijusių su aukščiau išvardintų Autorių garantijų nesilaikymu;
7) Autoriai už šiame rašte pateiktos informacijos teisingumą atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Autorius
Henrikas Labanauskas _____
(parašas)

Dalinio failų šifravimo pernešamose laikmenose galimybių tyrimas

Santrauka

Dalinis failų šifravimas – tai failų šifravimas neužšifruojant viso failo, taip taupant techninius resursus ir sumažinant šifravimo laiką. Praktikoje dalinis failų šifravimas pernešamose laikmenose gali būti pritaikomas asmeniniam naudojimui, taip pat ir komercinėje veikloje kurioje reikia šifruoti duomenis į pernešamas laikmenas, taip pat pirminiam šifravimui kai informacija šifruojama dažnai ir greitis yra labai svarbus. Šiame darbe yra tiriamas dažnai sutinkamų failų tipų tinkamumas daliniam šifravimui, kiek duomenų reikia užšifruoti, jog failas nebūtų greitai atkurtas pasinaudojus viešai prieinama programine įranga. Atliekami greičio testai tarp dalinio ir pilno šifravimo nustatyti ar dalinis šifravimas duoda apčiuopiamą naudą. Darbe išsikeltų tikslų pasiekimui yra realizuota testavimo sistema kuri leidžia nesunkiai pilnai ir dalinai šifruoti failus sekantu operacijų laiką. Darbo pabaigoje aptariami tinkami failų tipai daliniam šifravimui, testavimo rezultatai ir išvados. Šiame darbe atlikti tyrimai parodė, jog dalinis failų šifravimas dideliems neatkuriamiems failų tipams gali sumažinti šifravimo laiką lyginant su pilnu šifravimu.

Investigation of partial encryption of files in removable media

Summary

Partial fail encryption - it's the encryption method that doesn't encrypt the whole file, that way saving technical resources and time for encryption. In practice partial fail encryption in removable media can be used for personal usage, also in commercial practice when it is required to encrypt data to removable media, also for initial encryption when data is being constantly encrypted and speed is a very important manner. This work examines regularly encountered files types compatibility for partial encryption and how much data it is required to finish the encryption, so it couldn't be decrypted by using publicly available software. Speed tests were made between partial and full encryption methods to diagnose if partial encryption has any real benefit. To accomplish set goals for this work, a testing system was established, which allows to encrypt files fully and partially by tracking operations time. By the end of the work it is discussed about compatible files types for partial encryption, test results and conclusion. The examinations made in this work, proven that partial encryption for bigger undecryptable file types can save time compared to full encryption method.

Turinys

LENTELIŲ SĄRAŠAS

PAVEIKSLIUKŲ SĄRAŠAS

Terminų ir santrumpų žodynėlis

DES	(angl. Data Encryption Standard) Duomenų šifravimo standartas
AES	(angl. Advanced Encryption Standard) Pažangesnis už DES šifravimo standartas
Brute Force	Slaptažodių nulaužimo technika perrinkant visus įmanomus slaptažodžius
XLSX	„Microsoft Office“ naudojamas formatas „Excel“ programoje
DOCX	„Microsoft Office“ naudojamas formatas „Word“ programoje
RAR	Populiarus failų archyvavimo formatas
JPG	Efektyvus grafinių failų suspaudimo formatas
PNG	Grafinių failų formatas kuris suglaudina failą be nuostolių
UML	(angl. Unified Modeling Language) Vieninga modeliavimo ir specifikacijų kūrimo kalba

1. ĮVADAS

1.1 TYRIMO PROBLEMATIKA

Duomenų šifravimo poreikis kilo dar prieš mūsų erą. Daugelį metų žinučių, laiškų ir kitos informacijos šifravimo poreikis iš karinės pusės. Dabartiniais kompiuterių laikais, šifravimas kaip ir duomenų apsauga įgavo didžiulį poreikį. Dar prieš 10 metų duomenis šifruodavo tik valstybinės institucijos, didelės korporacijos ar fanatikai. Šiomis dienomis tai tapo labai įprastu reiškiniu daugelio vartotojų tarpe.

Informaciją šiais laikais dažniausiais perduodama dvejais kanalais internetu ir pernešamosiomis laikmenomis. Pernešamos laikmenos dažniau naudojamos dideliems failams, tokiems kaip filmai, žaidimai, audio kolekcijos ir t.t. Pernešamos laikmenos užtikrina didesnį perdavimo greitį ir patikimumą. Norint apsaugoti duomenis nuo nepageidaujamos peržiūros ir naudojimo, duomenis reikia apsaugoti – užšifruoti.

Speciali programinė įranga užšifruoja ar blokuoja priėjimą prie informacijos taip apsaugant ją nuo nepageidaujamų akių. Tačiau tuo pačiu vartotojui norint įprastai naudotis užkoduotą informaciją, ją reikia užkoduoti, atkoduoti, leisti vartotojui modifikuoti informaciją ir vėl ją užkoduoti. Visi šie procesai užima laiko, ypač tai pasijaučia jeigu dirbama su dideliais failais ar informacija įrašoma ar skaitoma dažnais intervalais.

1.2 TYRIMO UŽDAVINIAI

Šiame išsikelti tokie uždaviniai:

- Išanalizuoti naudojamus algoritmus duomenų šifravimui, jų privalumus ir trūkumus.
- Atlikti dalinių failų šifravimo analizę
- Ištirti failų tipus kurie yra tinkami daliniam šifravimui
- Sukurti sistemą kuri leistų ištestuoti failų tipus
- Apibendrinti surinktą informaciją

2. Failų šifravimo pernešamose laikmenose galimybių analizė

2.1 ANALIZĖS TIKSLAS

Analizės tikslas yra išanalizuoti pagrindinius naudojamus algoritmus skirtus duomenims užšifruoti. Algoritmų analizėje atkreipiamas dėmesys į algoritmų spartą, saugumą ir realų panaudojimą. Gauti rezultatai panaudoti kuriant dalinio failų šifravimo prototipą ir atliekant testavimą.

2.2 ANALIZĖS SRITIS IR PROBLEMA

Analizuojami duomenų apsaugojimo metodai pernešamose laikmenose. Esant dideliam duomenų migravimui retai susimąstoma apie jų saugumą. Šiuolaikiniai kompiuteriai ir saugūs šifravimo algoritmai leidžia pakankamai greitai ir saugiai užšifruoti didelius duomenų kiekius. Vis gi šifruojant dažnai ir didelius informacijos kiekius pernešamose laikmenose susiduriama su skaitymo ir įrašymo sulėtėjimo dėl šifravimo ar dešifravimo procesų.

2.3 ANALIZĖS UŽDAVINIAI

Išanalizuoti esančius ir dažniausiai sutinkamus šifravimo algoritmus. Atlikti dalinio failų šifravimo ir realaus pritaikymo analizę. Panaudojant gautus rezultatus sukurti prototipą, kuris leistų realiai išbandyti dalinį failų šifravimą.

2.4 TYRIMO PLANAS

1. Šifravimo algoritmų analizė.
2. Dalinio failų šifravimo esamų sprendimų analizė.
3. Failų tipų kurie yra tinkami naudoti daliniam šifravimui analizė.
4. Reikalavimų kūrimas: naudojamiems algoritmams, metodams ir prototipui skirtam daliniam failų šifravimui.
5. Prototipo kūrimas kuris realizuotų pasirinktus metodus ir algoritmus.
6. Prototipo testavimas, metodų efektyvumo tyrimas.
7. Informacijos apibendrinimas baigiamajame darbe.

2.5 ANALIZĖS METODAI

Analizėje bus atlikta šifravimo algoritmų analizė kurioje bus išsirinktas algoritmas kuris šiuo metu yra laikomas saugiu, taip pat bus kreipiamas dėmesys į algoritmo spartą, bei reikalingų resursų kiekį užšifruojant ir atšifruojant duomenis. Atliekant failų tipų analizę, kurie yra tinkami daliniam failų šifravimui bus taikomas eksperimento metodas, kuris leis nustatyti ar failas gali būti atkurtas po dalinio užšifravimo ar ne. Apjungus gautą analizės metu informacija bus sukurtas prototipas, kuris su pasirinktu šifravimo algoritmu ir failų tipais atliks testavimą nustatyti dalinio failų šifravimo efektyvumą.

2.6 DARBO SPECIFIKACIJA

2.6.1 Duomenų apsauga

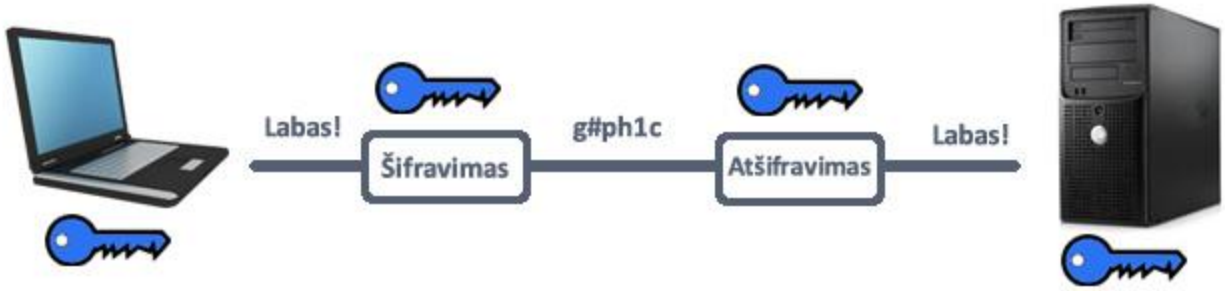
Pasitelkiant šifravimo algoritmus ir programinę įrangą galima nesudėtingai užšifruoti pernešamą laikmeną su pasirinktais saugumo kriterijais. Tačiau, jeigu tenka dažnai šifruoti arba šifruoti didelius duomenų failus tai užima daug laiko ir resursų. Todėl natūraliai kyla poreikis sumažinti resursų ir laiko sunaudojimą apsaugant duomenis.

2.6.2 Šifravimas

Duomenų apsauga yra pasiekiama naudojant šifravimo metodus, kurie yra skirstomi į dvi rūšis: simetriniai ir asimetriniai. Simetriniai šifravimo metodai – tai tokie metodai, kuriuose naudojamas vienas slaptas (abiem pusėm žinomas) raktas. Asimetriniuose šifravimo metoduose naudojami du raktai: viešas (skirtas informacijai užkoduoti) ir slaptas (skirtas informacijai atkoduoti). Tik panaudojant privatų raktą galima iššifruoti viešu raktu užšifruotą informaciją ir atvirkščiai. Dideliems duomenų srautams tinkamesni yra simetriniai šifravimo metodai, tuo tarpu asimetrinių šifravimo metodai pasireiškia kai reikia užšifruoti nedidelį kiekį informacijos, pavyzdžiui autentifikacijoje ar apsikeičiant slaptu šifravimo raktu.

2.6.3 Simetrinis šifravimas

Simetrinis šifravimas dar yra žinomas kaip bendro rakto ar bendros paslapties šifravimas. Simetriniame šifravime naudojamas vienas raktas tiek užšifruoti tiek atšifruoti informacijai. 2.1 paveikslėlyje pavaizduota kaip vartotojas A (kompiuteris) užšifruoja žinutę su raktu, gauna šifruotą žinutę (angl. ciphertext) ir vartotojas B (serveris) iššifruoja žinutę su tokiu pačiu raktu.

