МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Орищенко Сергій Олександрович

УДК 004.02

Інформаційна система шифрування мультимедійних даних

124 – МНР.ПЗ.0-607м.11953167

Автореферат

магістерської наукової роботи на здобуття освітньої кваліфікації

Магістр комп’ютерних наук

Миколаїв – 2019

Магістерська наукова робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем

Науковий керівник: к.ф.м.н., доцент Кулаковська Інесса Василівна

Рецензент: д.т.н., професор Дихта Леонід Михайлович

Захист відбудеться «28» лютого 2019 р. о $9^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською науковою роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений « » лютого 2019 р.

Секретар
екзаменаційної комісії,
к.пед.н., доцент Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Проблема забезпечення необхідного рівня захисту інформації виявилася (і це предметно підтверджено як теоретичними дослідженнями, так і досвідом практичного вирішення) досить складною, це вимагає для рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів та застосування специфічних засобів і методів, а створення цілісної системи організаційних заходів та застосування специфічних засобів і методів із захисту інформації.

Обсяг циркулюючої в суспільстві інформації стабільно зростає. Популярність всесвітньої мережі Інтернет в останні роки сприяє подвоєнню інформації кожен рік. Фактично, на порозі нового тисячоліття людство створило інформаційну цивілізацію, в якій від успішної роботи засобів обробки інформації залежить добробут і навіть виживання людства в його нинішній якості. Події, що сталися за цей період зміни можна охарактеризувати наступним чином:

- обсяги оброблюваної інформації зросли за півстоліття на кілька порядків;
- доступ до певних даних дозволяє контролювати значні матеріальні та фінансові цінності;
- характер оброблюваних даних став надзвичайно різноманітним і більше не зводиться до виключно текстових форматів;
- суб'єктами інформаційних процесів тепер є не тільки люди, а й створені ними автоматичні системи, які діють за закладеною в них програмою;
- обчислювальні "здібності" сучасних комп'ютерів підняли на абсолютно новий рівень як можливості по реалізації шифрів, раніше недосяжних за своєї високої складності, так і можливості додатків по їх взлому. Перераховані вище зміни призвели до того, що незабаром після розповсюдження комп'ютерів в діловій сфері практична криптографія зробила в своєму розвитку величезний стрибок, причому відразу в кількох напрямках:

По-перше, були розроблені стійкі блокові шифри з секретним ключем, призначені для вирішення класичного завдання - забезпечення секретності і цілісності, переданих або збережених даних;

По-друге, були створені методи вирішення нових, нетрадиційних завдань сфери захисту інформації, найбільш відомими з яких є завдання підпису цифрового документа і відкритого розподілу ключів. У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку.

Об'єктом дослідження є процеси шифрування мультимедійних даних.

Предметом дослідження є методи та технології шифрування даних.

Метою даної роботи є створення програми для успішної обробки даних за допомогою алгоритму.

Виходячи з мети науково-дослідницької роботи, поставлені такі завдання, а саме:

- провести аналіз підходів до шифрування даних;
- дослідити вже існуючі інструменти та програми;
- провести аналіз варіантів шифрування даних різних форматів;
- провести аналіз можливості побудови середовища для відтворення зашифрованих даних;
- розробити власний застосунок, який буде шифрувати мультимедійних даних.

Методи дослідження. Під час проектування та розробки інформаційної системи було використано технології блочного шифрування та алгоритм шифрування AES, а також мову програмування Python та її фреймворк графічного інтерфейсу Tkinter.

Практичне значення отриманих результатів. Отримані результати досліджень було використані під час розробки інформаційної системи. Система розроблена у вигляді десктопного застосунку. Вибір програмної реалізації зумовлений тим, мова програмування Python є ідеальним поєднанням швидкості роботи коду та зручності алгоритмічної реалізації, насамперед логічного та побітового спектру. За допомогою фреймворку Tkinter було реалізовано зручний та зрозумілий графічний користувацький інтерфейс. Інформаційна система реалізує основні принципи блочного шифрування, організовуючи роботу з мультимедійними файлами на хорошому рівні.

Особистий внесок здобувача. Викладені в роботі результати отримано автором самостійно на основі існуючих на даний момент розробок та досліджень в даній сфері. Щодо розглянутих в магістерському дослідженні задач, які розв'язані в працях, спільних з науковим керівником, І.В. Кулаковською, а саме: постановка проблеми досліджень і загальне керівництво роботою.

