Д/р
13986

Одеський національний університет імені І. І. Мечникова

Інститут інформаційних та соціальних технологій

кафедра системного програмного забезпечення та технологій дистанційного навчання

Дипломна робота

бакалавра (СД)

на тему: **«Analysis and data encryption using by capacities of Cryptology Studio»**

«Аналіз та шифрування інформації засобами Cryptology Studio »

Текст: диск.

Виконав: студент **денної** форми навчання
Напрям підготовки **6.050102**
Дороганов Євгеній Олександрович
Керівник Ходиревська І.Ю.
Рецензент к. фіз.-мат. н., доц. Гоцульський В.Я.

Рекомендовано до захисту:
Протокол засідання кафедри
№ 10 від 31.05 2017 р.

Завідувач кафедри
(підпис) Альошин О.М.

Захищено на засіданні ЕК № 4
протокол № 23 від 26.06 2017 р.

Оцінка відмінно / A / 97
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК
(підпис) Шварц.О.І.

Одеса – 2017

790/04

CONTENTS

Introduction 3
Chapter 1. Justification of the relevance of the work, the formation of the problem and its current state. 6
Chapter 2. Methods and algorithms of modeling 14
Section 2.1.Algorithms and functions in Cryptology Studio 14
Section 2.2.Metro Framework, as a template for the user interface of the program. 55
Section 2.3. The interface of Cryptology Studio. 57
Chapter 3. Functionality for registered and unregistered users. 61
Section 3.1. Two-factor registration system in the program Cryptology Studio 61
Section 3.2. A set of tools for registered users 62
Section 3.3 A toolkit for unregistered users. 66
Chapter 4. Results of testing the program Cryptology Studio 70
Conclusions 73
Bibliography 75

Introduction

Modern society is the main generator of the information environment and full consumer of it. Based on this fact, it can be said with certainty, that during this development develops, internal continuous connections and dependencies arise between users of the global, or separately taken, information space. Since the time when small groups of people began to form tribes, settlements, cities, empires, and ending with today, in the course of time, inside such human ones, or, in terms of the newest period of the development of society, within man-machine infrastructures, information volumes were arising, which for one or some another reasons was not disclosed or could not be disclosed - in other words, secrets appeared inside the information exchange system. Secrets, or secret information, humanity is trying to disguise and better hide from the enemies since the Egyptian pharaohs. The more rapidly the society developed, the more sophisticated the methods of controlled distortion of information-its encryption. Until the 19th century, all encryption was "manual", i.e. it was completely performed by a person's hand. With the advent of complex computational mechanisms and rotary machines, part of this task fell on mechanisms. But when powerful computers entered the life of mankind, the role of man in this process was reduced to a minimum and consisted in the development of such algorithms of new generation of encryption that would enable the information so transformed by using the power of computer technology that the enemy could in no way be able to Declassify. The complexity of methods and algorithms of encryption increases in direct proportion to the rapid development of the computers themselves. Today, a lot of algorithms which have been developed, are sufficiently capable of preserving the integrity and confidentiality of information, taking into account the modern capabilities of computing computer technology. The most popular algorithms in the modern information environment are symmetric algorithms - DES, 3DES, AES, - and asymmetric algorithms, such as RSA-1024, RSA-2048 bits. No matter how well the algorithms for strong data encryption were designed and implemented,

neither of them will guarantee full information security, and this result can only be achieved by conjuncture of several algorithms of various types.

This direction has developed gradually and consistently, therefore the entire development process is a perfectly formed structured sequence of discoveries and innovations. Proceeding from this, we can safely say that there are very few gaps and shortcomings in such a direction of scientific and practical activity. But, unfortunately, it is impossible not to say that often people who begin to learn cryptology and experts working in the field of computer security, neglect information related to cryptographic analysis and the study of older, at first glance, irrelevant, algorithms. On the other hand, all new algorithms to some extent are improved, extended and modified versions of older, unusable algorithms. Even a cipher, unknown to society, obtained by combining and compiling several obsolete ciphers, can cause considerable difficulties for people and specialists unfamiliar with the structure and structure of not actual encryption algorithms.

Therefore, the purpose of this study is to create a holistic software that would be a powerful tool that includes both various encryption algorithms, as well as the ability to analyze information and manipulate encrypted data. Such software should provide an opportunity to work with old, no longer used ciphers, to train future computer security specialists in the basics of cryptology science, and with the latest encryption algorithms, which make it possible to encrypt the original information so that the enemy can not recover it.