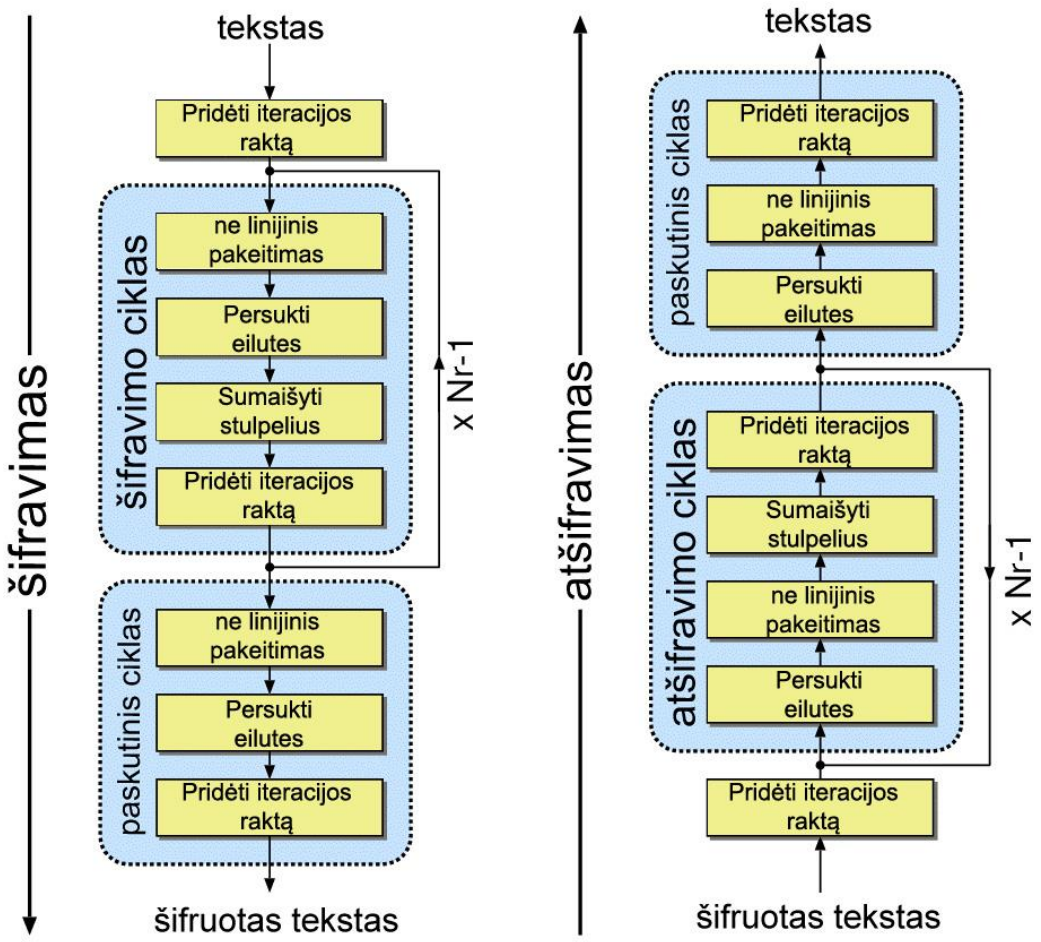


2.1 pav. Simetrinis šifravimas

Patys žinomiausi simetrinio šifravimo algoritmai yra DES, 3DES, AES ir RC4. Simetriniai šifravimo algoritmai gali būti labai greiti ir sąlyginai mažas jų sudėtingumas leidžia nesunkiai pritaikyti techninėje įrangoje. Vis dėlto, šie algoritmai reikalauja, kad visi nariai dalyvaujantis šifravime būtų taip sukonfigūruoti, jog žinotų slaptą raktą. Nors šie algoritmai gali būti labai saugūs, jie gali būti nulaužti pasinaudojus perrinkimo (angl. brute-force) metodais.

2.6.3.1 AES

AES (Advanced Encryption Standard) - dar kitaip vadinamas Rijndael algoritmu yra simetrinio šifravimo algoritmas kuris pakeitė pasenusį DES algoritmą. AES turi fiksuotą 128 bitų bloko ilgį ir 128, 192 arba 256 bitų šifravimo raktus. Atitinkamai nuo rakto ilgio, tiek ciklų yra daroma užšifruojant ir atšifruojant informaciją. 128 bitų raktas - 10 ciklų ir 4x4 dydžio matrica stulpelių sumaišymui, 192 bitų raktas - 12 ciklų ir 4x6 dydžio matrica stulpelių sumaišymui, 256 bitų raktas – 14 ciklų ir 4x8 dydžio matrica stulpelių sumaišymui. „SubBytes“ komandai naudojama sugeneruotos lentelės kurios vadinamos „S-Box“.



2.1 pav. AES algoritmas

Šifravimo metu į algoritmą perduodamas tekstas, vykdomas ciklų kiekis priklauso nuo rakto ilgio ir paskutinis ciklas skiriasi nuo visų kitų. Pagal tokią tvarką vyksta šifravimas:

1. Rakto išskleidimas - ciklų raktai gaunami pagal Rijndael apskaičiuotą lentelę.
2. Pradinis ciklas
   a. Pridėti iteracijos raktą – kiekvienas teksto baitas yra sujungiamas su ciklo raktu naudojant XOR komandą.
3. Ciklai
   a. Ne linijinis pakeitimas – ne linijinis pakeitimas, kur kiekvienas baitas yra pakeičiamas reikšme iš „S-Box“ lentelės.
   b. Persukti eilutes - perkėlimo žingsnis, kiekviena eilė yra persukama pagal nustatytą baitų skaičių. Nulinė eilutė nesukama, pirmoji – vienu baitu, antroji – dviem, trečioji – trimis baitais.
   c. Sumaišyti stulpelius - sumaišymo operacija, stulpelis sudauginamas su iš anksto nustatyta matrica kuri priklauso nuo rakto ilgio. 128 bitų rakto ilgio matrica (žr 2.2 pav.)

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

2.2 pav. MixColumns matrica

d. Pridėti iteracijos raktą – kiekvienas teksto baitas yra sujungiamas su ciklo raktu naudojant XOR komandą.

Paskutinis ciklas (nėra Sumaišyti stulpelius operacijos)

1. Ne linijinis pakeitimas
2. Persukti eilutes
3. Pridėti iteracijos raktą

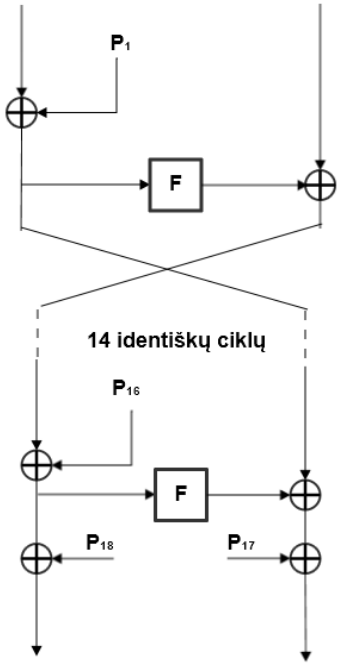
AES algoritmas yra laikomas saugiu, o naudojant 192 ir 256 bitų raktus laikomas ypatingai saugiu kadangi yra sudaroma atitinkamai 3.4×10^{38} ir 1.1×10^{77} kombinacijų, tokiam skaičiui kombinacijų nulaužti net ir su superkompiuteriu prireiktų milijonų metų. Tokie saugumo įvertinimai gauti iš JAV saugumo departamento ir AES šifravimas yra taikomas net ir aukščiausiuose lygmenyse.

AES standartiškai naudoja 128 bitų blokus, kurie yra du kartus didesni nei DES. AES turi nesudėtingą struktūrą, didelį greitį, nerasta jokių silpnųjų raktų, o galimybė padidinti rakto ilgį šį algoritmą išlaikys saugiu dar ilgą laiką.

2.6.3.2 Blowfish

Blowfish (žr. 2.3 pav.) yra simetrinis, blokinis algoritmas paremtas Feistelio struktūra, kuris turi didelę šifravimo spartą ir yra atsparus kryptoanalitinėm atakom. Blowfish buvo vienas pirmųjų blokinių šifravimo algoritmų kuris neturėjo sąsajų su patentuota informacija, yra nemokamas ir laisvai prieinamas kiekvienas norinčiam, tai sąlygojo šio algoritmo populiarumą. Visgi algoritmas turi keletą trukumų, yra atrasta silpnųjų raktų kurie įtakoja algoritmo stiprumą ir jeigu dažnai yra keičiami šifravimo raktai tai šis algoritmas veikia lėčiau nei analogiški. Blowfish duomenis šifruoja imdamas po 64 bitų blokus, rakto ilgis yra kintamas nuo 32 iki 448 bitų. Informacijos užkodavimą sudaro 16 etapų, imamą 32 bitų kairioji dalis (iš 64 bitų bloko) ir atliekami veiksmai:

1. Kairiosios dalies bitai sudedami, su operacija mod 2, su einamo ciklo i, rakto P_i bitais. Gautas rezultatas yra įrašomas į kairiąja bloko pusę.
2. Kairysis blokas apdorojamas funkcija F bei operacija mod 2, rezultatas sudedamas su dešiniąja bloko puse.
3. Visuose cikluose, išskyrus paskutinį, kairioji ir dešinioji bloko pusės sukeičiamos vietomis.



2.3 pav. Blowfish algoritmas

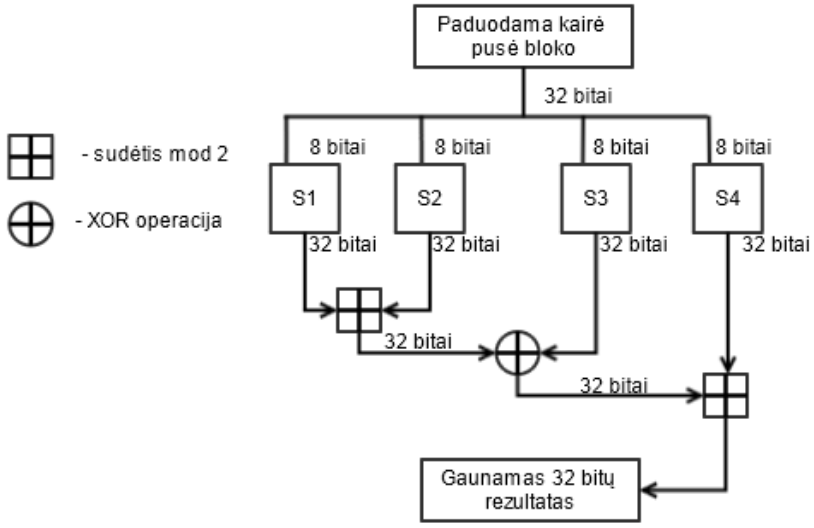
Funkcija F

1) Funkcijai paduodamas 32 bitų blokas, kuris skaidomas į keturias sekas po 8 bitus (a, b, c, d). Kiekviena iš sekų tampa S bloko įėjimu. Naudojami keturi S blokai kiekvienas turintis 256 reikšmes po 32 bitus. S blokų reikšmės nėra pastovios, nes priklauso nuo šifravimo rakto.

2) Pirmosios dvi S blokų S_1, S_2 sekos sudedamos su operacija mod 2^{32}.

3) Trečiasis S blokas sudedamas su rezultatu gautu antrajame žingsnyje naudojant operaciją mod 2.

4) Naudojant operaciją mod 2 sudėjus trečio žingsnio rezultatą su ketvirtu S bloku, gaunamas F funkcijos rezultatas.



2.4 pav. Funkcija F „BlowFish“ algoritme

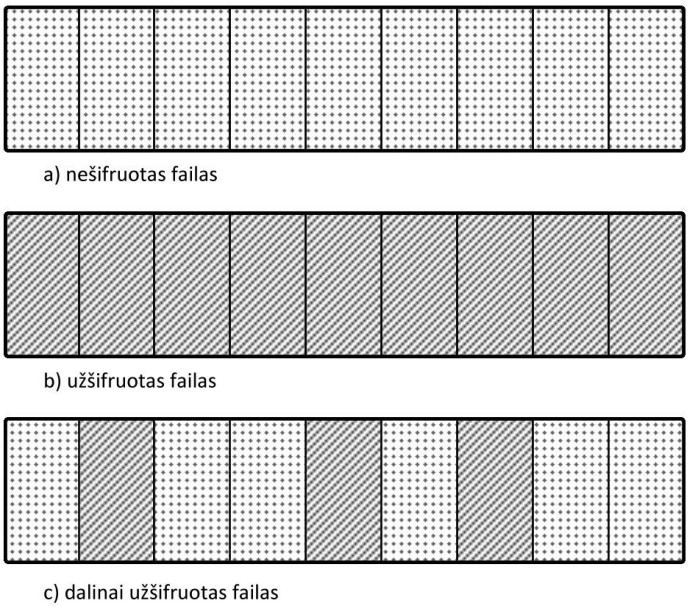
2.6.4 Apsaugos metodų pažeidžiamumai

Duomenų apsaugos metodai turi pažeidžiamumų, kai kurie yra labai sudėtingi ir reikalaujantys tam tikrų žinių ar įvykių, kiti paprasti, tačiau reikalaujantys labai daug laiko užduočiai atlikti. Labai senas ir plačiai paplitęs metodas yra visų galimų kombinacijų perrinkimas (angl. brute force). Šis

metodas yra pavojingas, kadangi turint didelį kiekį techninių resursų ir laiko galima perrinkti visus galimus slaptažodžius. Nors su vienu kompiuteriu tai padaryti būtų neįmanoma, atakų rengėjai labai nesudėtingai gali paskleisti virusą ir taip priversti labai didelį kiekį užkrėstų kompiuterių perrinkinėti slaptažodžius. Tokio tipo ataka įmanoma nulaužti DES slaptažodį per trumpą laiką. Šiuolaikiniai metodai kaip „BlowFish“ ir „AES“ yra pakankamai apsaugoti nuo tokio tipo atakų, kadangi jų raktų ilgiai gali būti ilgesni nei 128 bitai. Kadangi yra galimybė „BlowFish“ ir „AES“ algoritmuose padidinti rakto ilgį, todėl šie algoritmai yra laikomi saugiais ir nenulaužiamais dar šimtą metų.

