МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КОСТЕВИЧ ІВАН МИХАЙЛОВИЧ

УДК 658.012.011.56:681.3.06

ПРОГРАМНА СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ МЕРЕЖЕВИХ ДАНИХ НА ОСНОВІ ВИКОРИСТАННЯ АСИМЕТРИЧНИХ АЛГОРИТМІВ

121 «Інженерія програмного забезпечення»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль 2018

Роботу виконано на кафедрі програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент,
доцент кафедри програмної інженерії
Кінах Ярослав Ігорович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Рецензент: кандидат фізико-математичних наук,
професор кафедри інформатики і
математичного моделювання,
Михайлишин Михайло Стахович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Захист відбудеться 19 лютого 2018 р. о $9^{.30}$ годині на засіданні екзаменаційної комісії №31 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, аудиторія 101.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Бурхливий розвиток комп'ютеризації всіх сфер життя надає нові можливості для національних економік. Поширення програмних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінок. Крім того що комп'ютерні злочини наносять значні економічні збитки, суспільство стає все залежнішим від роботи програмних систем у різноманітних сферах життя аж до національної безпеки. Будь-який збій у функціонуванні таких систем може привести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних мереж, а також можливість під'єднання до них через звичайні телефонні лінії зв'язку посилюють можливості їх використання для несанкціонованого доступу.

Об'єкт, методи та джерела дослідження. Об'єктом дослідження є асиметричні системи шифрування інформації RSA та Ель-Гамала, як складова частина програмних систем, що забезпечують захист інформації в комп'ютерних мережах.

Предмет дослідження - програми та алгоритми, що дозволяють оцінити рівень надійності асиметричних систем шифрування інформації RSA та Ель-Гамала, з врахуванням розвитку криптоаналітичної науки.

У даній дослідницькій роботі застосовуються методи з таких областей знань: для дослідження та аналізу криптографічних перетворень алгоритмів RSA та Ель-Гамала - теорія чисел та алгебра Евкліда; при досліджені методів криптоаналізу та організації паралельних обчислень - лінійна алгебра, теорія складності та теорія Галуа.

Наукова новизна отриманих результатів:

- дістала подальший розвиток методологія оцінки криптографічної стійкості асиметричних систем шифрування RSA та Ель-Гамала на основі використання методу ЗРЧП;
- розроблено нове програмне забезпечення, яке дозволяє виконувати матричні операції методу ЗРЧП паралельно на N комп'ютерах;
- запропоновано та досліджено організацію високопродуктивної обчислювальної структури, орієнтовану на сучасну інтегральну технологію для суперрідких матриць, які представлені системами алгебраїчних рівнянь або конгруенцій великої розмірності;
- застосовано блокові методи розпаралелювання матричних операцій методу ЗРЧП, які дозволяють швидше, в порівнянні з існуючими алгоритмами, проводити криптоаналіз систем шифрування інформації RSA та Ель-Гамала;
- розроблена та запропонована нова програмна обчислювальна структура, що дозволяє визначати рівень стіцкості систем шифрування RSA та Ель-Гамала.

Практичне значення отриманих результатів.

За результатами проведених досліджень впроваджено методологію розрахунку стійкості асиметричних криптосистем, що дозволяє розв'язувати задачу знаходження закритого ключа за відкритим, а також оцінювати якість ключового

матеріалу асиметричних систем шифрування RSA та Ель-Гамала. Запропоноване програмне забезпечення зменшує час виконання алгоритму ЗРЧП.

Забезпечення навчального процесу методикою аналізу криптографічних властивостей систем шифрування RSA та Ель-Гамала за спеціальністю “Інженерія програмного забезпечення”.

Обґрунтування вимог до паралельної реалізації алгоритму ЗРЧП, що використовується для криптоаналізу систем шифрування RSA та Ель-Гамала.

Апробація. Окремі результати роботи доповідались на XX науковій конференції ТНТУ ім. І. Пулюя, 17-18 травня 2017 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 5-ти частин, висновків, переліку використаних посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 97 аркушів формату А4, 4 додатки, графічна частина – 12 слайдів графічної частини.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено огляд сучасних досягнень науки і техніки в розробці методик захисту даних на основі асиметричних алгоритмів, описано загальну специфіку тематики та завдання розробки.