The main objectives of this study include:

1. Analysis and implementation of actual encryption algorithms and analysis methods.
2. Introduction of historically known algorithms, for possible teaching cryptography of students and schoolchildren.
3. Develop a user-friendly interface.
4. Ensuring the integrity of the product.
5. Control of compliance of available algorithms with modern standards of their use.

Since modern society is rapidly developing and the amount of information it produces is steadily growing, the volume of classified information is also increasing. To ensure that the user's personal information is always a secret, he needs to at least get a little acquainted with the basic concepts of information security. This direction is already topical now, and the expediency of such a study is that such a program will help to easily teach students, schoolchildren and people interested in cryptography, not only the basics of information security, but also the more complex, topical to date methods of controlled distortion Information, while addressing some aspects of cybersecurity.

Conclusions

In the result of writing a thesis and researching the cryptographic component of the information environment, a software product was developed called Cryptology Studio, which has a wide range of capabilities, functions and algorithms. This result of the study can be assessed as "excellent", because in the course of writing the work, not only was a large number of cryptographic algorithms implemented, but also the possibility of analyzing information was included. Since all algorithms and analysis processes are often interrelated, the Cryptology Studio program will become an indispensable tool for people who are trying to learn the basics of information security and learn how to analyze the data received after encryption and decryption. The scientific value of this program can be attributed not only to the presence of a number of known encryption, hashing and analysis algorithms, but also the unprecedented way to send e-mail from the program, where such a message can be both ordinary and encrypted, and it can be deciphered Only knowing the key and having the program Cryptology Studio at hand. Also, the scientific value of the program can be attributed to the fact that it can be used for permanent training of schoolchildren, students and people who want to get acquainted with the subject of information security. Also, methodologists, with ease, can include Cryptology Studio in programs, courses and teaching methods, as it represents a balanced complex of clear and unobtrusive interface, powerful and fast encryption algorithms, convenient and simple analysis methods.

This software product can be installed on any personal computer, since it consumes a minimum of RAM and does not burden the computer processor in any way. The practical value of the program is precisely the minimum consumption of resources, the speed of work in complex tasks and clear design. Such a product can be used in teaching and reading computer security subjects, both in universities and colleges, vocational schools, lyceums and, even, in schools.

To start working with this program, the user only needs to install it, register if he wants to use all the power of the program, and enjoy. No ads, no intrusive forms and complex, incomprehensible design. And in return - minimalist design, high speed of work, completely free access, as well as integrity, simplicity.

Only power! Only security! Only Cryptology Studio!

Bibliography

1. Suetonius, *Vita Divi Julii* 56.6
2. https://en.wikipedia.org/wiki/Caesar_cipher - cite_ref-2 *Luciano, Dennis; Gordon Prichett (January 1987). "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". The College Mathematics Journal. **18** (1): 2–17. doi:10.2307/2686311. JSTOR 2686311.*
3. *"Intro to Numbers Stations". Retrieved 13 September 2014.*
4. *"The only unbreakable cryptosystem known—the Vernam cipher". Pro-technix.com. Retrieved 2014-03-17.*
5. *"One-Time Pad (OTP)". Cryptomuseum.com. Retrieved 2014-03-17.*
6. *Shannon, Claude (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal. **28** (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.*
7. *Miller, Frank (1882). Telegraphic code to insure privacy and secrecy in the transmission of telegrams. C.M. Cornwell.*
8. ^ Jump up to:[a] [b] *Bellovin, Steven M. (2011). "Frank Miller: Inventor of the One-Time Pad". Cryptologia. **35** (3): 203–222. doi:10.1080/01611194.2011.583711. ISSN 0161-1194.*
9. *"'Secret signaling system patent' on Google.Com". google.com. Retrieved 3 February 2016.*
10. *Kahn, David (1996). The Codebreakers. Macmillan. pp. 397–8. ISBN 0-684-83130-9.*
11. *"One-Time-Pad (Vernam's Cipher) Frequently Asked Questions, with photo". Retrieved 2006-05-12.*
12. *Savory, Stuart (2001). "Chiffriergerätebau : One-Time-Pad, with photo" (in German). Retrieved 2006-07-24.*
13. *Kahn, David (1967). The Codebreakers. Macmillan. pp. 398 ff. ISBN 0-684-83130-9.*
14. *Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4.*
15. *Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. p. 142. ISBN 978-0-19-162588-6.*
16. *Smith, Laurence D. (1943). "Substitution Ciphers". Cryptography the Science of Secret Writing: The Science of Secret Writing. Dover Publications. p. 81. ISBN 0-486-20247-X.*
17. http://practicalcryptography.com/ciphers/homophonic-substitution-cipher
18. http://practicalcryptography.com/ciphers/rail-fence-cipher/
19. Andrei Popov (February 2015). *Prohibiting RC4 Cipher Suites*. RFC 7465.