2.6.5 Dalinis failų šifravimas

Dalinis failų šifravimas yra tik tam tikrų informacijos blokų šifravimas vietoje viso failo šifravimo (2.5 pav.). Naudojant įprastą šifravimą imamas failas nuo pradžios ir visa informacija šifruojama iki failo pabaigos, taikant dalinį šifravimą galima užšifruoti tik failo pradžia, failo pabaigą ar bet kokiu kitu norimu šablonu. Svarbiausia, jog užšifruojant ir atšifruojant būtų nuskaitomas ir naudojama tas pats informacijos blokas. Labai didelę įtaką daliniam failų šifravimui turi šifruojamo failo tipas. Kadangi vienus failus galima atidaryti ir peržiūrėti su užkoduota dalimi informacijos tai įtakoja kokią dalį failo reikia užšifruoti, jog failo nebūtų galima atkurti pasinaudojus pagalbine programine įranga.



2.5 pav. Nešifruoto, užšifruoto ir dalinai užšifruoto failo struktūra

Keletas galimų dalinio šifravimo modelių:

Failo pradžios šifravimas – šifruojant tik failo pradžią galima sumažinti šifravimo laiką, užšifruojama antraštės (angl. header) informacija, todėl sunkiau nustatyti kokio tipo tai failas. Tačiau toks šifravimas netinka tekstiniams, vaizdo ir audio failams, kadangi išmetus užšifruotą dalį ar ją pakeitus standartine antrašte galima pilnai arba dalinai atkurti failą. Šio algoritmo užšifravimo pseudo kodas aprašytas žemiau (žr. encryptFile).

```
Procedure encryptFile
// objektas bufferSize = objektas, kuris nurodo buferio dydį šifravime
// objektas crypt count = objektas, kuris nurodo kiek kartų buferis bus šifruojamas

{01}begin
{02}  Start stopwatch
{03}  Open stream for reading, writing and crypting
{04}  read data to buffer
{05}     if crypt count > cryptlenght
{06}        write buffer to file
{07}     else
{08}        white buffer to file using cryptography stream
{09}     do until end of file
{10}  Stop stopwatch
{11}end.
```

Failo vidurio šifravimas – failo vidurio šifravimas identiškas failo pradžios šifravimui, tik paliekama dar ir antraštės informacija, todėl padidėja tikimybė atkurti dalinai užšifruotą failą.

Failo pabaigos šifravimas – failo pabaigos šifravimas identiškas failo vidurio šifravimui.

Atsitiktinių blokų šifravimas – tokį šifravimą būtų galima realizuoti dvejais būdais. Pirmasis kai šifruojamas nustatytas blokas, pvz. užšifruojamas kas 20 blokas. Tokiu būdu būtų užšifruota informacija pasiskirsčiusi visame faile. Antrasis būdas yra šifruoti blokus pagal nustatytą seką, pvz. šifruoti 5, 201, 765 ir t.t blokus. Abudu būdai yra netinkami failų tipams kuriuos galima atkurti išmetus užšifruotus blokus (garso, vaizdo ir tekstiniai failai).

2.6.6 Potencialūs vartotojai

Potencialūs tokių sistemų vartotojai gali būti labai įvairūs. Paprasčiausi eiliniai vartotojai, kurie šifruoja labai dažnai arba šifruoja didelius duomenų kiekius, į pernešamąsias laikmenas tai leistų sutaupyti laiko ir resursų atliekamiems šifravimams. Pažengę vartotojai galėtų dalinį šifravimą naudoti kaip pirminį šifravimą duomenims kai dar nežinoma ar duomenys ateityje bus pilnai šifruojami ar ne, taip būtų sutaupyta laiko, o duomenys būtų apsaugoti. Dabartiniais laikais, kai labai daug informacijos yra stebima valdžios institucijų, didžiųjų interneto svetainių ar interneto tiekėjų, informacijos apsauga atrodo labai natūralus ir suprantamas dalykas tiek tarp pradedančiųjų vartotojų, tiek tarp specialistų ar įmonių.

2.6.7 Vartotojų tikslai ir problemos

Iš visų keliamų vartotojų tikslų gali būti išskirtos dvi pagrindinės kategorijos. Vartotojams svarbiausia patogumas naudojantis ir duomenų saugumas. Patogumo naudojantis programine įranga nori kiekvienas vartotojas, tačiau tai labiau orientuota į paprastus, eilinius vartotojus. Tokiems vartotojams turėtų būtį aiškiai pateiktos šifravimo galimybės, paaiškinta dalinio šifravimo privalumai ir kaip veikia pats šifravimas. Pažengusiems vartotojams ir specialistams labiau rūpi kaip duomenys yra apsaugomi, ar yra pasiekiamas norimas saugumo lygis ir ar jų svarbi informacija išliks saugi patekus į pašalinių asmenų rankas. Tik suderinus patogią, aiškią ir duomenų apsaugą, bus galima pasiekti abiejų tipų vartotojus.

2.7 ESAMŲ SPRENDIMŲ ANALIZĖ

Yra sukurta nemažai sprendimų failų šifravimui, pateikiu plačiausiai sutinkamus sprendimus.

2.7.1.1 TrueCrypt

TrueCrypt [7] viena plačiausiai naudojama programinė įranga. Pradėta leisti dar 2004 ir reguliariai atnaujinama atvirojo kodo programa yra viena populiariausia duomenų apsaugos

programų šiuo metu. Ši programinė įranga labai mėgstama pažengusių vartotojų, kadangi galima kurti atskirus šifruotus diskus ir particijas, apsaugoti jau esamus diskus ir atmintines, šifruoti informacija realiu laiku (angl. on-the-fly). Programa naudoja:

- AES, Serpent, Twofish ir Cascades šifravimo algoritmus.
- RIPEMD-160, SHA-512 ir Whirpool maišos funkcijas.

Prie sistemos trūkumų būtų galima paminėti, jog sistema nėra tinkanti pradedantiesiems vartotojams, kadangi didelis pasirinkimų skaičius ir senamadiška vartotojo sąsają apsunkina darbą. Taip pat ši programa neturi galimybės užšifruotus duomenis pririšti prie tam tikro techninės įrangos identifikacinio numerio (angl. hardware id).

2.7.1.2 BitLocker

Bitlocker [8] tai standartinė programa įtraukta į "Microsoft Windows" operacinę sistemą nuo "Vista" versijos. Ši programinė įranga užšifruoja visą diską. Pagal nutylėjimą naudojamas AES algoritmas su 128 bitų ilgio raktu, nors yra galimybė šifruoti naudojantis 256 bitų raktu. Naudojimasis Bitlocker pakankamai intuityvus ir įprastas "Windows" vartotojams, todėl ši programa labai tinkama daugeliui vartotojų, kadangi nereikia instaliuoti papildomų programų, viskas paprasta, nėra sudėtingų pasirinkimo variantų. Praktiškai pažvelgus atrodo, jog programa labai tinkama daugeliui vartotojų, tačiau pastebėta nemažai šios programos trūkumų: Palaikomos tik "Windows Ultimate" versijos, nėra šifravimo algoritmų pasirinkimo, nenaudojant papildomų apsaugos priemonių yra pažeidžiama fizinių atakų.

2.7.1.3 Dr. Falk´s Store O´Crypt

Dr. Falk´s Store O´Crypt [9] - tai kiek kitokia šifravimo programa kadangi ji jau yra įdiegta į USB atmintinę kurią reikia pirkti iš gamintojo. Store O´Crypt šifruoja duomenis AES algoritmu naudojantis 256 bitų raktą, labai nesudėtingą vartotojo sąsają. Programa kartu su USB atmintine yra geras sprendimas neieškant alternatyvų, kadangi nereikia rūpintis programine įranga, ji iškart prieinama įjungus USB atmintinę "Windows" operacinėje sistemoje. Taip pat realizuota apsauga nuo perrinkimo atakų (anga. brute force) po nustatyto kiekio neteisingų bandymų nebeleidžia daugiau įvesti slaptažodžio. Tokio tipo atmintinės tinkamos naudoti asmeniniaos tikslais ar įmonės viduje, tačiau norint pritaikyti plačiau kyla problemų. Sistema veikia tik ant "Windows" operacinės sistemos, taip pat norint naudoti ne vieną atmintinę (sakykime įmonės viduje), kaina yra apie penkis kartus didesnė nei įprastų USB atmintinių.

2.8 ESAMŲ SISTEMŲ ANALIZĖS APIBENDRINIMAS

Apsaugoti duomenims pernešamosiose laikmenose yra sukurta labai daug sprendimų. Tačiau nei vienas sprendimas nesiūlo dalinio failų šifravimo. Labiausiai paplitęs AES šifravimo algoritmas yra visiškai saugus su 192 bitų ir didesniu raktu, yra blokinis algoritmas todėl yra puikiai tinkamas naudoti daliniam šifravimui.

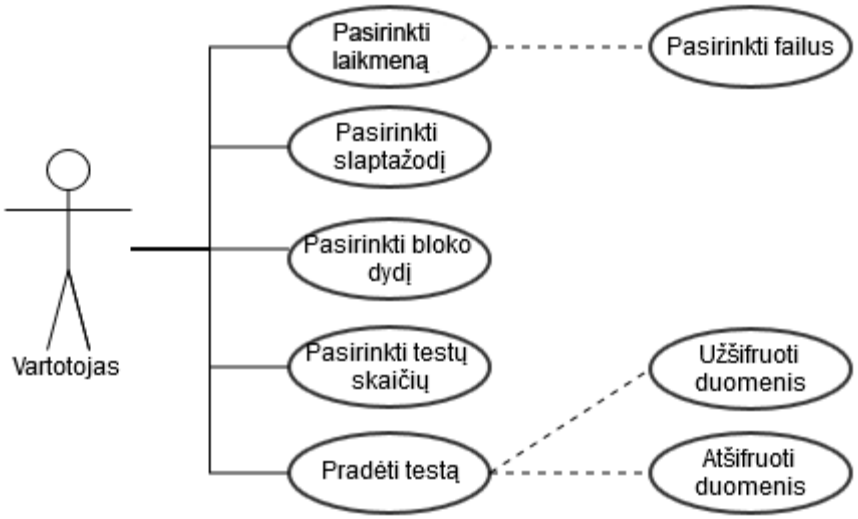
2.9 ANALIZĖS IŠVADOS

1. Nėra programos kuri leistų atlikti dalinį duomenų šifravimą.
2. Nėra žinoma kurie failų tipai yra tinkami daliniam šifravimui.
3. Atlikus sukurtų sistemų analizę pastebėta, jog duomenims apsaugoti dažniausiai naudojamas AES algoritmas su 128 arba 256 bitų raktu.

3. REIKALAVIMŲ SPECIFIKACIJA

3.1 FUNKCINIAI REIKALAVIMAI

Funkciniai reikalavimai nusako kokias paslaugas atliks sistema, kaip reaguos į įvedimo ir išvedimo duomenis, kaip sistema elgsis tam tikrose situacijose. Funkciniai reikalavimai atvaizduojami panaudos atvejų diagrama (žr. 3.1 pav.)



