ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

Факультет математики, фізики, комп'ютерних наук і технологій

Кафедра математики та інформатики

ДИПЛОМНА РОБОТА

на тему:

«Криптографічний захист електронного журналу вчителя»

Студента 2 курсу МСОІ групи
Галузь знань 01 Освіта / Педагогіка
Спеціальності 014 Середня освіта
(Інформатика)
СВО магістра
Трохимчука Василя Анатолійовича (підпис)

Керівник: кандидат педагогічних наук,
старший викладач
кафедри математики та інформатики
Косовець Олена Павлівна

Розширена шкала _____
Кількість балів_____ Оцінка: ECTS_____
Голова комісії_____ _____
(підпис) (ініціали, прізвище)
Члени комісії_____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)
_____ _____
(підпис) (ініціали, прізвище)

Вінниця – 2020

ТЕМА ДИПЛОМНОЇ РОБОТИ АНГЛІЙСЬКОЮ МОВОЮ: Cryptographic protection of the teacher's electronic journal

АНОТАЦІЯ

У даній дипломній роботі розглянуто методи і засоби захисту інформації в електронних журналах вчителя від несанкціонованого доступу, а також дано повний опис можливих каналів витоку відомостей про навчальну діяльність учнів.

З прийняттям в Україні законів «Про електронний цифровий підпис», «Про електронні документи і електронний документообіг» перед вчителями виникла необхідність організації і впровадження систем конфіденційного зв'язку, на основі ухвалення самостійних рішень, що вимагають певного рівня підготовки в області криптографічного захисту інформації.

Метою роботи є доступний і компактний виклад основних понять і підходів до технологій криптозахисту електронних журналів, які використовуються в практичній діяльності вчителя закладів загальної середньої освіти.

Об'єктом дослідження є технології криптографічного захисту електронних класних журналів вчителя закладів загальної середньої освіти.

Предметом дослідження є криптографічні методи захисту інформації електронних журналів вчителя закладів середньої освіти.

Ключові слова: технології криптографічного захисту, електронний журнал вчителя інформатики, технологій криптозахисту електронних журналів.

ABSTRACT

This thesis discusses the methods and means of protecting information in electronic journals of teachers from unauthorized access, as well as gives a complete description of possible channels of leakage of information about students' learning activities.

With the adoption in Ukraine of the laws "On electronic digital signature", "On electronic documents and electronic document management" before teachers there was a need to organize and implement confidential communication systems, based on independent decisions that require a certain level of training in cryptographic information protection.

The aim of the work is an accessible and compact presentation of the basic concepts and approaches to cryptographic technologies of electronic journals, which are used in the practical activities of teachers of general secondary education.

The object of research is the technology of cryptographic protection of electronic class journals of teachers of general secondary education.

The subject of the research is cryptographic methods of information protection of electronic journals of secondary school teachers.

Keywords: cryptographic protection technologies, electronic journal of computer science teacher, cryptographic protection technologies of electronic journals.

ЗМІСТ

ВСТУП

У сучасних умовах дистанційного навчання захист інформації стає усе більш актуальною і одночасно усе більш складною проблемою. Це обумовлено як масовим застосуванням методів автоматизованої обробки даних, так і широким поширенням методів і засобів несанкціонованого доступу до даних. Тому особливу роль в організації навчального процесу методи протидії потенційним загрозам займає підхід, при якому засоби захисту інформації використовуються комплексно, кожне відповідно до свого навчального призначення.

Різні методи і засоби захисту інформації в електронних журналах вчителя від несанкціонованого доступу, а також досить повний опис можливих каналів витоку відомостей, представлені в нашій роботі.

З прийняттям в Україні законів «Про електронний цифровий підпис», «Про електронні документи і електронний документообіг» перед вчителями виникла необхідність організації і впровадження систем конфіденційного зв'язку, на основі ухвалення самостійних рішень, що вимагають певного рівня підготовки в області криптографічного захисту інформації.

Як правило, користувачі використовують різні комерційні криптозасоби, які розробляються з використанням типових криптовузлів і методів, виходячи з рекомендацій відповідних міжнародних стандартів.

Внаслідок цього комерційні криптозасоби (при відповідній класифікації) мають аналогічні властивості і особливості, у багатьох відношеннях визначувані лише специфікою вибору параметрів криптоалгоритмів (у тому числі, ключів). Тому якісні стандартизовані криптоалгоритми можуть мати (і дійсно володіють) слабкості, залежні від конкретних значень їх параметрів.

У дипломній роботі подано коло питань, пов'язаних з мотивуванням вибору параметрів поширених криптоалгоритмів і процедур їх генерації у процесі захисту вчителями класного журналу.

Актуальність теми очевидна, оскільки інформація в сучасному суспільстві - одна з найцінніших речей в житті, що вимагає захисту від несанкціонованого проникнення осіб, що не мають до неї доступу.

Метою роботи є доступний і компактний виклад основних понять і підходів до технологій криптозахисту електронних журналів, які використовуються в практичній діяльності вчителя закладів загальної середньої освіти.

Об'єктом дослідження є технології криптографічного захисту електронних класних журналів вчителя закладів загальної середньої освіти.

Предметом дослідження є криптографічні методи захисту інформації електронних журналів вчителя закладів середньої освіти.

