МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра системного програмного забезпечення та технологій дистанційного навчання

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття освітньо-кваліфікаційного рівня «бакалавр»

(освітньо-кваліфікаційний рівень)

на тему «Побудова криптосистем з використанням регулярної і контекстно-вільних граматик з багатобарвним розфарбуванням»
«Creation of cryptosystems using regular and context-free grammars with multi-colored coloring»

Виконав: студент 5-го курсу заочної форми навчання
спеціальності 123 Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)
Валєк Роберт Антонович
(прізвище, ім'я, по-батькові)

Керівник ст. викл. Орлов С. В.
(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент доц. Петрушина
(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри
№___ від «___»_____ 2019 р.

Завідувач кафедри
_____ _Ю.О. Гунченко_
(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___
протокол № __ від «___» ____ 2019 р.
Оцінка _____/_____/
_____
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК
_____ _О.О. Арсірій_
(підпис) (прізвище, ініціали)

Одеса - 2019

АНОТАЦИЯ

Ця робота фокусується на практичній реалізації повноцінної симетричної системи шифрування на основі формальних граматик, досліджуючи ідею використання скінченних автоматів, еквівалентних регулярним граматикам, як криптографічних ключів.

Повністю функціональна система реалізована на JavaScript (стандарт EcmaScript2019), що включає засоби програмної репрезентації і генерації скінченних автоматів, алгоритми шифрування і дешифрування, а також ряд допоміжних і аналітичних компонентів.

ABSTRACT

This work focuses on practical implementation of a proper symmetrical encryption system based on formal grammars, exploring the idea of using finite state machines, equivalent to regular grammars, as cryptographic keys.

Fully functional system is implemented in JavaScript (EcmaScript2019 standard), including means of programmatic representation and generation of finite state machines, encryption and decryption algorithms, and various analytical and miscellaneous features.

АННОТАЦИЯ

В работе рассматривается построение и практическая реализация полноценной симметричной системы шифрования с использованием формальных грамматик. В качестве ключей шифрования и расшифровки используются конечные автоматы, прямо соответсвующие регулярным грамматикам.

Функционирующая реализация выполнена на интерпретируемом языке JavaScript (стандарт EcmaScript2019), содержащая методы программного представления и генерации конечных автоматов, алгоритмы шифрования и расшифровки с их использованием, а также ряд вспомогательных и аналитических компонентов.

ЗМІСТ

ВСТУП

На сьогоднішний день, ефективне шифрування є принциповою необхідністю для будь-якого виду електронної передачі даних. Саме криптографія є ключовим інструментом захисту переданої інформації в сучасних комп'ютерних мережах.

Сучасні криптосистеми ґрунтуються на математичних алгоритмах і понятті обчислювальної складності в контексті актуальних обчислювальних систем. Таким чином, зростання продуктивності комп'ютерів, а також виникнення нових обчислювальних алгоритмів вимагає постійного вдосконалення методів, використовуваних в шифруванні.

Старіння в використовуваних алгоритмів є постійною проблемою. Наприклад, поширено використовуваний метод шифрування Secure Hash Algorithm 1 (SHA-1), розроблений агенством національної безпеки (NSA) США та який є федеральним стандартом обробки інформації (FIPS) США був випущений у 1995 г., але вже у 2005 г. був оголошений нестійким до масованих спроб злому [1]. На даний момент друга версія алгоритму (SHA-2, що вийшла у 2001 г.) також вважається ненадійною, і переважним є використання найбільш актуального Secure Hash Algorithm 3 (2015 г.) [2]. Примітно, що вибір чергового стандартизованого алгоритму проводиться у вигляді відкритого конкурсу між різноманітними заявленими кандидатами [3].

Метою даної роботи є розробка нової криптосистеми на основі запропонованої теоретичної моделі.

Об’єкт досліду: системи шифрування.

Предмет досліду: застосування регулярних і контекстно-вільних граматик у криптографічних системах.

Визначення завдання: реалізувати повноцінну криптосистему, що використовує регулярні та контекстно-вільні граматики та багатобарвну розмальовку для шифрування й відновлення тексту; виконати аналіз основних характеристик системи.

ВИСНОВОК

Початкове завдання з побудови криптосистеми виконано в повній мірі. Розроблено універсальну платформу для роботи з довільними скінченними автоматами, на базі якої буде реалізовано всі функції, необхідні для шифрування і дешифрування. Для оцінки якості системи розроблено окремий модуль автоматичного тестування та обчислення метрик для всіх ключових функціональностей.

Надійність первісної моделі шифрування було значно вдосконалено як за допомогою адаптування класичних технік, що використовуються в шифруванні, так і рішеннями, унікальними для даної системи. В результаті декількох етапів оптимізації досягнута

продуктивність, що дозволяє застосування даної криптосистеми на призначених для користувача пристроях і в контексті інших програм. Для зручного самостійного використання продукту розроблено канонічний Unix-like інтерфейс, що дозволяє спільне використання з іншими програмами на рівні операційної системи, а також зручний доступ до налаштування загальних параметрів системи.

За криптостійкістю реалізована система можна порівняти з системами, заснованими на факторизації простих чисел (напр. RSA), проте сильно програє розповсюдженим системам в швидкості розшифрування.

Вся логіка роботи криптосистеми була реалізована на найбільш сучасній версії широко розповсюдженої мови JavaScript без використання сторонніх бібліотек.

Встановлене завдання виконано повною мірою.

ЛІТЕРАТУРА

1) "Announcing Approval of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard". 2015-08-05.

2) NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition. NIST (October 2, 2012)

3) Buchmann, Johannes A. Introduction to Cryptography (2nd ed.).

4) Schneier, Bruce (February 18, 2005). "Schneier on Security: Cryptanalysis of SHA-1”

5) Chomsky, Noam (Sep 1956). "Three models for the description of language”

6) Meduna, Alexander (2014), Formal Languages and Computation: Models and Their Applications, CRC Press, p. 233

7) Belzer, Jack; Holzman, Albert George; Kent, Allen (1975). Encyclopedia of Computer Science and Technology

8) С. В. Кондакова, С. В. Орлов. Науковий часопис НПУ імені М.П.Драгоманова. Серія 1. Фізико-математичні науки — 2012, №13 (2). С. 77-83

9) Michael Sipser (1997). Introduction to the Theory of Computation 1st. Cengage Learning. The Church-Turing Thesis (Page 130)

10) Andrasiu, M., Atanasiu, A., Pàun, G. and Salomaa, A.: A new cryptosystem based on formal language theory. Bull. Math. de la Soc. Sci. Math. de Roumanie, Tome 36, (1992).