3.1 pav. Panaudos atvejų diagrama

3.1 lentelė. „Pasirinkti laikmeną“ panauda

Panaudojimo atvejis	**Pasirinkti laikmeną**
Aprašymas	Pasirenkama pernešama laikmena, į kurią bus įrašomi užšifruoti failai
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Paleista programa
Rezultatai	Pasirinkta pernešama laikmena kuri bus naudojama tolimesniame šifravimo etape

3.2 lentelė. „Pasirinkti failus“ panauda

Panaudojimo atvejis	**Pasirinkti failus**
Aprašymas	Pasirenkama failai, kurie bus užšifruojami ir atšifruojami
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkta laikmena
Rezultatai	Pasirinkti failai kurie bus naudojami tolimesniame šifravimo procese

3.3 lentelė. „Pasirinkti slaptažodį“ panauda

Panaudojimo atvejis	**Pasirinkti slaptažodį**
Aprašymas	Pasirenkamas slaptažodis, kuriuo bus užšifruojami duomenys
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkti failai
Rezultatai	Nustatomas slaptažodis, kuris bus naudojamas kartu su šifravimo algoritmu

3.4 lentelė. „Pasirinkti slaptažodį“ panauda

Panaudojimo atvejis	**Pasirinkti slaptažodį**
Aprašymas	Įvedamas slaptažodis, kuris tenkina minimalius reikalavimus (minimaliai 8 simboliai, tarp jų skaičiai ir raidės).
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkti šifravimo algoritmą
Rezultatai	Nustatomas slaptažodis kuris bus naudojamas kartu su šifravimo algoritmu

3.5 lentelė. „Pasirinkti bloko dydį“ panauda

Panaudojimo atvejis	**Pasirinkti bloko dydį**
Aprašymas	Pasirenkamas bloko dydis, kuris naudojamas šifravime
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkti laikmeną, pasirinkti failus, pasirinkti slaptažodį
Rezultatai	Pasirinktas bloko dydis nurodo kokio dydžio blokais informacija imama iš failo ir užšifruojama ar atšifruojama

3.6 lentelė. „Pasirinkti testų skaičių“ panauda

Panaudojimo atvejis	**Pasirinkti testų skaičių**
Aprašymas	Pasirenkamas skaičius kiek bus atliekama testų užšifruojant ir atšifruojant failus.
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkti laikmeną, pasirinkti failus, pasirinkti slaptažodį, pasirinkti bloko dydį
Rezultatai	Nurodytas testų skaičius bus vykdomas su pasirinktais failais ir bus skaičiuojamas kiekvienos operacijos laikas, taip pat ir bendras laikas kiek užtruko užšifravimas, atšifravimas

3.7 lentelė. „Pradėti testą“ panauda

Panaudojimo atvejis	**Pradėti testą**
Aprašymas	Pradedamas testavimas
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pasirinkti laikmeną, pasirinkti failus, pasirinkti slaptažodį, pasirinkti bloko dydį, pasirinkti testų skaičių
Rezultatai	Pradedamas užšifravimas ir atšifravimas su pasirinktais parametrais

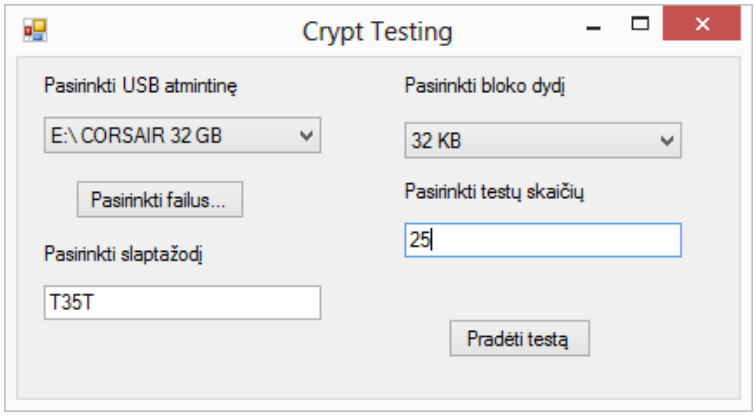
3.8 lentelė. „Užšifruoti duomenis“ panauda

Panaudojimo atvejis	**Užšifruoti duomenis**
Aprašymas	Užšifruojami duomenys
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pradėti testą
Rezultatai	Pradedamas užšifravimas su pasirinktais parametrais

3.9 lentelė. „Atšifruoti duomenis“ panauda

Panaudojimo atvejis	**Atšifruoti duomenis**
Aprašymas	Atšifruojami duomenys
Aktoriai	Sistemos vartotojas
Prieš-sąlyga	Pradėti testą
Rezultatai	Pradedamas atšifravimas su pasirinktais parametrais

Kuriamam duomenų apsaugos prototipui sukurta bandomoji vartotojo sąsaja kuri būtų nesudėtinga, tačiau leistu vartotojui pasirinkti naudojamus šifravimo parametrus ir veiktu pagal nurodytus funkcinius reikalavimus (žr. 3.2 pav.)



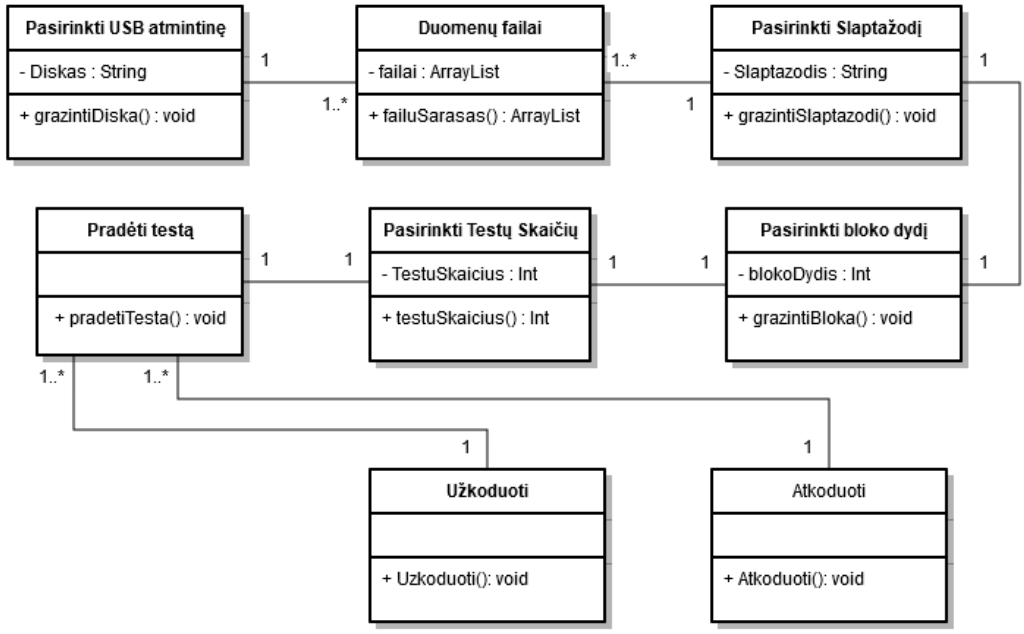
3.2 pav. Prototipo bandomoji vartotojo sąsaja

3.2 NEFUNKCINIAI REIKALAVIMAI

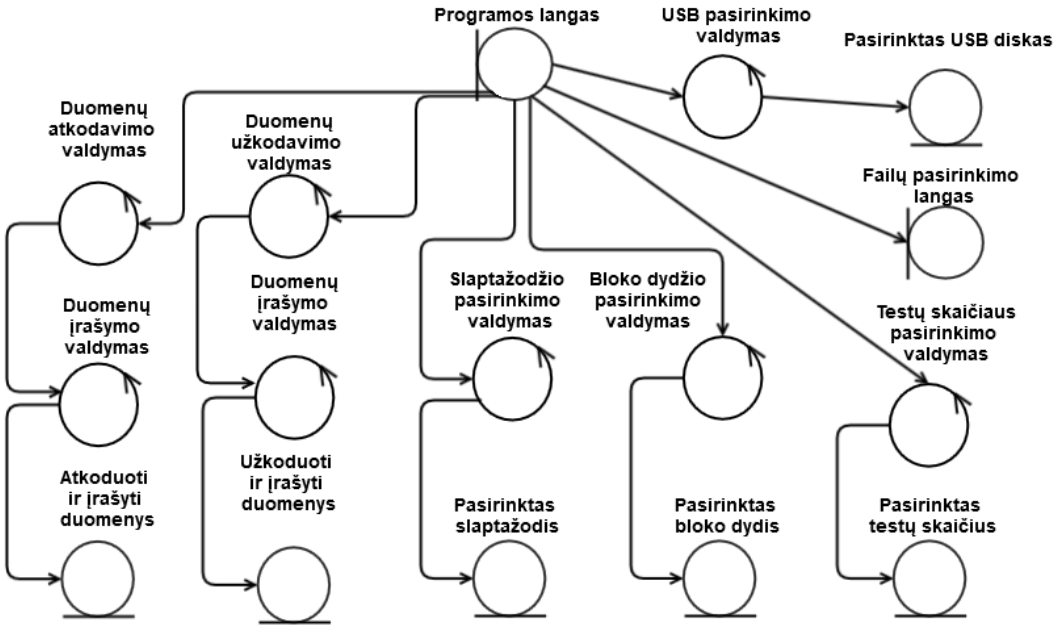
- Sistema turi veikti Windows operacinėje sistemoje.
- Sistema turi veikti patikimai, be trukdžių.
- Sistema turi turėti nesudėtingą valdymą ir šifravimo parametrų pasirinkimą.
- Sistema turi parodyti testavimo rezultatus ekrane.
- Sistema negali naudoti komercinės programinės įrangos (ar jos dalių).
- Sistema negali veikti žymiai lėčiau nei analogiškos sistemos

3.3 DALYKINĖS SRITIES MODELIS

UML diagramose atvaizduotas dalykinės srities modelis. Jis nurodo galimas sistemos klases, pagrindinius metodus. Tai nėra galutinis sistemos modelis, todėl prototipo kūrimo eigoje jis gali keistis. Ši diagrama (žr. 3.3 pav. ir 3.4 pav.) atvaizduoja ir leidžia susidaryti vaizdą apie tikėtiną sistemos architektūrą ir pagrindinius elementus.



3.3 pav. Projektuojamos sistemos klasių diagrama



3.4 pav. Projektuojamos sistemos veiksmų diagrama

3.4 REIKALAVIMŲ ANALIZĖS IŠVADOS

Atlikus reikalavimų analizę buvo sukurtas sistemos veiklos modelis. Sukurtas modelis kuriame apibrėžiami svarbiausi naudojami metodai, vartotojo ir pačios sistemos elgsena.

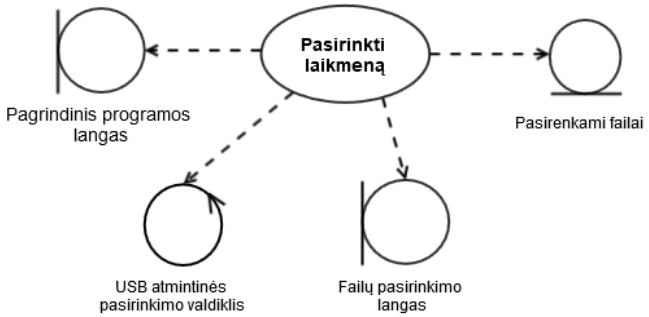
3.5 SISTEMOS APŽVALGA

Atlikus duomenų šifravimo algoritmų ir analogiškų sistemų analizę, pasirinktas šifravimo algoritmas ir funkcijos ,kurios bus naudojamos kuriamoje sistemoje. Kuriama sistema, naudos laisvai prieinamus ir nemokamus algoritmus, bus nemokama ir atvirojo kodo (angl. open source), leis vartotojui nesudėtingai užšifruoti duomenis pernešamoje laikmenoje su pasirinktu bloko dydžiu,

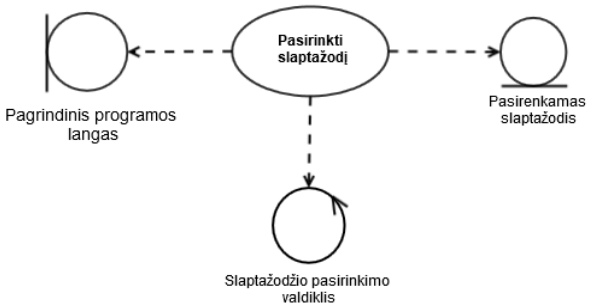
slaptažodžiu ir norimų testų skaičiumi. Sistema dirbs visose "Microsoft Windows" versijose ir norint ištestuoti duomenis nereikės įsidiegti jokios papildomos programinės įrangos.

3.6 SISTEMOS ARCHITEKTŪRA

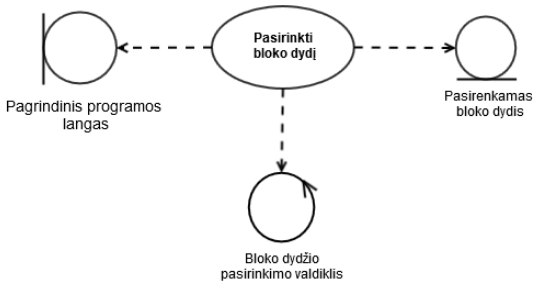
Sistemos naudos diagramose nurodomos kokios klasės ir kaip bendrauja vykdant tam tikrą panaudos atvejį. Kiekvienam panaudos atvejui yra sukuriama atskira diagrama. Žemiau parodytos diagramos šešiems sistemos panaudos atvejams.