У теоретичній частині дипломної роботи розглянуті питання про науку криптологію, напрям її криптографії і основні методології криптографічного захисту інформації.

Особливості вибору параметрів блокових шифрів проілюстровані на прикладі режиму простої заміни. Для цього шифру розглянуті елементарні приклади слабких ключів, приведена загальна методика побудови підобласті стійких довготривалих ключів і їх тестування.

При виконанні практичної частини дипломної роботи, присвяченої реалізації технологій захисту електронного журналу вчителя, використаний електронний журнал, який дозволяє створити розклад класу, додавання батька, формування учбового плану, звіт за звідними оцінками, форма відправки повідомлень, форма виставляння оцінок, список журналів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдошин С.М., Савельева А.А. Алгоритм решения систем линейных уравнений в кольцах вычетов. *Информационные технологии*. 2006. № 2. с.50-54.

2. Бунин О. Занимательное шифрование. *Мир ПК*. 2003 № 7.

3. Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США. *Системы безопасности*. М.: Гротэк, 2001, №№1, 2.

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

5. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

6. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронно-цифровой подписи на базе асимметричного криптографического алгоритма.

7. Додохов А.Л., Сабанів А.Г. Дослідження застосування СУБД Oracle для захисту персональних даних. *Доповіді Томського державного університету систем управління і радіоелектроніки*, 2011, №2(24), С.267-270.

8. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии. *Современные тенденции технических наук: материалы IM Междунар. науч. конф.* Казань : Бук, 2015. С.10-13.

9. Иванов К. К., Юрченко Р. Н., Ярмонов А. С. Алгоритмы шифрования данных. *Молодой ученый*. 2016. № 29 (133). С. 18-20. URL: https://moluch.ru/archive/133/37180/ (дата обращения: 14.10.2020).

10. Иванов М.А. Криптографические методы защиты информации в

компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2011. 368 с.

11. Крысин А. В. Информационная безопасность. Практическое руководство М.: СПАРРК, К.:ВЕК+,2013.

12. Курило А. Информационная безопасность в организации: взгляд практика. *Открытые системы*, #07-08. 2002.

13. Лукашов И. В. Криптография? Железно! *Мир ПК*. 2013. № 3.

14. Нил Стивенсон Криптономикон. 1999 г.

15. Отставнов М. Краткий путеводитель по миру PGP. *Компьютерра*, №48, 1997.

16. Панасенко С. П. Защита информации в компьютерных сетях. *Мир ПК*. 2016. № 2.

17. Панасенко С. П. Чтобы понять язык криптографов. *Мир ПК*. 2016. № 5.

18. Панасенко С. П. Чтобы понять язык криптографов. *Мир ПК*. 2016. № 6.

19. Панасенко С. П., Ракитин В. В. Аппаратные шифраторы. *Мир ПК*. 2002. № 8

20. Партыка Т. Л., Попов И. И. Информационная безопасность : учеб. пособие для студентов учреждений среднего профессионального образования. М.: ФОРУМ: ИНФРА-М, 2004.

21. Тарасюк М. В. Защищенные информационные технологии. Проектирование и применени. М.: СО- ЛОН-Пресс, 2004.

22. Шеннон К.Э. Работы по теории информации и кибернетике. М.: И.Л., 1963, с. 333-402.

23. Adleman L. A Subexponential Algorithm for the Discrete Logarithm with Application to Cryptography, Proc. IEEE 20-th Annual Symposium on Foundations of Computer Science (FOCS), 1979.

24. ANSI X3.92, “American National Standard for Data Encryption Algorithm (DEA),” American National Standards Institute, 1981.

25. Coppersmith D., Odlyzko A., Schroeppel R. Discrete logarithms in GF(p). *Algorithmica*. 1986. V. 1. pp. 1-15.

26. Diffie W., Hellman M.E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, v. IT-22, n. 6, Nov 1976, pp. 644 - 654.

27. ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, v. IT-31, n. 4, 1985, pp. 469-472.

28. FIPS PUB 186. Digital Signature Standard (DSS).

29. FIPS PUB 186-2. Digital Signature Standard (DSS).

30. Gordon L.A., Loeb M.P., Lucyshyn W., Richardson R. CSI/FBI Computer Crime and Security Survey 2005. *Computer Security Institute Publications*, 2005 - 26 p.

31. International Organization for Standardization. *Code of Practice for Information Security Management* / ISO 17799.

32. International Organization for Standartization. *The Common Criteria for Information Technology Security Evaluation* . ISO 15408.

33. Lieven M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414. 20–27 Dec. 2001.

34. Odlyzko A.M. Discrete logarithms: The past and the future. AT&T Labs-Research, 1999.-25 p.

35. RIJNDAEL description. Submission to NIST by Joan Daemen, Vincent Rijmen. http://csrc.nist.gov/encryption/aes/round1/docs.htm.

36. Rivest R.L., Shamir A., Adleman L.M. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, v. 21, n. 2, Feb 1978, pp. 120-126.

37. Schirokauer O. Discrete logarithms and local units. Phil. Trans. R. Soc. Lond. A. 1993. V. 345. pp. 409—423.

38. Schneier B. Snake Oil, Crypto-Gram <*http://www.counterpane.com/Crypto-Gram.html*>, February, 1999.

39. Uniform Rating System for Information Technology. Federal financial institutions examination council.1999 - 11 p.