Мета і завдання дослідження.

Метою даного магістерського дослідження є: реалізація алгоритму шифрування AES за допомогою методів блочного шифрування, результатом якої і стане інформаційна система. Відповідно до мети дослідження в магістерській роботі були поставлені та реалізовані наступні завдання:

1. Провести дослідження сучасниї алгоритмів шифрування та технологій технологій їй реалізації.
2. Провести класифікацію методів шифрування та інструментів для побудови власного проекта.
3. Проектування та розробка інформаційної системи, що функціонує на основі мови програмування Python..
4. Програмна реалізація та інформаційного застосунку “Media Encoder”.
5. Зробити висновки на основі отриманих результатів.

Слід зазначити, що кінцевою точкою виконаної роботи має бути не лише розробка якісного інформаційного застосунку широкого спектру призначення, але і визначення чіткого алгоритму побудови якісної системи за актуальними тенденціями та інструментами.

Об'єктом дослідження являються процеси шифрування мультимедійних даних.

Предметом дослідження виступає: методи та актуальні тенденції у сучасному шифруванні мультимедійних даних, і насамперед можливості їх програмної реалізації.

Наукова новизна отриманих результатів.

1. Запропоновані найактуальніші системи швидкісного та багатоефективного проектування та розроблення десктопної інформаційної системи.

2. Проведено наукове дослідження сучасних технологій та підходів до розробки шифрувальних систем, класифікація технологій та інструментів для їх розробки.

Структура магістерської наукової роботи Магістерська робота складається із вступу, чотирьох розділів, розбитих на підрозділи, методичної частини, висновків і списку використаних джерел. Також присутній спеціальний розділ з охорони праці. Загальний обсяг роботи складає ____ сторінки, ___ рисунків та ____ посилань на літературні джерела.

Основний зміст роботи

У **вступі** подано загальну характеристику досліджуваної теми, обґрунтовано актуальність магістерського дослідження, сформульовано мету, завдання, зазначені видатні фахівці з даної проблематики, відзначено наукову новизну та практичну цінність дослідження, подано інформацію про апробацію, структуру та обсяг роботи.

У **першому розділі** були досліджені актуальні системи, визначено переваги розробленої інформаційної системи, сформовані основні вимоги до створюваної інформаційної системи. Розглянуті особливості структури подібних інформаційних систем, їх основні якості та функції, переваги та недоліки. Провівши аналіз останніх досліджень, існуючих методів та підходів до шифрування, можна зробити висновок, що інформаційні десктопні системи отримують особливу перевагу там, де проводиться робота з великими обсягами даних. Це може бути персональний комп’ютер на одного користувача, або точка доступу чи сервер на підприємстві. Так само приведена інформаційна система виявляється вигіднішою в разі необхідності безпосередньої роботи без доступу до мережі інтернет, наприклад, коли користувач працює без виходу онлайн чи коли йому необхідно обробити велику кількість даних будучи певним що він знаходиться без підключення до інтернет, що буває критично важливо при певних умовах. У цьому випадку вигода полягає у відсутності необхідності підключення мережі інтернет і у швидкодії інформаційної системи.

У **другому розділі** приведено детальний аналіз сучасних технологій та підходів до шифрування даних, класифікація методів блочного шифрування та

інструментів до програмної реалізації даних методів. Було виконано порівняльний аналіз найбільш поширених алгоритмів шифрування, а також методів саме шифрування даних блочного типу. Зробивши огляд використання мови програмування Python для реалізації алгоритмів шифрування даних, можна зробити висновок, що особливість системи в тому, що вона не вимагає підключення масивних пакетів даних, дозволяє реалізувати шифрувальні операції та користувацький інтерфейс силами власного пакетного середовища, та вимагає приблизно базового володіння основами функціонального та об'єктно орієнтованого програмування.

Незважаючи на різноманітність мов програмування, в основі методології саме блочного шифрування лежить єдиний принцип. Мова програмування Python чудово підходить для створення систем, що працюють з великими обсягами даних та реалізують бітову логіку на базовому рівні. Також для графічного представлення даної системи було використано фреймворк Tkinter, який дозволяє створити базовий та зручний інтерфейс, не обтяжений модулями і додатковими пакетами.