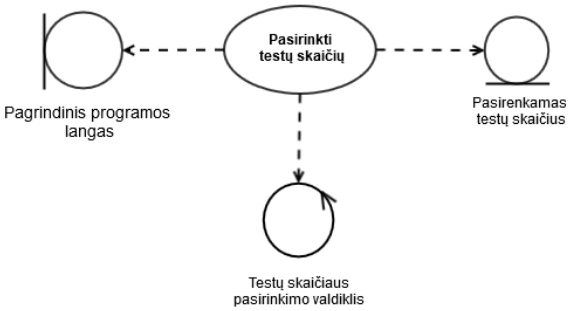
3.5 pav. Panaudos atvejo „Pasirinkti laikmeną“ analizės diagrama



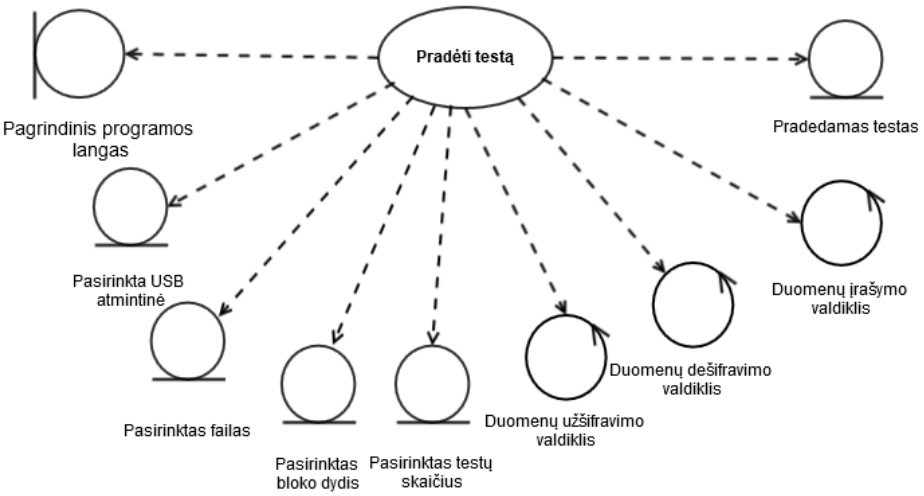
3.6 pav. Panaudos atvejo „Pasirinkti slaptažodį“ analizės diagrama



3.7 pav. Panaudos atvejo „Pasirinkti bloko dydį“ analizės diagrama



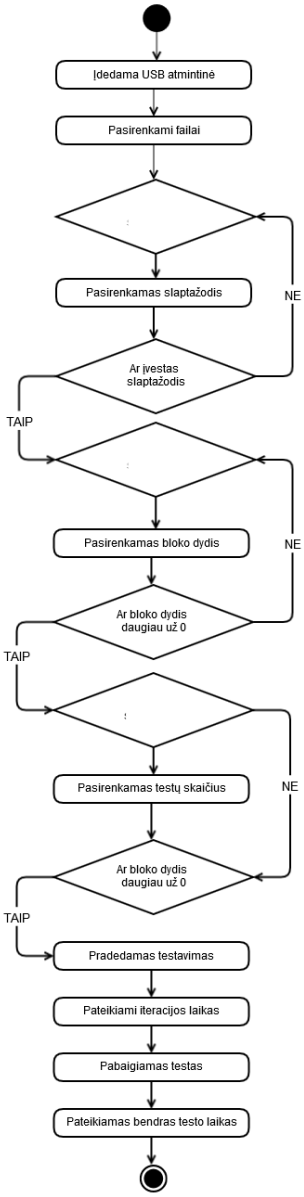
3.8 pav. Panaudos atvejo „Pasirinkti testų skaičių“ analizės diagrama



3.9 pav. Panaudos atvejo „Pradėti testą“ analizės diagrama

3.7 SISTEMOS VEIKLOS MODELIS

Kiekvieną sistemos panaudojimo atvejį galima detalizuoti vienu veiklos modeliu. Veiklos modelis atvaizduoja kokie procesai vyksta sistemoje, šis modelis aprašomas sekų ir būsenų diagramomis. Vartotojui įvedus visus reikiamus duomenis sistema dirba automatiškai. Paveikslėlyje 3.10 atvaizduojama sistemos būsenos atliekant failų dalinį apsaugojimą išmatuojant šifravimo greitį.



3.10 pav. UML veiklos diagrama

4. EKSPERIMENTINIS SISTEMOS TYRIMAS

Norint ištirti dalinio failų šifravimo naudą ir panaudojamumą buvo išsikelti du eksperimento tikslai. Pirmasis – ištirti skirtingų failų tipų atkuriamumą po užšifravimo, antrasis – pamatuoti užšifravimo ir dešifravimo greičius su pilnu ir daliniu šifravimu.

4.1 EKSPERIMENTŲ PLANAS

4.1.1 Naudojami failų tipai

Norint praktiškai panaudoti dalinį duomenų šifravimą reikia išsiaiškinti kokiems failų tipams šis šifravimas yra pritaikomas. Tam atliekama failų atkuriamumo analizė. Atliekant šią analizę testiniai failai yra dalinai užšifruojami ir bandoma atkurti pradinį failą pasitelkiant specializuotą programinę įrangą. Gavus rezultatus galima susidaryti bendrą vaizdą kokia dalis failo turėtų būti užšifruota, jog šio nebūtų įmanoma iššifruoti. Analizei pasirinkti pagrindiniai grafikos failai (JPG ir PNG), dokumentai (DOC, XLS) ir failų archyvai (RAR).

4.1.2 Testavimo eiga

Testavimas atliekamas tokia tvarka:

1. Išsirenkami skirtingų dydžių testiniai failai.
2. Sukuriamos failų kopijos kuriose užšifruojamas nustatytas informacijos kiekis pradžioje failo.
3. Specializuotos programinės įrangos pagalba bandoma atkurti užšifruotus failus.
4. Nustatomos ribos kiek reikia failo užšifruoti, jog jo nebūtų galima atkurti.
5. Nustatoma failo atkūrimas priklauso nuo failo dydžio.

4.1.3 Greičių testavimas

Greičio testui bus naudojama viena pernešama laikmena, kuri bus išjungiama ir įjungiama prieš kiekvieną testą, jog būtų sukuriamos vienodos sąlygos. Pirmiausia failas pilnai užšifruojamas nustatytą kartų kiekį, tada pamatuojamas užšifravimo, atšifravimo ir bendras laikas. Testas kartojamas su daliniu šifravimu nustatant koks kiekis informacijos bus užšifruota. Gauti laikai palyginami tarpusavyje.

4.1.4 Testavimo įranga

Visi testai atliekami su vienu kompiuteriu ir tokia pačia pernešama laikmena, norint sukūrti identiškas testavimo sąlygas.

Tyrimui atlikti buvo pasirinkta techninė bei programinė įranga aprašyta lentelėje žemiau (žr. 4.1 lentelę.).

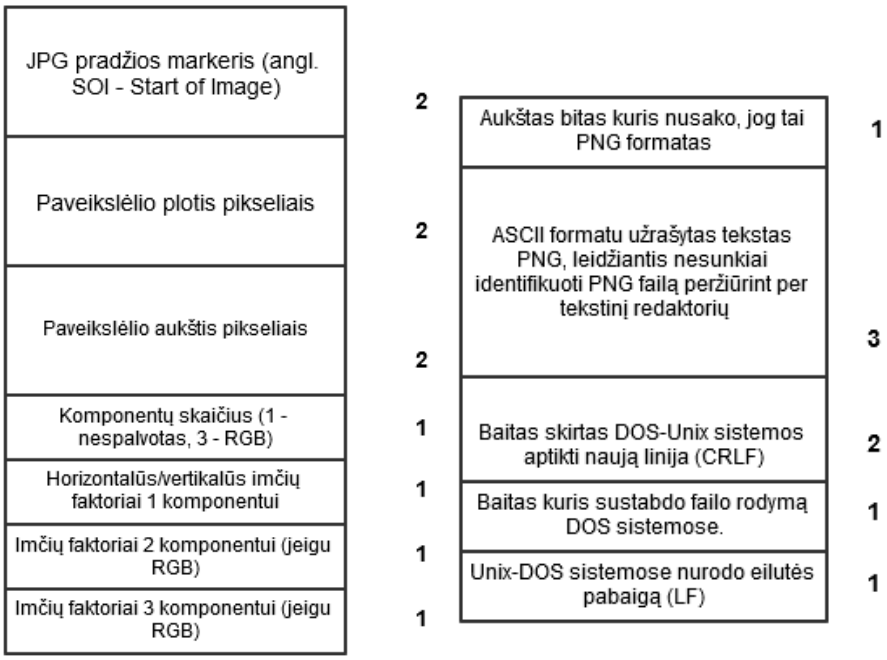
4.1 lentelė. Naudojama techninė įranga testavime

Procesorius	AMD Phenom II X4 B50 3.20 GHZ
Operatyvioji atmintis (RAM)	4 GB
Sistemos tipas	64-bitų operacinė sistema
Kietasis diskas	Western Digital 500 GB SATA2

Testuojant su kitokia techninės įrangos komplektacija, testo rezultatai gali skirtis nuo pateikiamų šiame darbe.

4.2 Eksperimentas su grafikos failais

Dėl didelio savo populiarumo grafikos failų testavimui pasirinkti JPEG ir PNG failų formatai. Testuojant pasirinkti trys skirtingo dydžio failai kiekvienam formatui. Failai bus dalinai užšifruoti ir pasitelkus grafikos failų atkūrimo įrankius bus siekiama nustatyti užšifravimo ribą nuo kurios failas tampa nebeatkuriamas. Pradžioje peržiūrima šifruojamo failo struktūra ir antraštės (angl. *header)*(žr. 4.1 pav.). Pirmasis nurodoma JPG failo antraštė, kurią sudaro 10 baitų ir PNG antraštė kurią sudaro 8 baitai. Tiriant nustatysime, ar užtenka užšifruoti tik failo antraštę, jog jis taptų nebeatkuriamas.



4.1 pav. JPG ir PNG failų antraštės

Naudojama programinė įranga

Užkoduotų JPG failų atkūrimui naudojama ši programinė įranga:

- Pix Recovery [9]
- JPEG Recovery PRO [10]
- Picture Doctor [11]

Užkoduotų PNG failų atkūrimui naudojama ši programinė įranga:

- Comfy File Repair [12]
- Pix Recovery [9]

Testiniai failai

JPG failų analizei pasirinkti trys skirtingo dydžio paveikslėliai:

a) Mažas – 606 kb dydžio
b) Vidutinis – 2961 kb dydžio
c) Didelis – 9422 kb dydžio

a) mažas b) vidutinis c) didelis

4.2 pav. Testuojami JPG paveikslėliai

PNG failų analizei pasirinkti trys skirtingo dydžio paveikslėliai:

a) Mažas – 205 kb dydžio
b) Vidutinis – 1118 kb dydžio
c) Didelis – 4953 kb dydžio

a) mažas b) vidutinis c) didelis

4.3 pav. Testuojami PNG paveikslėliai

Šifravimas

JPG testiniuose failuose užšifruota 2, 4, 8, 16 ir 32 kilobaitai informacijos paimtos iš failo pradžios. Taip iš viso gautas 15 dalinai užšifruotas JPG failas. PNG testiniuose failuose užšifruota 1, 2, 4, 8 ir 16 baitai iš failo pradžios. Taip iš viso gautas 15 dalinai užšifruotas PNG failas.

Failų atkūrimas

Užšifruotus failus bandoma atkurti, lentelėse nurodomas užšifruotas informacijos kiekis, paveikslėlio dydis ir ar pavyko atkurti failą.

JPG paveikslėlių atkūriamumo testavimas

Pix Recovery

4.2 lentelė. Pix Recovery failų atkūrimas

	Mažas paveikslėlis	Vidutinis paveikslėlis	Didelis paveikslėlis
2 kb	Taip	Taip	Taip
4 kb	Taip	Taip	Taip
8 kb	Taip	Taip	Taip
16 kb	Taip	Taip	Ne
32 kb	Ne	Ne	Ne

Pavyko atkurti 11 iš 15 failų. Nepavyko atkurti nei vieno failo užšifravus 32 kilobaitus informacijos, taip pat didelio paveikslėlio su 16 kilobaitų šifravimu.

JPEG Recovery Pro

4.3 lentelė. JPEG Recovery Pro failų atkūrimas

	Mažas paveikslėlis	Vidutinis paveikslėlis	Didelis paveikslėlis
2 kb	Taip	Taip	Taip

4 kb	Taip	Taip	Taip
8 kb	Taip	Taip	Taip
16 kb	Taip	Taip	Ne
32 kb	Ne	Ne	Ne

Pavyko atkurti 11 iš 15 failų. Nepavyko atkurti nei vieno failo užšifravus 32 kilobaitus informacijos, taip pat didelio paveikslėlio su 16 kilobaitų šifravimu.

Picture Doctor

4.4 lentelė. Picture Doctor failų atkūrimas

	Mažas paveikslėlis	Vidutinis paveikslėlis	Didelis paveikslėlis
2 kb	Taip	Taip	Taip
4 kb	Taip	Taip	Taip
8 kb	Taip	Ne	Ne
16 kb	Ne	Ne	Ne
32 kb	Ne	Ne	Ne

Pavyko atkurti 7 iš 15 failų. Tai prasčiausias rezultatas iš viso testo, kadangi pavyko atkurti tik 2 ir 4 kilobaitų užšifravimą ir mažą paveikslėlį su 8 kilobaitų šifravimu.

Ištestavus tris specializuotas programas gautas 64% atkuriamumo vidurkis ir nei vienai programai nepavyko įveikti 32 kilobaitų šifravimo.

PNG paveikslėlių atkūriamumo testavimas

Comfy File Repair

4.5 lentelė. Comfy File Repair failų atkūrimas

	Mažas paveikslėlis	Vidutinis paveikslėlis	Didelis paveikslėlis
1 baitas	Taip	Taip	Taip
2 baitai	Taip	Taip	Taip
4 baitai	Taip	Taip	Taip
8 baitai	Ne	Ne	Ne
16 baitų	Ne	Ne	Ne

Pavyko atkurti 9 iš 15 failų. Nepavyko atkurti nei vieno failo užšifravus 8 ir 16 baitų informacijos.

