ЗАВДАННЯ
на лабораторну роботу №7
з навчальної дисципліни «Захист інформації у комп'ютерних системах»

Тема:

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ СИМЕТРИЧНОГО І АСИМЕТРИЧНОГО ШИФРУВАННЯ ТА ЇХ УРАЗЛИВОСТІ

Мета:

дослідити виявити та узагальнити особливості реалізації симетричних і асиметричних криптоалгоритмів та показників їх ефективності з метою реалізації процесів ефективного криптографічного захисту інформації для її безпечені циркуляції в локальних та глобальних комп'ютерних мережах.

Рекомендована література.

1.Навчально-методичний комплекс з дисципліни: Захист інформації в комп'ютерних системах [https://drive.google.com/drive/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d?usp=sharing].

2.Нормативні документи з питань технічного захисту інформації [http://195.78.68.84/dsszzi/control/uk/doccatalog/list?currDir=41640].

3.Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015. – 226 с. : іл.

4.Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с

5.Хорошко В.А. Методи й засоби захисту інформації / ВА Хорошко, АА Чекатков - К.: ЮНІОР, 2003.

6.Антонюк А.Ф. Основи захисту інформації в автоматизованих системах. Навчальний посібник. - К.: Академія, 2003.

7.Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

8.Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. – К.: Вид. Національної академії внутр. справ, 2012. – 104 с.

9.Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510.

І. Завдання на лабораторну роботу.

В межах масштабного проекту з розробки криптографічної системи Вам поставлене завдання розробити універсальний скрипт з використанням можливостей мови програмування Python, що вміщує у себе набір криптоалгоритмів – від простих класичних підходів до алгоритмів з високим ступенем захищеності. Результати розробки планується застосувати як підсистему криптографічного захисту корпоративної КСЗІ та в якості, що забезпечує надійний захист інформації що передається відкритими каналами зв'язку поза межами без пекового периметру КСЗІ.

Розробка скрипта здійснюється за нарощуванням функціональності.

До скрипта має бути імплементовані забоби тестування та визначення параметрів стійкості криптоалгоритма.

Скрипт повинен супроводжуватись описом криптоалгоритму: математична модель; структурна схема алгоритма або блок-схема алгоритма, діаграма класів тощо.

Завдання IV етапу – Лр№7.

1.1. Розробити програмний скрипт, що реалізує ***симетричний та (або) асиметричний криптоалгоритм за технічними умовами***, відповідно до умов варіанту, вказаному у таблиці додатку 1. Скрипт повинен реалізовувати шифрування та дешифрування текстового повідомлення, вказаного у завданні.

1.2. Здійснити взаємний обмін повідомленнями між абонентами, вказаними у таблиці додатку 1.

1.3. Розробити скрипт для дослідження стійкості криптоалгоритму шляхом його взламу. Алгоритм взламу та комбінаторні варіанти апріорної інформації, що є в наявності для криптоаналізу обрати самостійно.

1.4. Провести дослідження:

1.4.1. Залежність часу, що витрачається на шифрування та дешифрування залежно від: параметрів шифру та об'єму повідомлення, що підлягає шифруванню.

1.4.2. Залежність часу, що витрачається на взлам шифру залежно від: параметрів шифру та об'єму повідомлення, що підлягає шифруванн.

1.4.3. Результати досліджень подати у формі таблиці.

1.4.4. Сформувати висновки.

1.5. Здйснити опис розробленого скрипта, що повинен містити:

математичну модель алгоритму;

структурну схему алгоритма або блок-схему алгоритму, діаграму класів тощо та їх опис з посиланням на математичну модель криптоалгоритму;

структура Python проекту та його опис;

результати роботи скрипта, що доводять його працездатність – вхіде, вихідне повідомлення – у формі скриншотів.

Завдання І рівня складності – максимально 8 балів – полягає у виконання завдань та досліджень п.п.1.1 – 1.5, за винятком п.п. 1.3. – без досліджень стійкості криптоалгоритму.

