Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління інформаційною безпекою, д.т.н., полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“28” травня 2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему **Удосконалення алгоритму реалізації криптографічного методу RSA**

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Юрій НЕНЕКА
(прізвище та ініціали)
Керівник Наталія КУХАРСЬКА
(прізвище та ініціали)
Рецензент Андрій МЕЛЬНИЧИН
(прізвище та ініціали)

Львів – 2021

АНОТАЦІЯ

Ненека Юрій «Удосконалення алгоритму реалізації криптографічного методу RSA». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 55 сторінок, 6 рисунків, 3 таблиці, 38 джерела.

Об'єкт дослідження – процес удосконалення алгоритму реалізації криптографічного методу RSA.

Предмет дослідження – програмний код, що виконує функції шифрування та розшифрування текстових повідомлень з використанням криптографічного алгоритму RSA.

Мета роботи – розробити додатковий алгоритм, застосування якого підвищить криптографічну стійкість шифру RSA та апробувати його.

У дипломній роботі бакалавра розглянуто питання захисту інформації, криптографічні методи захисту інформації. Проаналізовано предмет криптографії та її актуальність, принцип роботи криптографічного алгоритму RSA. Описано процес програмної реалізації мовою програмування *Python* удосконаленого криптографічного алгоритму *RSA*.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, КРИПТОГРАФІЯ, RSA, PYTHON.

ABSTRACT

Neneka Yuriy "Improvement of the algorithm for implementing the cryptographic method RSA". Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 56 pages, 29 figures, 3 tables, 38 sources.

The object of research is the process of improving the algorithm for implementing the cryptographic method RSA.

The subject of research is program code that performs the functions of encryption and decryption of text messages using the cryptographic algorithm RSA.

The purpose of the work is to develop an additional algorithm, the application of which will increase the cryptographic stability of the RSA cipher and test it.

In the diploma work of the bachelor the questions of information protection, cryptographic methods of information protection are considered. The subject of cryptography and its relevance, the principle of operation of the cryptographic algorithm RSA are analyzed. The process of software implementation of the RSA advanced cryptographic algorithm in the Python programming language is described.

INFORMATION SECURITY, INFORMATION PROTECTION, CRYPTOGRAPHY, RSA, PYTHON.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі для шифрування текстових конфіденційних повідомлень запропоновано та реалізовано мовою програмування Python підхід до вдосконалення алгоритму шифрування RSA.

У першому розділі описано актуальність питання забезпечення цілісності, конфіденційності та достовірності інформації за допомогою використання методів криптографії. У сучасних інформаційних системах люди часто обмінюються даними. Для того щоб бути впевненими в тому, що інформація не буде піддана перекручуванням, або не буде підмінена цілком. Отже, метою застосування криптографічних методів є захист інформаційної системи від цілеспрямованих атак з боку зловмисника.

У другому розділі зроблено огляд основних класів шифрів, розглянуто їхні відмінності, виокремлено головні переваги та недоліки. Однією з проблем більшості шифрів є великі витрати при використанні. На практиці ні одна з криптосистем не є абсолютно стійкою. На сьогоднішній день найкращий показник стійкості мають асиметричні системи шифрування, зокрема RSA.

У третьому розділі розглянуто криптографічний метод шифрування – RSA, вказано на його недоліки. Запропоновано підхід до вдосконалення шифру RSA за допомогою використання процедури розбивання текстового повідомлення на блоки та додаткових алгоритмів заплутування всередині них. Здійснено програмну реалізацію удосконаленого методу шифрування/розшифрування мовою програмування Python версії 3.9 IntelliJ IDEA Community Edition 2018.3.5.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.

2. Алферов А.П.,Зубов А.Ю.,Кузьмин А.С.,Черемушкин А.В. Основы криптографии: Учебное пособие. — М.: Гелиос АРВ, 2001. — 480 с.

3. Арустамов Е.А.Безпека життєдіяльності: Навчальний посібник. // Воронін В.О., Зенченко А.Д., Смирнов С.А. // Видавничо-торгова корпорація "Дашков і К" // 2005р. //

4. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979. — 535 с.