В розділі «Розробка програмної системи» описано предметну область та специфіку галузі захисту програм та даних. Досліджено методики криптування даних. Проаналізовано специфіку галузі криптографічного захисту інформації, існуючі розробки та прикладне програмне забезпечення. Спроектовано методологію програмної системи, реалізовано і протестовано бібліотеку з набором методів та алгоритмів обробки вхідних даних. Розроблено програмну систему з метою оцінки криптографічної стійкості асиметричних алгоритмів захисту інформіції.

В розділі «Спеціальна частина» описано тематику досліджень, методи та математичні моделі обробки криптографічних даних з метою визначення рівня криптографічної стійкості асиметричних алгоритмів. Розроблено методологію комплексного підходу отримання кількісних характеристик захисту програм та даних асиметричними алгоритмами. Удосконалено методи розпаралелення криптоаналітичних алгоритмів та способи оптимізації програмного забезпечення, їх ефективність.

В розділі «Обґрунтування економічної ефективності» розглянуто питання організації виробництва програм і виконано розрахунки техніко-економічної ефективності проектних рішень з огляду двох підходів програмування – об’єктно-орієнтованого та процедурного. Проаналізовано економічні-господарські чинники, що виникають в процесі розробки, та фактори, які впливають на реалізацію проекту.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» висвітлено питання особливості дотримання стандартних норм та правил Охорони праці в сфері розробки ПЗ із використанням сучасних персональних комп’ютерів. Досліджено позитивний вплив здорового способу життя на професійну діяльність інженерів. Проаналізовано негативний вплив іонізуючого випромінювання техніки та ефективні засоби захисту інженерів від нього.

В розділі «Екологія» досліджено сучасні методології моделювання екологічних задач, вплив програмного моделювання на природоохоронну кон’юктуру. Окреслено значення науково-технічного прогресу в системі забезпечення якісного стану середовища.

У загальних висновках щодо дипломної роботи описано результати дослідницької діяльності в ході реалізації проекту захисту програм та даних на основі використання асиметричних алгоритмів. Резюмовано актуальність отриманих наукових досягнень та розроблюваних методологів захисту програм та даних з допомогою асиметричних алгоритмів. Також, у висновках зазначено основні якісні та кількісні характеристики, які можна отримати, користуючись розробленою технологією захситу інформації в комп’ютерних мережах. Зазначено ефективні програмні рішення для реалізації методології захисту програм та даних із використанням комп’ютерногомережевого обладнання.

В додатках до пояснювальної записки наведено зразки програмного коду паралельної реалізації бібліотеки та системи комп’ютеризованого аналізу

параметрів криптографічних ключів. Проілюстровано роботу розробленої програмної системи із використанням розроблюваної методології. Додано диск з програмним забезпеченням, інструкцією користувача та пояснювальною запискою до розробки.

В графічній частині наведено презентаційний матеріал з поясненням розроблюваного методу захисту програм та даних із використанням криптографічних асиметричних алгоритмів. Проілюстровано результати досліджень та отримані зразки тестування ключового матеріалу для криптографічного захисту інформації та ресурсів комп'ютерних мереж.

ВИСНОВКИ

Розмір ключа в алгоритмі RSA корелює із розміром модуля криптографічного перетворення. Два числа, добутком яких є модуль криптографічного перетворення, повинні мати приблизно однакову довжину оскільки в цьому випадку знайти співмножники складніше, чим у випадку коли довжина чисел значно відрізняються. Якщо передбачається використовувати 2048-бітний модуль, то кожне число повинно мати довжину, приблизно, 1024 біти. Якщо два числа суттєво не відрізняються один від одного, то виникає потенційна загроза безпеки, проте ймовірність такого випадку прямує до нуля.

Оптимальний розмір програмного модуля криптографічного перетворення визначається вимогами безпеки для програм та даних: модуль більшого розміру підвищує рівень інформаційної безпеки, але й сповільнює роботу алгоритму RSA. Довжина криптомодуля обирається, в першу чергу, на основі значимості даних, що захищаються і необхідної стійкості захищених даних і в другу чергу - на основі оцінки можливих загроз. Аналіз захисту програм та даних, що забезпечується довжиною модуля криптографічного перетворення, застосовують при криптоаналізі модуля дискретного логарифму, але те ж можна застосувати і до методу RSA.