Завдання ІІ рівня складності – максимально 10 балів – полягає у виконання завдань та досліджень п.п.1.1 – 1.5 у повному обсязі.

ІІ. Порядок виконання завдання лабораторної роботи.

1.1. Обрати завдання лабораторної роботи за рівнем складності.

1.2. Реалізувати завдання та дослідження за п.п.1.1.-1.5.

1.3. Оформити звіт з лабораторної роботи та своєчасно представити його викладачеві.

ІІІ. Структура звіту з лабораторної роботи (додаток 1).

1. Титульний аркуш, що містить інформацію: номер, тема, навчальна дисципліна, виконавець роботи, роботу прийняв.

2. Мета і завдання лабораторної роботи.

3. Результати виконання лабораторної роботи за за п.п.1.1.-1.4.

4. Висновки.

5. Підпис виконавця, викладача, що прийняв роботу.

6. Архів проекту з кодом розробленого скрипта.

7. Звіт з лабораторної роботи оформлюється відповідно до вимог 3008:2015 «ЗВІТИ У СФЕРІ НАУКИ І ТЕХНІКИ. СТРУКТУРА ТА ПРАВИЛА ОФОРМЛЕННЯ.

Технічні вимоги до звіту: аркуш формату А4 шрифтом Times New Roman 12 pt через 1,0 інтервал. Поля: зверху - 2 см, знизу - 2 см, справа - 2 см, зліва - 2,5 см, абзац - 1,25 см.

ІV. Звітність за лабораторну роботу.

Результатом виконання лабораторної роботи є:

4.1. Звіт з лабораторної роботи в електронному вигляді. Файл звіту кодується за формою:

Прізвіще_Ім'я_(укр.)_номер групи_номер лр.*

4.2. Архів проекту з кодом розробленого скрипта

4.3. Оформлений звіт надається викладачеві в електронному вигляді.

Своєчасним вважається надання звіту до початку заняття з наступної Лр.

Оформлені звітні матеріали надсилаються за адресою:

ziks582@gmail.com

V. Порядок оцінювання та захисту лабораторної роботи.

Оцінювання результатів виконання лабораторної роботи здійснюється у відповідності до положень модульно-рейтингової системи робочої програми навчальної дисципліни з урахуванням обраного студентом рівня складності завдання на лабораторну роботу.

Максимальний ваговий бал за одну роботу – 10 (з урахуванням обраного рівня складності завдання). Максимальна кількість балів за всі лабораторні роботи дорівнює

10 бала * 8 = 80 бали.

5.1. Охайне оформлення звіту з лабораторної роботи – 1 бал.

5.2. Своєчасний захист роботи – 1 бал.

5.3. Виконання роботи в повному обсязі (теоретичне обґрунтування, практична частина, пояснення отриманих результатів, висновки) – 8 балів.

*** Для умов дистанційного навчання бали за усні відповіді розподіляються по іншим пунктам та застосовуються у разі необхідності уточнення додаткових питань.

Допускається також письмове опитування.

VI. Підготовка до лабораторної роботи.

6.1. Підготовка до лабораторної роботи включає опрацювання лекційного матеріалу за темою, ознайомлення зі змістом основної і додаткової рекомендованої літератури за предметом досліджень.

6.2. Контрольні питання.

1. Технології захисту інформації з використанням крипто алгоритмів.
2. Конвеер задач криптографічного захисту та їхня сутність.
3. Класифікація шифроалгоритмів.
4. Пояснити сутність понять: криптологія, кодування, шифрування інформації
5. Сутність, призначення типи класичних шифрів.
6. Показники ефективності криптоалгоритмів.
7. Сутність, алгоритм, переваги і недоліки шифру Цезаря.
8. Сутність, алгоритм, переваги і недоліки шифру скитала.
9. Сутність, алгоритм, переваги і недоліки шифру Віженера.
10. Сутність, алгоритм, переваги і недоліки шифру Уітстона.
11. Сутність, алгоритм, переваги і недоліки потокових шифрів.
12 Сутність, алгоритм, переваги і недоліки шифрування методом гамування.
13. Алгоритми блочного шифрування – сутність, властивості,реалізація.
14. Характеристики стійкості алгоритмів блочного шифрування.
15. Алгоритми блочного шифруванн: сутність, приклади, реалізація.
16. Алгоритми потокового шифрування: сутність, приклади, реалізація.
17. Алгоритми блочного шифрування: сутність, приклади, реалізація.
18. Сучасні криптоалгоритми симетричного шифрування.
19. Симетричні криптографічні системи та їх стандарти.
20. Асиметричні криптографічні системи та їх стандарти.