У **третьому розділі** приведено детальний аналіз реалізації поставленої криптографічної задачі. Було виконано порівняльний аналіз найбільш поширених методів блочного шифрування. Крім того було проведено розбір нюансів, пов'язаних з обробкою байт коду мультимедійних даних. Режими блочного шифрування являють собою на даний момент, найбільш доступний та сильний інструментарій по шифруванню великих обсягів бітової інформації, тому було проведено детальний порівняльний аналіз кожного з них.

Незважаючи на те, що реалізований алгоритм являє собою закінчений продукт, було критично важливо доповнити його також і графічним користувацьким інтерфейсом. В першу чергу для того, щоб програма могла застосовуватись не тільки професіональним користувачем, а і користувачем з базовими знаннями в сфері. Було приведено зразки коду реалізації кожного ключового об'єкту системи, приведено класові та функціональні зв'язки, також потрібні для роботи виключення. Було приведено зразки реалізації кожного

режиму блочного шифрування у коді, а також реалізацію самого алгоритму шифрування AES.

У **четвертому розділі** продемонстрована саме реалізація особистого проекту «Інформаційна система шифрування мультимедійних даних Media Encoder». У висновках робиться аналіз виконаної роботи. (рис. 1.1).

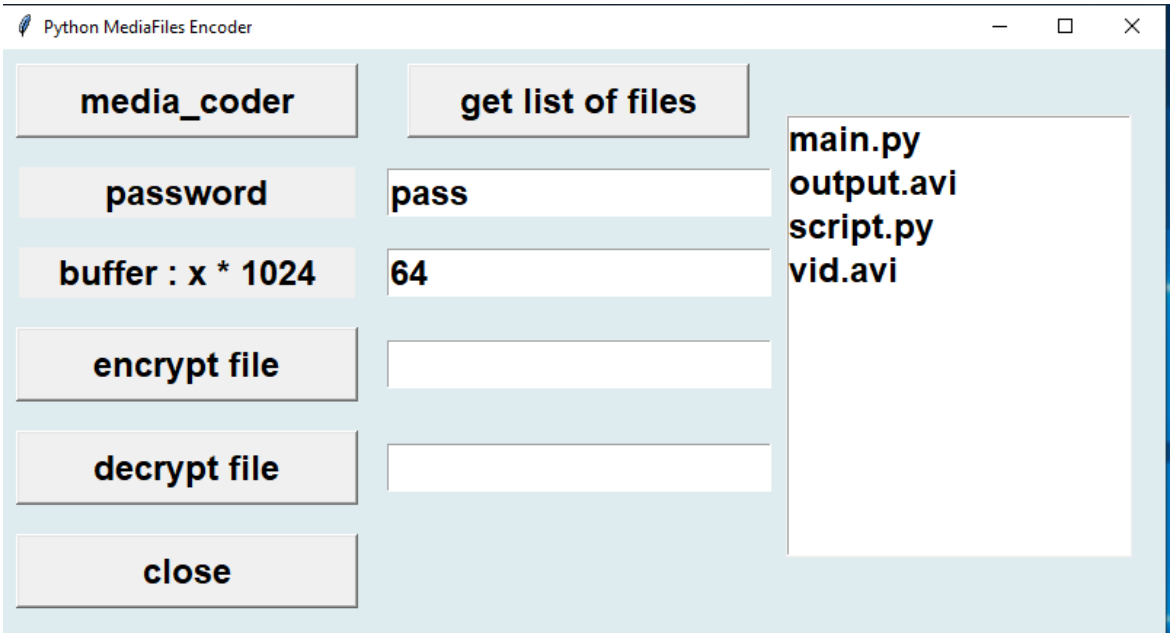

Рис 1.1. Головне вікно застосунку «Media Encoder»

В даній частині дипломної роботи описано процес користування даним застосунком, було пояснено ключові моменти та нюанси з безпосереднього користувацього досвіду шифрування даних.

У п’ятому розділі присвячений охороні праці у виробничому приміщенні, було виконано розрахунок природного освітлення, розрахунок загального рівномірного освітлення люмінесцентними лампами у виробничому приміщенні, розрахунок параметрів спліт-системи кондиціонування та підбір обладнання тепловологісної обробки повітря, визначено необхідної холодо - та теплопродуктивності спліт-системи кондиціонування в офісі» .