Ключ індивідуального користувача має визначений термін існування, що минає через якийсь час, наприклад, через тиждень. Це дає можливість регулярно заміняти ключі і забезпечувати необхідний рівень безпеки. Після закінчення терміну існування ключа, користувач повинен створити новий ключ, попередньо упевнившись, що параметри криптосистеми залишилися старими, зокрема що система використовує ключі тієї ж довжини. Звичайно, заміна ключа не захищає від нападу на повідомлення, зашифровані старим ключем, але для цього розмір ключа повинен підбиратися відповідно до очікуваного часу актуальності даних.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Карпінський М.П., Кінах Я.І., Костевич І.М. Криптографічний захист мережевих даних на основі асиметричних алгоритмів / Матеріали XX наукової конференції ТНТУ ім. І. Пулюя, 2017. – 78 с.

АНОТАЦІЯ

Магістерська робота на тему «Програмна система криптографічного захисту мережевих даних на основі використання асиметричних алгоритмів» Костевича Івана Михайловича. – Тернопільський національний технічний університет імені Івана Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра програмної інженерії, група СПмз–61 // Тернопіль, 2018.

С. – 124, рис. – 25, табл. – 4, слайдів. – 12, додат. – 4, бібліогр. – 62.

Метою досліджень є оцінка рівня надійності систем шифрування RSA та Ель-Гамала на основі використання перспективних методів криптоаналізу, розвиток методів та засобів криптоаналізу, що базуються на факторизації та дискретному логарифмуванню чисел багатократної точності.

Методи та програмні засоби, використані при виконанні розробки системи: мова програмування С++ та її бібліотеки, середовище розробки Corba, середовище розробки та моделювання MatCad, методологію об’єктно - орієнтованої розробки програмного забезпечення.

Результатом роботи є подальший розвиток метод оцінки надійності асиметричних систем шифрування RSA та Ель-Гамала на основі використання методу ЗРЧП; програмне забезпечення, яке дозволяє виконувати матричні операції методу ЗРЧП паралельно на N комп'ютерах; запропоновано та досліджено організацію високопродуктивної обчислювальної структури, орієнтовану на сучасну інтегральну технологію для суперрідких матриць. Застосовано блочні методи розпаралелювання матричних операцій методу ЗРЧП, які дозволяють більш ефективно, в порівнянні з існуючими алгоритмами.

Ключові слова: ПРОГРАМНА СИСТЕМА, КРИПТОГРАФІЧНИЙ ЗАХИСТ, ПАРАЛЕЛЬНЕ ПРОГРАМУВАННЯ, ОБЧИСЛВАЛЬНА СТРУКТУРА, АВТОМАТИЗАЦІЯ, РОЗПАРАЛЕЛЕННЯ, АЛГОРИТМИ.

ABSTRACT

Master's work on the theme "Software system of cryptographic protection of network data using the use of asymmetric algorithms" Kostevich Ivan Mikhailovich. - Ivan Puluj Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Software Engineering, SPMS-61 Group // Ternopil, 2018.

Pages. – 124, pictures. – 25, tables. – 4, slides – 12, add. – 4, bibl.ref. – 62.

The purpose of the research is to evaluate the reliability of RSA and El Gamal encryption systems based on the use of promising methods of cryptanalysis, the development of methods and tools for cryptanalysis, based on factorization and discrete logarithm of numbers of multiple accuracy.
Methods and tools used to develop the system: C ++ programming language and its library, Corba development environment, MatCad development and modeling environment, and object - oriented software development methodology.
The result of the work is the further development of the method for assessing the reliability of asymmetric RSA and El Gamal encryption systems based on the use of the GPCR method; software that allows to perform matrix operations of the RTF method in parallel on N computers. The organization of a high-performance computing structure focused on modern integral technology for super-rigid matrices is proposed and investigated. Block methods of parallelizing the matrix operations of the GPCR method are applied, which allow more efficiently, in comparison with existing algorithms.

Keywords: SOFTWARE SYSTEM, CRYPTOGRAPHIC PROTECTION, PARALLEL PROGRAMMING, CALCULATION STRUCTURE, AUTOMATION, DISTRIBUTION, ALGORITHMS.