20. *Lucian Constantin (14 May 2014). "Microsoft continues RC4 encryption phase-out plan with .NET security updates". ComputerWorld.*
21. J. Katz; Y. Lindell (2014), *Introduction to Modern Cryptography*, Chapman and Hall/CRC, p. 77
22. Rivest, Ron; Schuldt, Jacob (27 October 2014). "Spritz – a spongy RC4-like stream cipher and hash function". Retrieved 26 October 2014.
23. *"FIPS 81 - Des Modes of Operation". csrc.nist.gov. Retrieved 2009-06-02.*
24. *"FIPS 74 - Guidelines for Implementing and Using the NBS Data". Itl.nist.gov. Retrieved 2009-06-02.*
25. *Merkle, Ralph; Hellman, Martin (July 1981). "On the Security of Multiple Encryption"(PDF). Communications of the ACM. **24** (7): 465–467. doi:10.1145/358699.358718.*
26. *van Oorschot, Paul; Wiener, Michael J. (1990). A known-plaintext attack on two-key triple encryption. EUROCRYPT'90, LNCS 473. pp. 318–325. CiteSeerX 10.1.1.66.6575*
27. Stefan Lucks: *Attacking Triple Encryption* (PDF), Fast Software Encryption 1998, pp 239–253.
28. Eli Biham: *How to Forge DES-Encrypted Messages in 2^{28} Steps* (PostScript), 1996.
29. Steven Levy, Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age, ISBN 0-14-024432-8, 2001.
30. Lars R. Knudsen, Vincent Rijmen, Ronald L. Rivest, Matthew J. B. Robshaw: On the Design and Security of RC2. Fast Software Encryption 1998: 206–221
31. John Kelsey, Bruce Schneier, David Wagner: Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. ICICS 1997: 233–246
32. *"Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.*
33. John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". *New York Times*.
34. Westlund, Harold B. (2002). "NIST reports measurable success of Advanced Encryption Standard". *Journal of Research of the National Institute of Standards and Technology*. Archived from the original on 2007-11-03.
35. *"Espacenet - Bibliografische Daten" (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.*
36. *"Espacenet - Bibliografische Daten" (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.*
37. *Garfinkel, Simson (December 1, 1994), PGP: Pretty Good Privacy, O'Reilly Media, pp. 101–102, ISBN 978-1-56592-098-9*
38. Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"

39. *Boneh, Dan (1999). "Twenty Years of attacks on the RS Cryptosystem". Notices of the American Mathematical Society. **46** (2): 203 213.*
40. A Course in Number Theory and Cryptography, Graduate Texts in Math. No 114, Springer-Verlag, New York, 1987. Neal Koblitz, Second edition, 1994. p 94
41. Johnson, J.; Kaliski, B. (February 2003). "Public-Key Cryptography Standard (PKCS) #1: RSA Cryptography Specifications Version 2.1". *www.ietf.org* Network Working Group. Retrieved 9 March 2016.
42. *Ciampa, Mark (2009). CompTIA Security+ 2008 in depth. Australia ; Unite States: Course Technology/Cengage Learning. p. 290.*
43. *Chad R, Dougherty (31 Dec 2008). "Vulnerability Note VU#836068 MD vulnerable to collision attacks". Vulnerability notes database. CERT Carnegi Mellon University Software Engineering Institute. Retrieved 3 February 2017.*
44. *Whittaker, Zack. "Font sharing site DaFont has been hacked, exposin thousands of accounts". ZDNet. Retrieved 18 May 2017.*
45. Schneier, Bruce (February 18, 2005). "Schneier on Security: Cryptanalysis o SHA-1"
46. *"Schneier on Security: Cryptanalysis of SHA-1". Schneier.com Retrieved 2011-11-08.*
47. https://en.wikipedia.org/wiki/SHA-2 - cite_ref-8 *Cryptology Group at Centrum Wiskund & Informatica (CWI) and the Google Research Security, Privacy and Ant abuse Group. "Shattered: We have broken SHA-1 in practice". SHAttered Retrieved 2017-02-23.*