Pix Recovery

4.6 lentelė. Pix Recovery failų atkūrimas

	Mažas paveikslėlis	Vidutinis paveikslėlis	Didelis paveikslėlis
1 baitas	Ne	Ne	Ne
2 baitai	Ne	Ne	Ne
4 baitai	Ne	Ne	Ne
8 baitai	Ne	Ne	Ne
16 baitų	Ne	Ne	Ne

Nepavyko atkurti nei vieno failo, nors programa skelbiasi atkurianti PNG failus ir JPG atkuriamumo teste pasirodė labai gerai.

Ištestavus tik dvi specializuotas programas, kadangi programų dirbančių su PNG failais yra labai nedaug, gautas 30% atkuriamumo vidurkis. Vienintelėi „Comfy File Repair“ pavyko atkurti 1, 2 ir 4 baitų šifravimą.

Testavimo greičiai

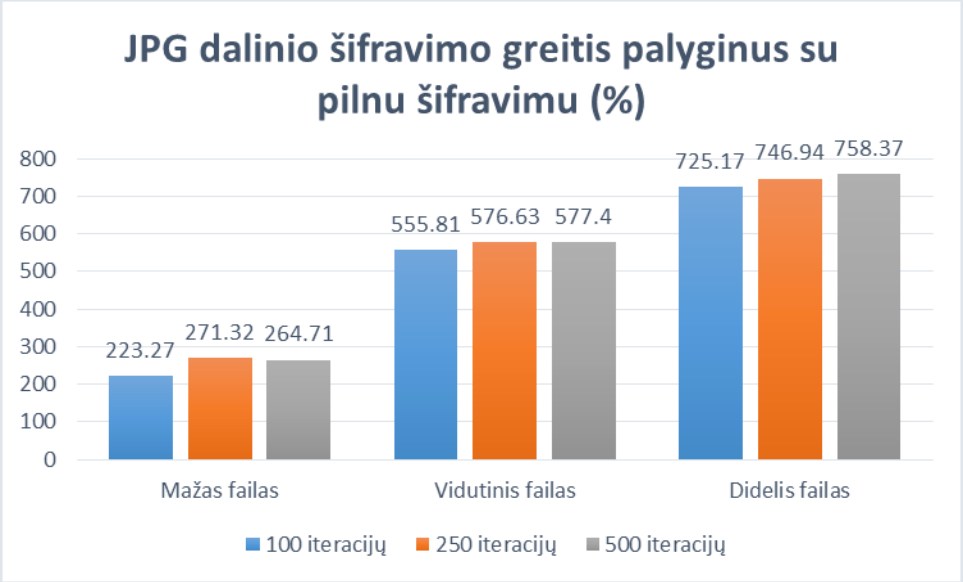
Greičio testavimui buvo pasirinkta užšifruoti 32 kilobaitus iš failo pradžios JPG failui ir 8 baitus PNG failui. Testą sudaro duomenų užšifravimas, dešifravimas kuris kartojamas 100, 250 ir 500 kartų. Laikas matuojamas milisekundėmis (ms).

JPG failų greičio testavimas

Testas atliekamas su mažu, vidutiniu ir dideliu failais.

4.7 lentelė. JPG failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

	100 kartų	250 kartų	500 kartų
Mažo failo dalinis užšifravimas	1852 ms	4065 ms	8264 ms
Mažo failo pilnas užšifravimas	5987 ms	15094 ms	30140 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	223,27 %	271,32 %	264,71 %
Vidutinio failo dalinis užšifravimas	3840 ms	9289 ms	18623 ms
Vidutinio failo pilnas užšifravimas	25183 ms	62852 ms	126153 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	555,81 %	576,63 %	577,40 %
Didelio failo dalinis užšifravimas	9318 ms	22774 ms	45037 ms
Didelio failo pilnas užšifravimas	76889 ms	192883 ms	386585 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	725,17 %	746,94 %	758,37 %



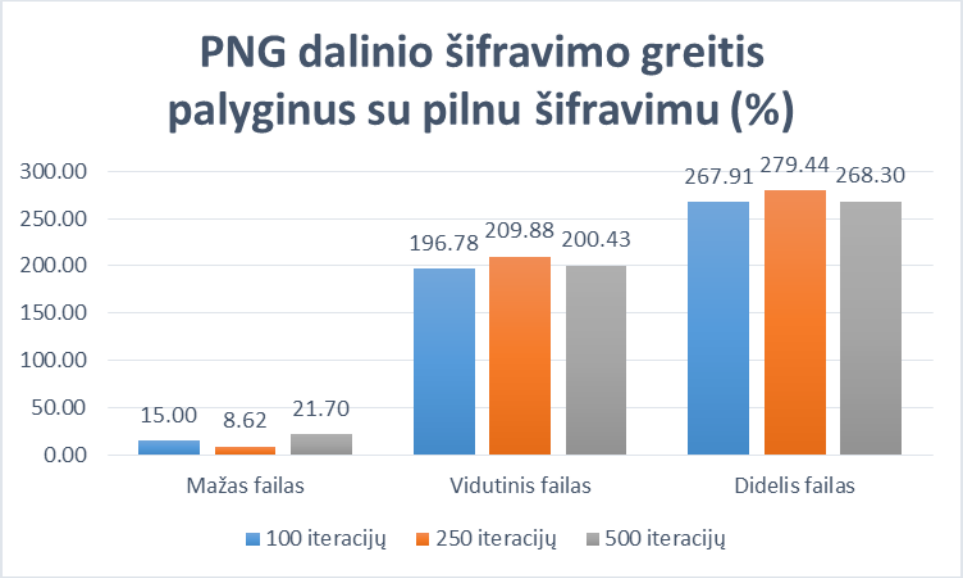
4.4 pav. JPG failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

PNG failų greičio testavimas

Testas atliekamas su mažu, vidutiniu ir dideliu failais

4.7 lentelė. PNG failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

	100 kartų	250 kartų	500 kartų
Mažo failo dalinis užšifravimas	3393 ms	8559 ms	14358 ms
Mažo failo pilnas užšifravimas	3902 ms	9297 ms	17474 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	15,00 %	8,62 %	21,70 %
Vidutinio failo dalinis užšifravimas	4883 ms	11656 ms	24195 ms
Vidutinio failo pilnas užšifravimas	14492 ms	36120 ms	72688 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	196,78 %	209,88 %	200,43 %
Didelio failo dalinis užšifravimas	16678 ms	40733 ms	83440 ms
Didelio failo pilnas užšifravimas	61360 ms	154556 ms	307309 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	267,91 %	279,44 %	268,30 %



4.5 pav. PNG failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

Testavimo išvados

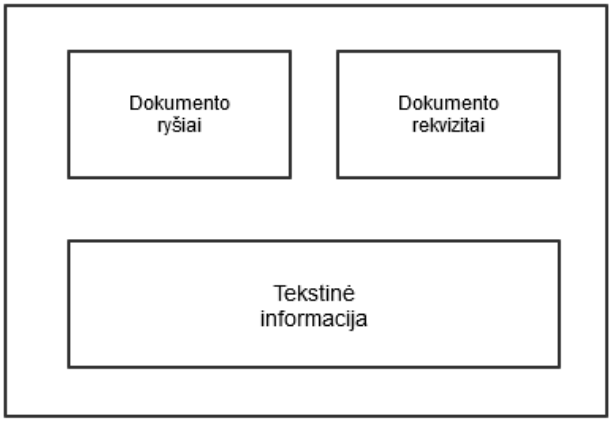
Failų atkuriamumo analizėje buvo naudojamos trys specializuotos programos atkurti JPG failams. Užšifravus 2, 4, 8, 16 ir 32 kilobaitus informacijos iš failo pradžios buvo nustatyta, jog nei vienai programai nepavyko atkurti nei vieno failo užšifravus 32 kilobaitus informacijos. Taipogi šifruojant didelį paveikslėlį, jis tapo nebeatkuriamas užšifravus 8 kilobaitus iš failo pradžios. Atlikus testavimą su PNG failais kuriuose buvo užšifruota 1, 2, 4, 8 ir 16 baitų informacijos iš failo pradžios, tik vienai iš dviejų programų pavyko atkurti failus kuriuose buvo užšifruoti 1, 2 ir 4 baitai. Vadinasi užšifravus puse PNG failo antraštės (angl. *header*) failo atkūrti nepavyksta.

Greičio testavimui JPG failams buvo šifruojami 32 kilobaitai informacijos, o PNG failams 8 baitai informacijos kadangi bandyta programinė įranga tokio šifravimo neįveikė. Testavimas su kiekvienu failu buvo atliekamas tris kartus, užšifruojant ir dešifruojant failą, 100, 250 ir 500 kartų.

Atlikus testavimą pastebėta, jog dalinis šifravimas parodo net iki 700% didesnę spartą lyginant su pilnu šifravimu. Tačiau ši sparta pasiekiama tik su vidutiniais ir dideliais failais, su mažais failais (ypač PNG) buvo gerokai mažesnis spartos skirtumas. Galima teigti, jog dalinis failų šifravimas gali būti naudingas daug kartų šifruojant ir dešifruojant didelius failus.

4.3 Eksperimentas su dokumentų failais

Labai dažnai sutinkami ir naudojami „Microsoft“ „Word“ ir „Excel“ failų tipai todėl jie pasirinkti daliniam šifravimui . Testuojant pasirinkti du skirtingo dydžio DOCX ir XLSX failai kurių informacija esanti failo pradžioje bus dalinai užšifruoti ir pasitelkus specializuotus failų atkūrimo įrankius bus siekiama nustatyti užšifravimo ribą nuo kurios failas tampa nebeatkuriamas. DOCX ir XLSX failų struktūra yra identiška (žr. 4.10 pav.). Dokumentas lyg archyvas savyje talpinantis 3 pagrindinius segmentus: dokumento ryšius, dokumento rekvizitus ir tekstinę informaciją (tekstas, stiliai, formatavimas).



4.6 pav. DOCX ir XLSX failų struktūra

Naudojama programinė įranga

DOCX failų atkūrimui naudojami įrankiai:

- Word Repair Toolbox [13]
- Recoveryfix for Word [14]
- DocRepair [15]

XLSX failų atkūrimui naudojami įrankiai:

- Recovery for Excel [16]
- Excel Repair Toolbox [17]

Testiniai failai

DOCX failų testavimui pasirinkta 10 skirtingų dydžių ir sudėties failų:

4.8 lentelė. Testuojami DOCX failai

Failo pavadinimas	**Failo sudėtis**	**Failo dydis**
Charter	Formatuotas tekstas	273 kb
Checker	Įvairūs šriftai, paveiksliukas	84 kb
Everything	Tekstas, lentelės, formatavimas	1311 kb
FAQ	Tekstas	25 kb
GetStarted	Tekstas, paveikslėliai, grafikai	1290 kb
Large	Neformatuotas tekstas, paveikslėlis	186 kb
Paper Template	Tekstas, paveikslėliai	62 kb
Report	Tekstas	138 kb
Small	Tekstas	42 kb
Thesis	Tekstas, paveikslėliai	519 kb

XLSX failų testavimui pasirinkta 10 skirtingų dydžių ir sudėties failų:

4.9 lentelė. Testuojami XLSX failai

Failo pavadinimas	**Failo sudėtis**	**Failo dydis**
Formula	Formulės	18 kb
FraudActivity	Skaičiai, 5 lapai	84 kb
London2012	Skaičiai su rūšiavimu	1134 kb
Military	Skaičiai, tekstas su rūšiavimu	63 kb
Retention	Pivot lentelės	452 kb
Statistics	Skaičiai	3545 kb

SupplierList	Tekstas	17 kb
SurfaceChallenge	Formos	56 kb
Test1	Skaičiai	121 kb
Test2	Skaičiai	41 kb

Failų atkūrimas

Užšifruotus failus bandoma atkurti, lentelėse nurodomas užšifruotas informacijos kiekis, failo dydis ir ar pavyko atkurti failą.

Testuojant DOCX failus, jie užšifruoti 256, 512, 1024, 2048 ir 4096 baitais informacijos. Buvo bandoma atkūrti failuose esantį tekstą, paveikslėlius ir grafikus.

4.10 lentelė. Antrojo DOCX failo atkūrimas

	Word Repair Toolbox	Recoveryfix for Word	DocRepair
256 baitai	Taip	Taip	Taip
512 baitai	Taip	Taip	Taip
1024 baitų	Taip	Taip	Taip
2048 baitai	Taip	Taip	Taip
4096 baitai	Ne	Ne	Ne
Paveikslėlis	Ne	Taip	Taip
Grafikas	Ne	Ne	Ne

Testuojant failus nei vienai programai nepavyko įveikti 4096 baitų šifravimo ir atkūrti grafiko, tačiau dviem programom pavyko atkurti paveiksliukus esančius dokumente. Paveikslėlio atkūrimas parodo, jog užšifravus tik nedidelę failo dalį paveikslėliai yra nesunkiai atkūriami nepriklausomai ar patį dokumento tekstą pavyksta atkūrti.