професор кафедри О.Писарчук

Додаток 1

Індивідуальне завдання на виконання Лр№7

Варіант - абоненти (порядковий номер в списку групи)	Технічне завдання на розробку криптосистеми та реалізації досліджень
1 - 2	1. Обміну підлягає інформація, що міститься у файлі *.docx (doc). 2. Для криптографічного захисту інформації використовувати стандарт симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри криптоалгоритму і повідомлення обрати самостійно.
3 - 4	1. Обміну підлягає інформація, що міститься у файлі *.txt, *.docx (doc). 2. Для криптографічного захисту інформації використовувати стандарт симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри криптоалгоритму і повідомлень обрати самостійно.
5 - 6	1. Обміну підлягає інформація, що міститься у файлі *.docx (doc). 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри крипто алгоритму і повідомлення обрати самостійно.
7 - 8	1. Обміну підлягає інформація, що міститься у файлі *.txt, *.docx (doc). 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри криптоалгоритму і повідомлень обрати самостійно.
9 - 10	1. Обміну підлягає інформація, що міститься у поштовому повідомленні. 2. Для криптографічного захисту інформації використовувати стандарт симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
11 - 12	1. Обміну підлягає інформація, що міститься у поштовому повідомленні. 2. Для криптографічного захисту інформації використовувати стандарт подвійного симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
13 - 14	1. Обміну підлягає інформація, що міститься у поштовому повідомленні. 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
15 - 16	1. Обміну підлягає інформація, що міститься у поштовому повідомленні. 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
17 - 18	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджеру. 2. Для криптографічного захисту інформації використовувати стандарт подвійного симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.

19 - 20	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджера. 2. Для криптографічного захисту інформації використовувати стандарт подвійного симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
21 - 22	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджера. 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
23 - 24	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджера. 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
25 - 26	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджеру. 2. Для криптографічного захисту інформації використовувати стандарт потрійного симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
27 - 28	1. Обміну підлягає інформація, що міститься у повідомленні, переданому з використанням месенджера. 2. Для криптографічного захисту інформації використовувати стандарт потрійного симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
29 - 30	1. Обміну підлягає інформація, що міститься у файлі *.docx (doc), переданих з використанням месенджера. 2. Для криптографічного захисту інформації використовувати стандарт симетричного шифрування Data Encryption Standard (DES). 3. Алгоритм шифрування реалізувати у формі «сирого» скрипта. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.
31 - 32	1. Обміну підлягає інформація, що міститься у файлі *.txt, *.docx (doc), переданих з використанням месенджера. 2. Для криптографічного захисту інформації використовувати алгоритм асиметричного шифрування RSA. 3. Алгоритм шифрування реалізувати у формі скрипта, що базується на можливостях криптографічних бібліотек python. 4. Параметри ключів обрати максимально наближеними до алгоритму з абсолютною стійкістю.

Додаток 2

СТРУКТУРА
звіту з лабораторної роботи

Міністерство освіти і науки України
Національний технічний університет України «КПІ» імені Ігоря Сікорського
Кафедра обчислювальної техніки ФІОТ

ЗВІТ
з лабораторної роботи №1
з навчальної дисципліни «Захист інформації у комп'ютерних системах»

Тема:
ДОСЛІДЖЕННЯ ПРОЦЕСІВ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

Виконав

Перевірив

Київ 2023

І. Мета:

ІІ. Завдання:

ІІІ. Результати виконання лабораторної роботи.

ІV. Висновки.

Виконав: