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
«___» _____ 2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему: «Побудова системи криптографічного захисту інформації на основі використання методу Triple DES»

Виконав:
здобувач 4-го курсу, групи КБ-41
спеціальності (освітньої програми)
125 “Кібербезпека"
Управління інформаційною безпекою
(шифр і назва спеціальності (освітньої програми))
Павло БРОВЧУК
(прізвище та ініціали)
Керівник Наталія КУХАРСЬКА
(прізвище та ініціали)
Рецензент Лах Ю. В.
(прізвище та ініціали)

Львів-2021

АНОТАЦІЯ

Бровчук П.В. “Побудова системи криптографічного захисту інформації на основі використання методу Triple DES”. Дипломна робота з спеціальності 125 “Кібербезпека” складається з текстової частини, що містить 3 розділи, 58 с., 2 таблиці, 15 рис., 43 джерела.

Об’єкт – процес шифрування конфіденційних повідомлень.

Мета роботи – побудувати систему криптографічного захисту інформації на основі шифру Triple DES з використанням мови програмування Python.

У дипломній роботі бакалавра описано можливі варіанти захисту інформації в автоматизованих системах, визначено місце криптографічних систем у сфері інформаційної безпеки.

Зроблено аналіз криптографічних методів шифрування та розшифрування даних. Описано алгоритм Triple DES методів шифрування та розшифрування конфіденційної інформації, сформульовано практичні рекомендації щодо шифрування та розшифрування даних на основі використання мови програмування Python.

КРИПТОГРАФІЯ, АЛГОРИТМ ШИФРУВАННЯ TRIPLE DES, ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ, PYTHON.

ABSTRACT

Brovchuk P.V. "Building a system of cryptographic data protection based on the use of the Triple DES method." Thesis in the specialty 125 "Cybersecurity" consists of a text part that has 3 chapters, 58 pages, 2 tables, 15 figures, 43 references.

The object of the work is the process of hiding confidential messages using the Triple DES encryption algorithm.

The aim of the work is to write on the basis of the Python programming language an algorithm for encrypting and decrypting Triple DES to hide confidential information in messages.

In the thesis are described possible variants of data protection in automated systems and is determined the place of cryptographic systems in the field of information security.

There was made the analysis of cryptographic methods of data encryption and decryption. There is described the algorithm of Triple DES methods of encryption and decryption of confidential information, and are formulated practical recommendations on data encryption and decryption based on the use of Python programming language.

CRYPTOGRAPHY, TRIPLE DES ENCRYPTION ALGORITHM, ENCRYPTION AND DECRIPTION OF CONFIDENTIAL INFORMATION, PYTHON.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі процедури шифрування та розшифрування секретного текстового повідомлення реалізовано мовою програмування Python на основі використання блочного шифру з симетричним ключем Triple DES.

У першому розділі описано основні поняття та підходи до захисту інформації, а також наслідки, які можуть виникнути в результаті атаки на інформацію, а саме: економічні втрати та моральна шкода. Визначено що інформація з точки зору інформаційної безпеки характеризується такими категоріями, як конфіденційність, цілісність, автентичність, апельованість, а з точки зору інформаційних систем надійністю, точністю, контролем доступу, контрольованістю, контролем ідентифікації, стійкістю до навмисних збоїв. Також розглянуто можливі методи захисту інформації, зокрема криптографічний захист.

У другому розділі докладно описано основні етапи алгоритму шифрування Triple DES та виокремлено основні сфери його застосування, а саме для приховування секретних повідомлень, захисту банківських даних. Також виявлено відмінності та побудовано структурну схему головних відмінностей алгоритмів шифрування DES та Triple DES. Реалізовано порівняння основних типів криптографічних шифрів та побудовано схему якості криптографічного захисту.

У третьому розділі розглянуто основні аспекти реалізації алгоритмів шифрування/розшифрування Triple DES мовою програмування Python.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ashwini, R. T. and Akshay, P. D. 2014. Review paper on FPGA based implementation of Advanced Encryption Standard (AES) algorithm. IJARCCE International Journal of Advanced Research in Computer and Communication Engineering, 3 (1).

2. Blomgren, P. and Kotronx, S.M. 2006 Cryptographic Protection of SCADA Communications. American Gas Association (AGA).

3. Brar, R. S. and Singh, S. 2013. Efficient Cryptography with Compression / Decompression Mechanism of Text Files against IP Spoofing., International Journal of Application or Innovation in Engineering and Management, (IJAIEM), 2 (7) .

4. Gong-bin Q. and Qing-feng J., and Shui-sheng Q. 2009 A new image encryption scheme based on DES algorithm and Chua's circuit, IEEE International Workshop on Imaging Systems and Techniques, pp. 168- 172.

5. Grabbe, O. 2011. The DES algorithm illustrated, Laissez Faire City, Vol. 2.

6. Jeffrey, H. and Pipher, J. and Silverman, J. H. 2008 .An Introduction to Mathematical Cryptography, Springer, New York.

7. Julia, J. and Ramlan, M., Salasiah, S. and Jazrin, R. 2012. Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key. International Journal of Cyber-Security and Digital Forensics,1 (3).

8. Ling, D. and Kefei, Ch. S. 2012. Cryptographic Protocol. Springer.

9. Magesh, B. V. T. Shankar Ganesh, K. 2014. A Comparative Analysis on Encryption and Decryption Algorithms. International Journal of Scientific and Research Publications. 4(12).

10. Manfred, L. and Johannes, M. 1986. American National Standard for Financial Institution Message Authentication, American Bankers Association.

11. 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.

12. Premnath, A.P. 2010. Application of NTRU Cryptographic Algorithm for securing SCADA communication. M.Sc. Thesis. Department of Computer Science .University of Nevada.

13. Priyan, K. and Vishal, P. 2016. Design and Implement Dynamic Key Generation to Enhance DES Algorithm. International Journal for Research in Applied Science & Engineering Technology, 4(7).

14. Rabah, K. 2005. Theory and implementation of data encryption standard . Information Technology Journal, 4: 307-325.

15. Rahul, L. and Gaurav, P. 2015. Implementation of AES-256 Bit. Inventi Journals, Information Security Volume. (issue3).

16. Rhee, M.Y. 2003. Internet Security: Cryptographic Principles, Algorithms and Protocols. Wiley. England.

17. Schneier, B. 1994. Description of a new variable-length key, 64-bit block cipher (blowfish) Springer pp. 191-204.

18. 'Souza, R. 2001. The NTRU Cryptosystem: Implementation and Comparative Analysis. Semester Project. George Mason University.

19. Vilas, V.D. and Dinesh, V.P. and Ashok, S. W. 2014. Performance Evaluation of AES using Hardware and Software Codesign. IJRITCC International Journal on Recent and Innovation Trends in Computing and Communication, 2 (6): 1638 – 1643.

20. Washington, D.C. 1982. America National Standard for Personal Identification Number (PIN) Management and Security. American Bankers Association.

21. Washington, DC. 1977 .Data Encryption Standard, Federal Information Processing Standards Publication (FIPS Pub) 4, National Bureau of Standards,

22. William, S. 2006. Cryptography and Network Security Principles and Practice, 5th edition.Prentice Hall

23. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 256 с.

24. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

25. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

26. Бабаш А. В. Криптография. – М.: СОЛОН-Пресс, 2007. – 511 с.

27. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии: Учебное пособие. М.: Горячая Линия - Телеком, 2002. – 175 с.

28. Бернет С., Пэйн С., Криптография. Официальное руководство RSA Security. Изд. 2-е, стереотипное. – М.: ООО «Бином-Пресс», 2007. – 384 с.: ил.

29. 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).

30. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

31. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей ІІ 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.

32. 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.

33. 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.

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

35. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006.–320 с.

36. Мухачев В.А., Хорошко В.А. Методы практической крипто-графии. К.: ООО Полиграф-Консалдинг, 2005. – 209 с.

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

38. 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.

39. 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.

40. Ростовцев А.Г. Алгебраические основы криптографии. М.: НПО «Мир и семья», ООО «Интерлайн», 2000. – 256 с.

41. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. М.: Издательство: АНО НПО "Профессионал", 2005. – 480 с.

42. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005. – 229 с.

43. 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).