Testuojant XLSX failus, juose užšifruota 8, 16 ir 32 kilobaitai informacijos. Buvo bandoma atkūrti tekstus, skaičius, formas ir grafikus.

4.11 lentelė. XLSX failų atkūrimas su Recovery for Excel

	Užšifruota 8 kb	**Užšifruota 16 kb**	**Užšifruota 32 kb**
Formula	Taip	Ne	Ne
FraudActivity	Dalinai, trūksta 1 lapo	Dalinai, trūksta 2 lapų	Dalinai, trūksta 2 lapų
London2012	Taip	Taip	Ne
Military	Ne	Ne	Ne
Retention	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne
Statistics	Ne	Ne	Ne
SupplierList	Ne	Ne	Ne
SurfaceChallenge	Dalinai, formos neveikia	Ne	Ne
Test1	Ne	Ne	Ne
Test2	Ne	Ne	Ne

Recovery for Excel Pavyko atkūrti nedaug failų, po atkūrtimo formos neveikia, grafikų nelikę.

4.12 lentelė. XLSX failų atkūrimas su Excel Repair Toolbox

	Užšifruota 8 kb	**Užšifruota 16 kb**	**Užšifruota 32 kb**
Formula	Atkūrtas tik tekstas, trūksta vieno lapo	Ne	Ne
FraudActivity	Dalinai, trūksta 2 lapų	Dalinai, trūksta 3 lapų	Dalinai, trūksta 3 lapų
London2012	Atkūrtas tik tekstas	Atkūrtas tik tekstas	Ne
Military	Ne	Ne	Ne
Retention	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne
Statistics	Ne	Ne	Ne
SupplierList	Ne	Ne	Ne
SurfaceChallenge	Ne	Ne	Ne
Test1	Ne	Ne	Ne
Test2	Ne	Ne	Ne

4.13 lentelė. XLSX failų atkūrimas su Kernel for Excel

	Užšifruota 8 kb	**Užšifruota 16 kb**	**Užšifruota 32 kb**
Formula	Atkūrtas tik tekstas, trūksta vieno lapo	Ne	Ne
FraudActivity	Dalinai, trūksta 2 lapų	Dalinai, trūksta 3 lapų	Dalinai, trūksta 3 lapų
London2012	Atkūrtas tik tekstas	Atkūrtas tik tekstas	Ne
Military	Ne	Ne	Ne
Retention	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne	Atkūrtas tekstas, pivot lentelė - ne
Statistics	Ne	Ne	Ne
SupplierList	Ne	Ne	Ne
SurfaceChallenge	Ne	Ne	Ne
Test1	Ne	Ne	Ne
Test2	Ne	Ne	Ne

Ištyrus failų atkuriamumą buvo pastebėta, jog lengviausiai atkuriami yra paprasti dokumentai su nedaug informacijos. Formulių, pivot lentelių ir grafikų nepavyko atkūrti nei vienai programai. Nustatyta, jog yra failų kurie yra atkuriami nepriklausomai nuo užšifruotos informacijos kiekio, tai gali sudaryti net daugiau nei trečdalį failo. Dėl tokių priežasčių dalinis šifravimas netenka prasmės ir XLSX failų tipas nebus naudojamas tolimesniame dalinio šifravimo testavime.

Testavimo greičiai

Greičio testas su x iteracijų užšifruojant 4096 baitus informacijos

4.14 lentelė. DOCX failų dalinio ir pilno šifravimų laikai (ms) su 100 iteracijų

Failo pavadinimas	**Bendras dalinio šifravimo laikas**	**Bendras pilno šifravimo laikas**	**Skirtumas tarp dalinio ir pilno šifravimo**
Charter	1715 ms	3527 ms	105,66 %
Checker	1380 ms	2024 ms	46,67 %
Everything	2587 ms	11797 ms	356,01 %
FAQ	1318 ms	1513 ms	14,80 %
GetStarted	3156 ms	11615 ms	268,03 %
Large	1422 ms	2748 ms	93,25 %
Paper Template	1316 ms	1802 ms	36,93 %
Report	1389 ms	2351 ms	69,26 %

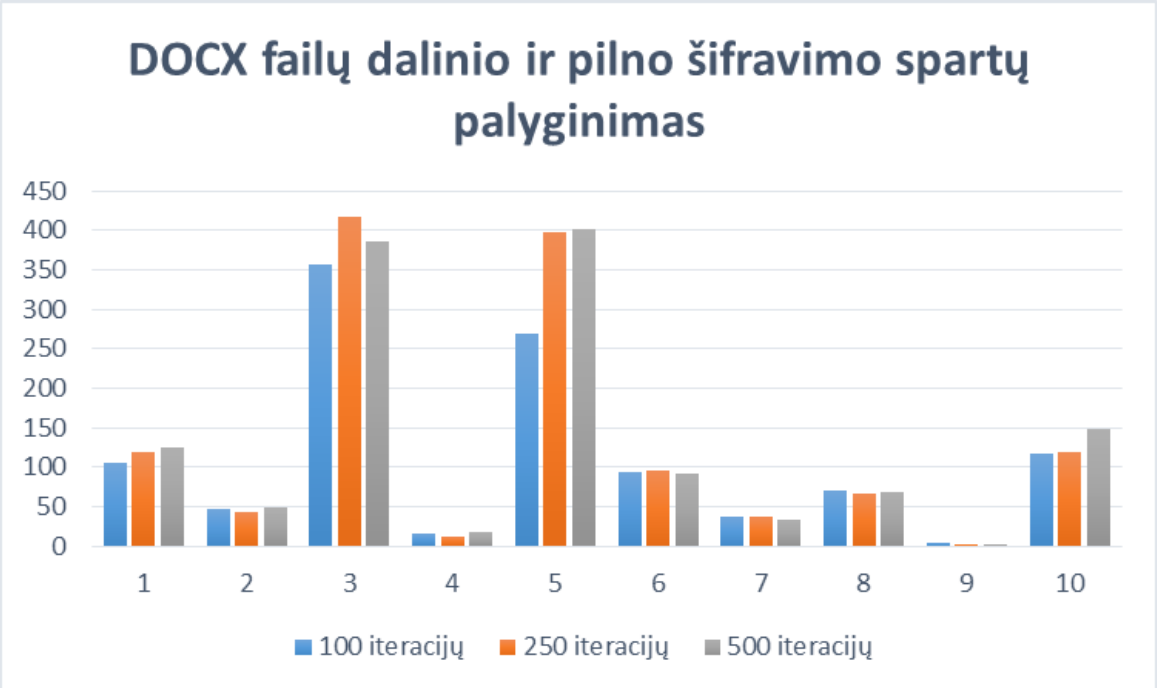
Small	19801 ms	20516 ms	3,61 %
Thesis	3175 ms	6902 ms	117,39 %

4.15 lentelė. DOCX failų dalinio ir pilno šifravimų laikai (ms) su 250 iteracijų

Failo pavadinimas	**Bendras dalinio šifravimo laikas**	**Bendras pilno šifravimo laikas**	**Skirtumas tarp dalinio ir pilno šifravimo**
Charter	3940 ms	8653 ms	119,62 %
Checker	3397 ms	4869 ms	43,33 %
Everything	5655 ms	29238 ms	417,03 %
FAQ	3294 ms	3683 ms	11,81 %
GetStarted	5776 ms	28684 ms	396,61 %
Large	3565 ms	6984 ms	95,90 %
Paper Template	3323 ms	4551 ms	36,95 %
Report	3569 ms	5923 ms	65,96 %
Small	49652 ms	50767 ms	2,25 %
Thesis	7776 ms	16976 ms	118,31 %

4.16 lentelė. DOCX failų dalinio ir pilno šifravimų laikai (ms) su 500 iteracijų

Failo pavadinimas	**Bendras dalinio šifravimo laikas**	**Bendras pilno šifravimo laikas**	**Skirtumas tarp dalinio ir pilno šifravimo**
Charter	7806 ms	17469 ms	123,79 %
Checker	6559 ms	9701 ms	47,90 %
Everything	12043 ms	58471 ms	385,52 %
FAQ	6571 ms	7667 ms	16,68 %
GetStarted	11477 ms	57498 ms	400,98 %
Large	7225 ms	13859 ms	91,82 %
Paper Template	6732 ms	9025 ms	34,06 %
Report	7053 ms	11894 ms	68,64 %
Small	99529 ms	101134 ms	1,61 %
Thesis	12614 ms	31315 ms	148,26 %



4.7 pav. DOCX failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

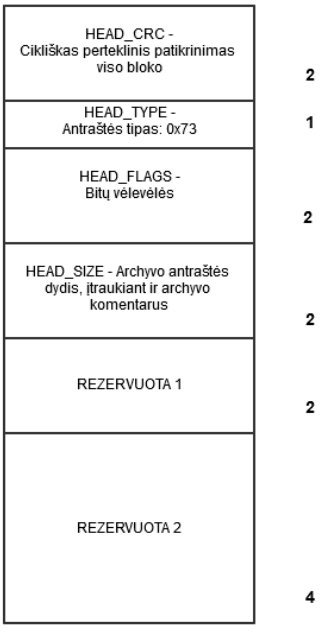
Testavimo išvados

Failų atkuriamumo analizėje buvo naudojamos trys specializuotos programos DOCX ir dvi programos XLSX failams atkurti. DOCX failams buvo užšifruota 256, 512, 1024, 2048 ir 4096 baitų informacijos iš failo pradžios. Atlikus analizę nustatyta, jog šio formato failai tampa visai nebeatkuriami užšifravus 4096 baitus informacijos, tačiau tai negalioja nuotraukoms. Net jeigu failas nėra perskaitomas nuotraukos gali būti atkūrtos. XLSX failams buvo šifruojama 8, 16 ir 32 kilobaitai informacijos. Atlikus analizę nustatyta, jog formų, formulių, grafikų ir pivot lentelių atkūrti neišeina, tačiau kai kuriuos failus įmanoma atkūrti net ir užšifravus didelę jų dalį. Dėl didelio failo atkuriamumo buvo atsisakyta XLSX formato daliniame šifravime.
Greičio testavime buvo bandoma dešimt DOCX failų, kuriuose buvo užšifruota 4096 baitai informacijos. Testavimas su kiekvienu failu buvo atliekamas tris kartus, užšifruojant ir dešifruojant failą, 100, 250 ir 500 kartų. Atlikus testavimą pastebėta, jog šifruojant ir dešifruojant failą nedideli kiekį kartų (50) matomas didžiausias skirtumas tarp dalinio ir pilno šifravimo kuris didėjant bandymų skaičiui krenta. Atlikus testavimą su 100, 250 ir 500 iteracijų pastebėta, jog dalinis šifravimas atliekamas greičiau ir tokią tendenciją (žr. X. pav.) išlaiko beveik visuose bandytuose failuose nepriklausomai nuo bandymų skaičiaus

Atlikus testavimą galima teigti, jog dalinis DOCX failų šifravimas yra greitesnis už pilna šifravimą. Nustatyta, jog XSLX formatas yra gerai atkuriamas ir nėra tinkamas daliniam šifravimui.

4.4 Eksperimentas su failų archyvais

Failų archyvų analizei pasirinktas RAR failų tipas, kadangi tai vienas populiariausių archyvavimo failų formatų. Testuojami 3 skirtingo dydžio archyvai kurių informacija esanti failo pradžioje bus dalinai užšifruoti ir pasitelkus specializuotus failų atkūrimo įrankius bus siekiama nustatyti užšifravimo ribą nuo kurios failas tampa nebeatkuriamas. RAR failo antraštė sudaryta iš 13 baitų (žr. X pav.), pagrindinė informacija yra saugoma pirmuose 7 baituose, likę šeši baitai rezervuoti papildomai informacijai.



4.8 pav. RAR failo header struktūra

Naudojama programinė įranga

Užkoduotų RAR archyvų atkūrimui bus pasinaudota šia programine įranga:

- DataNumen RAR Repair [18]
- RAR Fix Toolbox [19]

- Yodot RAR Repair [20]

Testiniai failai

Testavimui pasirinkti trys skirtingi archyvai, kiekvienas jų suspaustas su tokiais pats nustatymais.

- Suspaudimo metodas: normalus
- Žodyno dydis: 4096 KB
- Archyvo formatas: RAR

Atlikus suspaudimą gauti tris archyvai:

1. Suarchyvuotas vienas grafinis failas (JPG), archyvas 2215 kb dydžio.
2. Suarchyvuotas vienas dokumentų failas (PDF), archyvas 16369 kb dydžio.
3. Suarchyvuoti 3 failai: grafinis failas (JPG), dokumentų failas (PDF) ir tekstinis (TXT) , archyvas 19073 kb dydžio.