5. Баканов М.И. Экономичесикй анализ / М.И. Баканов, А.Д. Шеремет. – Москва: ФиС, 2001. - 654с.

6. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: «Горячая линия – Телеком». 2001. 140с.

7. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.

8. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. М.: «Вильямс», 2002. - 499с.

9. Бондарь А. InterBase и Firebird. Практическое руководство для умных пользователей и начинающих разработчиков / А. Бондарь. – СПб.: БХВ-Петербург, 2007. – 592 с. ISBN 978-5-9775-0098-2.

10. Брюс Шнайер. Прикладная криптография. М.: «Триумф», 2006. - 608с.

11. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ

БЖД, 2020, 249 с. (С.121-124).

12. Введение в криптографию. / Под ред. В.В. Ященко. — 2-е изд., испр. — М.: МЦНМО: «ЧеРо», 2006. — 272 с.

13. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів "Проблеми та перспективи розвитку системи безпеки життєдіяльності" (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

14. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.

15. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція "Інформаційна безпека в сучасному суспільстві" (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

16. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. — М.: «ТЕИС», 1999. — 69 с.

17. Економічні вказівки до виконання організаційно-економічного розділу дипломних проектів та курсових робіт з дисципліни «Економіка і організація виробництва» / Г.К. Яловий, В.П. Пашин, В.С. Сичов. – Київ: НТУУ «КПІ». 2007 – 99с

18. Кнут Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы. — М.: Мир, 1977. — 724 с.

19. Лагун А.Е., Полотай О.І. Особливості приховування інформації в зображеннях з використанням молодшого значущого біта. Вісник ЛДУ БЖД. – 2019. –№ 20. – С. 17-22.

20. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

21. Мельник Л.Г. Экономика предприятия / Л.Г. Мельник – Сумы: Университетская книга, 2003. – 638с

22. Молдовян А.А, Молдовян Н.А., Советов Б.Я. Криптография. — СПб.: «Лань», 2000. — 224 с.

23. О.Белей, Н.Мальцева, О.Полотай Фізичний зміст комп'ютерної стеганографії. Вісник Львівського Державного університету безпеки життєдіяльності Том 23 (2021):. С. 27-32.

24. Полотай О.І., Гриник Р.О. Застосування генетичного алгоритму для розкриття ранцевої криптосистеми Меркля-Хелмана Вісник ЛДУ БЖД. – 2016. – Т. 21, № 2. – С. 201-206.

25. Полотай О.І., Гриник Р.О. Побудова інтелектуальної моделі криптоаналізу шифру Рабіна на базі генетичного алгоритму. Інформаційна безпека та комп'ютерні технології" ("Information Security and Computer Technologies") : Збірник тез доповідей Міжнародної науково- практичної конференції, 24-25 березня 2016 року, м. Кіровоград: КНТУ, 2016. – С. 24-26.

26. С. Панасенко. Алгоритмы шифрования. Специальный справочник. Санкт-Петербург: «БХВ- Петербург». 2009. 577с.

27. Савицкая Г.В. Экономический анализ / Г.В. Савицкая – Москва: Новое Издание, 2004. – 640с.

28. Савчук А.Н. Основы охраны труда // Просвещение // 2000р.

29. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.

30. Советов Б.Я. Криптография. — СПб.: «Лань», 2000. — 224 с.

31. Ухлинов А.М. Управление безопасностью информации в автоматизированых системах. - М.: МИФИ, 2011.

32. Фримен Э., Сьерра К., Бейтс Б. Паттерны проектирования. – СПб.: Питер, 2011. – 656 с.

33. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.

34. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

35. Alan G. Konheim. Computer security and cryptography. NJ. USA. 2006. 350p.

A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 с.

36. O.Polotai, Kukharska, N., Lagun, A. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 174–177.

37. RSA алгоритм. Шифровка. Информационная безопасность, криптография, тайнопись. Простые числа. [Електронний ресурс]. Доступний за адресою:[https://www.youtube.com/watch?v=xqPgE-hPIfE]

38. Specification for the Advanced Encryption Standard (AES). [Електронний ресурс]. Доступний за адресою:[http://csrc.nist.gov / publications/fips/fips197/fips-197.pdf], 10.01.2015.