Представлені розрахунки свідчать, що площа вікон, влаштованих у виробничому приміщенні більша за площу вікон, що необхідна для забезпечення нормованої природної освітленості у виробничому приміщенні, природне освітлення для заданого розряду зорової роботи достатнє. Але при застосуванні

бокового освітлення створюється висока освітленість поблизу вікон і низька у глибині приміщення, тому можливе утворення тіней від устаткування.

У **шостому розділі** для закріплення знань і навичок студентам пропонується виконати ряд практичних робіт з використанням методів, підходів та алгоритмів оптимізації. За допомогою яких, студент має можливість оволодіти фаховими знаннями в даній предметній області. Кожна практична робота містить мету, завдання, ідею того чи іншого методу, приклади, варіанти виконання. Також пропонується відповісти на контрольні питання і подивитись на пакети прикладних програм. Все це надає студентові фундаментальні вміння використовувати теоретичні засади і підходи у практичних і реальних ситуаціях.

ВИСНОВКИ

У даній дипломній роботі було розроблено і описано процес створення інформаційної системи шифрування мультимедійних даних за допомогою мови програмування Python та його фреймворку графічного інтерфейсу Tkinter. Результати відповідають поставленим вимогам, було реалізовано задумані механізми і функціональності, це означає, що першочергова мета досягнута. Під час проведення тестування була проведена перевірка застосунку на успішне виконання поставлених перед ним цілей з шифрування мультимедійних даних у формі відео-, аудіо- та фото-файлів. Перевірка на зручність користування системою показала, що інформаційна система є зручним як для користувачів, так і для адміністраторів. Перевірка валідності системи не виявила помилок коду. Можливі подальші дослідження, які матимуть наукову та практичну цінність для розробленої системи і допомагатимуть робити її кращою, сучаснішою, але головне зручнішою для користувачів.

АНОТАЦІЯ

до магістерської наукової роботи

на тему: «Інформаційна система шифрування мультимедійних даних»

Студент: Орищенко Сергій Олександрович

Науковий керівник: к.ф.-м.н., доцент Кулаковська Інесса Василівна

В дипломній роботі представлено інформаційну систему, що реалізує алгоритм шифрування Rijndael та шифрує мультимедійні дані користувача.

Актуальність даної роботи полягає в тому, що успішне функціонування системи шифрування даних залежить від реалізованого в ній алгоритму.

Мета дослідження полягає в створенні інформаційного середовища, для проведення шифрування та дешифрування мультимедійних даних.

Об'єктом дослідження є процеси шифрування мультимедійних даних.

Предметом дослідження є методи та технології шифрування даних.

Робота складається з трьох частин: фахова частина та дві спеціальні частини: охорона праці та безпека у надзвичайних ситуаціях, методичні матеріали.

У вступі проводиться короткий огляд поставленої задачі.

У першому розділі наводиться загальна проблематика сфери.

Другий розділ присвячено аналізу алгоритму шифрування та методам обробки даних.

Третій розділ присвячено розгляду програмної реалізації даної системи.

В четвертому розділі приводиться огляд роботи та функціонування системи.

У висновках проводиться аналіз виконаної роботи та отриманих результатів.

Спеціальна частина з охорони праці та безпеки у надзвичайних ситуаціях присвячена питанням з охорони праці на робочих місцях.

***Ключові слова**: криптографія, криптоаналіз, симетричне та асиметричне шифрування.*

ABSTRACT

of the master's research work
"Information system of cryptographic encryption of multimedia data"

Student: S.O.Oryschenko

Research manager: Candidate of P-M Sciences, Docent I.V. Kulakovska

The dissertation presents the information system that implements the Rijndael encryption algorithm and encrypts the multimedia data of the user.

The urgency of this work lies in the fact that the successful functioning of the data encryption system depends on the algorithm implemented in it.

The purpose of the study is to create an information environment for encrypting and decrypting multimedia data.

The object of the study is the process of encrypting multimedia data.

The subject of the study is data encryption methods and technologies.

The work consists of three parts: a specialty and two special parts: labor protection and emergency safety, methodological materials.

The introduction provides a brief overview of the task.

The first section gives a general perspective of the sphere.

The second section is devoted to the analysis of the encryption algorithm and data processing methods.

The third section is devoted to the consideration of software implementation of this system.

The fourth section gives an overview of the operation and operation of the system.

The conclusions are made by analyzing the work performed and the results obtained.

The special part on occupational safety and security in emergency situations is devoted to the issues of occupational safety at work.

***Key words**: cryptography, cryptanalysis, symmetric and asymmetric encryption.*