Failų atkūrimas

Užšifruotus failus bandoma atkurti, lentelėse nurodomas užšifruotas informacijos kiekis, failo dydis ir ar pavyko atkurti failą.

Pirmojo RAR failo testavime visos bandytos atkūrimo programos pasirodė vienodai

4.17 lentelė. Pirmojo RAR failo atkūrimas

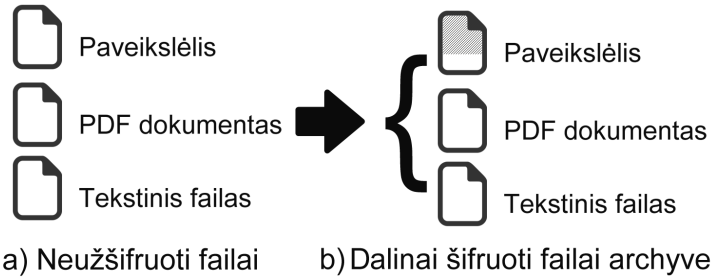
	1 baitai	2 baitai	4 baitų	8 baitai	16 baitų
Ar pavyko atkurti	Taip	Taip	Taip	Taip	Ne

Antrojo RAR failo testavime visos bandytos atkūrimo programos taip pat pasirodė visiškai vienodai. Neįtakojo nei didesnis failo dydis, nei kitoks failo tipas.

4.18 lentelė. Antrojo RAR failo atkūrimas

	1 baitai	2 baitai	4 baitų	8 baitai	16 baitų
Ar pavyko atkurti	Taip	Taip	Taip	Taip	Ne

Trečiojo failo testavimas buvo kiek kitoks, kadangi užšifruota tik pati archyvo pradžia, toliau esantys failai nesunkiai perskaitomi. Neturėjo įtakos ar užšifruojama tik 16 baitų ar 1 megabaitas, dalinai užšifruotas failas praleidžiamas, o toliau sekantys failai nesunkiai atšifruojami (žr pav. 4.13).



4.9 pav. Neužšifruotų ir dalinai užšifruotų failų archyve schema

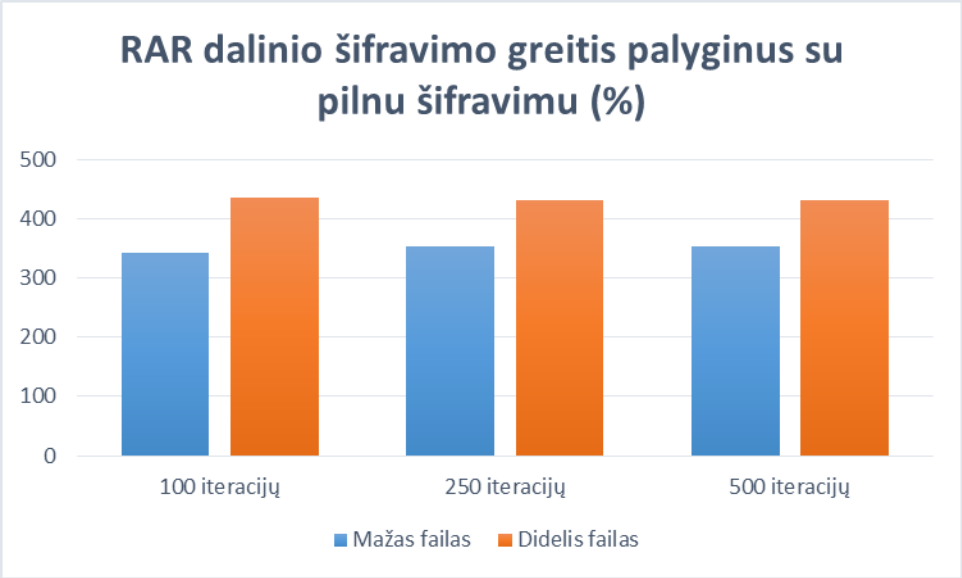
Neužšifruoti failai dedami į archyva parodyta tvarka. Todėl šifruojant archyvo pradžią buvo užšifruojamas tik pirmasis failas, kiti likę failai liko nepaliesti ir buvo nesunkiai atkurti.Norint užšifruoti visus failus reiktų išarchyvuoti archyvą ir šifruoti kiekvieną failą atskirai, toks šifravimas būtų nenaudingas nei laiko, nei resursų atžvilgiu. Esant tokiems rezultatams prieita prie išvados, jog

failų archyvai kurie turi daugiau nei vieną failą nėra tinkami daliniam failų šifravimui ir nebus naudojami greičio testavime.

Testavimo greičiai
Greičio testas atliekamas su RAR failais

4.19 lentelė. RAR failų dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

	100 kartų	250 kartų	500 kartų
Pirmojo failo dalinis užšifravimas	5690 ms	13990 ms	28197 ms
Pirmojo failo pilnas užšifravimas	25190 ms	63245 ms	127560 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	342,71 %	352,07 %	352,39 %
Antrojo failo dalinis užšifravimas	33695 ms	85442 ms	170219 ms
Antrojo failo pilnas užšifravimas	180283 ms	454072 ms	902361 ms
Skirtumas tarp pilno ir dalinio šifravimo laiko	435,04 %	431,44 %	430,12 %



4.10 pav. RAR pirmo failo dalinio ir pilno šifravimų laikai (ms) su 100, 250 ir 500 iteracijų

Testavimo išvados

Failų atkuriamumo analizėje buvo naudojamos trys specializuotos programos archyviniams failams RAR formatu atkurti. Testavimui buvo pasirinkti trys archyvai, pirmajame archyve buvo nuotrauka, antrąjame – didelis dokumentas PDF formatu, trečiąjame – prieš tai naudota nuotrauka, dokumentas ir priedo tekstinis failas. Atlikus analizę nustatyta, jog užšifravus pirmus 16 archyvo baitus archyvas tampa nebeatkuriamas pasinaudojus turimomis atkūrimo programomis. Tačiau jeigu archyve yra daugiau nei vienas failas tada failas tampa atkuriamas. Failo atkuriamuma įtakoja tai, jog užkodavus archyvo pradžią įtakoja, tik patį pirmąjį failą esantį archyve. Norint užšifruoti visus archyvo failus juos reikia šifruoti po vieną arba žinoti tikslų kiekvieno failo dydį ir jų išsidėstymą archyve. Tokios procedūros užimtų per daug laiko ir resursų, todėl failų archyvas su 3 failais, nebuvo naudojamas greičio bandyme.

Greičio testavime buvo bandomi du archyvai kurių 16 pradžios baitų buvo užšifruota. Testavimas su kiekvienu failu buvo atliekamas tris kartus, užšifruojant ir dešifruojant failą, 100, 250 ir 500 kartų. Atlikus testą pastebėtos dvi tendencijos. Pirmoji, jog dalinio šifravimo pranašumas

išlaikomas visuose testavimuose ir siekia 349% mažam ir 432% dideliam failams. Antroji tendencija rodo, jog didėjant failo dydžiui skirtumas tarp dalinio ir pilno šifravimo didėja, dalinio šifravimo naudai. Atlikus testavimą galima teigti, jog dalinis RAR failų šifravimas yra ženkliai greitesnis už pilną šifravimą ir failo formatas yra tinkamas dalinio šifravimo pritaikymui, su sąlyga, jog archyve yra tik vienas failas.

5. REZULTATŲ APIBENDRINIMAS IR IŠVADOS

1. Atlikus šifravimo algoritmų ir esamų sistemų analizę pasirinkta naudoti AES šifravimą su 256 bitų raktu. Išsikėlus reikalavimus daliniam šifravimui sukurta veikianti testavimo sistema, kuri buvo naudojama tyrime.
2. Atliekant failų atkuriamumo analizę buvo testuojami skirtingi failų tipai, dydžiai ir jų atkuriamumas po užšifravimo. Atlikus analizę nustatyti failų tipai, kurie tinka daliniam failų šifravimui.
3. Atlikus greičio testavimą su tinkamais failų tipais, gauti daug žadantys rezultatai: grafinių failų testuose, didelių JPG failų šifravime dalinis šifravimas parodė vidutiniškai 522%, o PNG failų 163% didesnę spartą. Ištestavus 10 dokumentų failų gauta vidutiniškai 124% didesnė sparta lyginant su standartiniu šifravimu.
4. Šiame darbe buvo ištirti populiarūs failų tipai, jų panaudojamumas daliniam šifravimui ir greičio palyginimas tarp dalinio ir pilno šifravimo. Pastebėta aiškus dalinio šifravimo pranašumas greičio atžvilgiu visuose failų formatuose, ypač greičio skirtumas pastebimas šifruojant vidutinius ir didelius failus.

6. LITERATŪROS ŠALTINIAI

[1] Description of Symmetric and Asymmetric Encryption [tinkle]. Prieiga per internetą: http://support.microsoft.com/kb/246071 [kreiptasi 2013-01-15]

[2] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 1996, 17p., 213-214p.ISBN 0-471-11709-9.

[3] Public-key cryptography [tinkle]. Prieiga per internetą: http://en.wikipedia.org/wiki/Public-key_cryptography [kreiptasi 2013-01-15]

[4] Symmetric Encryption, Asymmetric Encryption, and Hashing [tinkle]. Prieiga per internetą: http://packetlife.net/blog/2010/nov/23/symmetric-asymmetric-encryption-hashing/ [kreiptasi 2013-01-15]

[5] USB flash drive security [tinkle]. Prieiga per internetą: http://en.wikipedia.org/wiki/USB_flash_drive_security [kreiptasi 2013-01-19]

[6] Announcing the ADVANCED ENCRYPTION STANDARD (AES) [tinkle]. Prieiga per internetą: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [kreiptasi 2013-03-01]

[7] TrueCrypt - Encryption Algorithms [tinkle]. Prieiga per internetą: http://www.truecrypt.org/docs/encryption-algorithms#Y0 [kreiptasi 2013-03-12]

[8] „BitLocker“ disko šifravimas [tinkle]. Prieiga per internetą: http://windows.microsoft.com/lt-lt/windows7/products/features/bitlocker [kreiptasi 2013-04-21]

[9] Dr. Falk's Store O'Crypt [tinkle]. Prieiga per internetą: www.fair-computer.de/en/produkte/dr-falks-store-ocrypt.html [kreiptasi 2013-05-05]

[10] PixRecovery - OfficeRecovery.com [tinkle]. Prieiga per internetą: http://www.officerecovery.com/pixrecovery/ [kreiptasi 2013-04-21]

[11] JPEG Recovery - Recover corrupted JPEG Picture after Data Recovery Processing [tinkle]. Prieiga per internetą: http://www.hketech.com/JPEG-recovery/ [kreiptasi 2014-03-05]

[12] Jpeg Repair Tool. Jpeg Recovery Software To Repair Corrupt Or Damaged Jpg Files. [tinkle]. Prieiga per internetą: http://www.softorbits.com/picdoctor/ [kreiptasi 2014-03-05]

[13] A program for recovering corrupted JPEG files, recovery after deletion [tinkle]. Prieiga per internetą: http://www.my-data-recovery.com/file-repair/software-4.html [kreiptasi 2014-04-01]

[14] Word Repair Toolbox makes Word repair, fast, simple, easy! [tinkle]. Prieiga per internetą: http://www.word.repairtoolbox.com/ [kreiptasi 2014-04-05]

[15] Free Download RecoveryFix for Word - Word File Recovery Software [tinkle]. Prieiga per internetą: http://www.recoveryfix.com/download-word-recovery.html [kreiptasi 2014-04-05]

[16] DocRepair - Corrupted MS Word File Recovery Software [tinkle]. Prieiga per internetą: http://www.jufsoft.com/docrepair/ [kreiptasi 2014-04-05]

[17] Recovery for Excel. Recover, Restore Corrupted Excel (xls, xlsx, xla) Spreadsheet [tinkle]. Prieiga per internetą: http://www.officerecovery.com/excel/ [kreiptasi 2013-04-17]

[18] Download Microsoft Excel repair tool and fix XLS files anywhere [tinkle]. Prieiga per internetą: http://www.excelrepairtoolbox.com/ [kreiptasi 2014-04-17]

[19] DataNumen RAR Repair - Repair corrupt RAR files. RAR recovery tool. [tinkle]. Prieiga per internetą: http://www.datanumen.com/rar-repair/ [kreiptasi 2014-04-21]

[20] Start the rar fix download and repair WinRAR files with RAR Fix Toolbox [tinkle]. Prieiga per internetą: http://www.rar.fixtoolbox.com/ [kreiptasi 2013-05-01]

[21] Winrar File Repair Software - Repair corrupt RAR files [tinkle]. Prieiga per internetą: http://www.yodot.com/rar-repair/ [kreiptasi 2013-05-02]