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

Бойко Микола Ігорович

УДК 004.056.55:621.39(075)

МЕТОДИ ТА ЗАСОБИ СИМЕТРИЧНОГО ШИФРУВАННЯ

123 «Комп'ютерна інженерія»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2018

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри біотехнічних систем
Лещишин Юрій Зіновійович
Тернопільський національний технічний університет імені Івана Пулюя.

Рецензент: кандидат технічних наук, старший викладач кафедри комп'ютерних наук
Назаревич Олег Богданович,
Тернопільський національний технічний університет імені Івана Пулюя.

Захист відбудеться 23 лютого 2018 р. о $10^{.00}$ годині на засіданні екзаменаційної комісії №34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 1-603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Сучасні засоби цифрового зв'язку для портативних пристроїв при теперішньому розвитку технологій базуються на цифрових модемах невеликої потужності із використанням різноманітних методів модуляції. Їх все частіше використовують у різноманітних портативних і побутових пристроях для передачі інформації і сигналів керування. Ця інформація потребує захисту від стороннього втручання. Одним з методів реалізації захисту інформації є використання криптографічних методів. Вибір конкретного методу шифрування (симетричного чи асиметричного) ґрунтується на його перевагах і недоліках стосовно поставленої задачі. Після чого необхідно перевірити – змоделювати як змінились характеристики системи зв'язку та оцінити її завадостійкість.

Зокрема для побудови систем цифрового зв'язку портативних пристроїв використовують мікроконтролери з малим споживанням енергії та невисокою обчислюваною потужністю. Тому для таких задач використовують симетричні алгоритми шифрування які базуються на одному ключі, що використовується для шифрування і дешифрування (або ключ дешифрування обчислюється за ключем шифрування).

Основною перевагою симетричних алгоритмів шифрування, для такої задачі, є невисокі вимоги до обчислюваної потужності та висока пропускна здатність. В цифрових системах зв'язку мікроконтролер, що виконує шифрування, є додатковим пристроєм до цифрового модему, тому немає потреби змінювати його конструкцію.

Моделювання таких систем цифрового зв'язку уможливлює порівняння їх ефективності при застосування різних методів шифрування та без них, а отже спроектувати портативні пристрої з високим рівнем захисту інформації.

Мета і задачі дослідження. Метою дослідження є моделювання та дослідження впливу методів та засобів симетричного шифрування на ефективність систем цифрового зв'язку.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

— проаналізувати відомі методи шифрування та сучасні системи цифрового зв'язку, для вибору напряму дослідження;

— розробити математичну модель цифрової системи зв'язку з шифруванням, що уможливить моделювання систем зв'язку;

— побудувати модель цифрової системи зв'язку, для дослідження їх ефективності при застосуванні методів симетричного шифрування;

— отримати характеристики ефективності цифрових систем зв'язку, для оцінки впливу на них методів симетричного шифрування.

Об'єкт дослідження — процес прийому та передачі сигналів в цифрових системах зв'язку із застосуванням методів симетричного шифрування.

Предмет дослідження — методи симетричного шифрування в цифрових системах зв'язку.

Методи дослідження базуються на положеннях:

— статистичної радіотехніки для побудови моделей систем цифрового зв’язку;

— криптографії для застосування методів симетричного шифрування.

Наукова новизна одержаних результатів.

1. Вперше отримано характеристики ефективності системи цифрового зв’язку з OFDM модуляцією при використання у її складі алгоритму шифрування AES-128, що уможливлює порівняння впливу різних методів шифрування на ефективність цифрових систем зв’язку.
2. Набуло подальшого розвитку застосування моделі каналу зв’язку із затуханням до задачі моделювання цифрової системи зв’язку з OFDM модуляцією.

Практичне значення одержаних результатів полягає в наступному: отримані результати, уможливлюють застосування методів шифрування при передачі інформації цифровими системами зв’язку портативних та IoT пристроїв, що підвищує захищеність їх використання.

Апробація. Окремі результати роботи доповідалися на VI міжнародній науково-технічній конференції молодих учених та студентів "Актуальні задачі сучасних технологій" Тернопільського національного технічного університету імені Івана Пулюя, Тернопіль (2017р.).

Структура роботи. Дипломна робота складається із вступу, семи розділів, висновку, викладених 103 сторінках, списку використаних джерел з 18 назв на 2 сторінках, додатків на 4 сторінках, загальний обсяг роботи становить 109 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми роботи, сформульовано мету і задачі дослідження, визначено об’єкт, предмет і методи дослідження, показано наукову новизну та практичне значення отриманих результатів, розкрито питання апробації результатів дипломної роботи на науково-технічній конференції.

У першому розділі «Аналіз існуючих методів шифрування та цифрових систем звязку» проведено огляд та порівняння існуючих методів апаратного шифрування. Вибрано симетричний алгоритм шифрування, як один з найпоширеніших та такий що має апаратну реалізацію в мікроконтролерах. Проаналізовано сучасні безпровідні методи цифрової передачі даних.

У другому розділі «Модель цифрової системи зв’язку з шифруванням» використано математичну модель однопроменевого каналу зв’язку із затуханням. Описано модель системи зв’язку на основі OFDM сигналів із використанням симетричного методу шифрування.

У третьому розділі «Моделювання методів симетричного шифрування в цифрових системах зв’язку» використано особливості моделювання методів шифрування та систем зв’язку в середовищі Matlab для побудови відповідних моделей. Проведено моделювання цифрової системи зв’язку із застосуванням методу симетричного шифрування AES-128 та отримано характеристикм ефективності такої системи.

У четвертому розділі «Обґрунтування економічної ефективності» на підставі виконаних розрахунків та нормативних даних встановлено, що планова калькуляція вартості проведення досліджень по темі становить 17553,31 грн.

У п'ятому розділі «Охорона праці та безпека в надзвичайних ситуаціях» висвітлено питання охорони праці при роботі з ЕОМ, зокрема приділено увагу вимогам електробезпеки під час експлуатації ЕОМ та вимогам до організації робочого місця оператора ЕОМ. Також розглянуто дії населення під час надзвичайних ситуацій природного характеру.

У шостому розділі «Екологія» проаналізовано вплив на людину електромагнітного випромінювання від ЕОМ, шляхи та методи його зменшення.

У додатках до дипломної роботи наведено текст програми отриманої засобами MATLAB 2009b для комп'ютерного імітаційного моделювання каналу зв'язку з OFDM та 16-QAM, шифрування та дешифрування за допомогою алгоритму AES-128. Також додано опубліковані тези конференцій.

ВИСНОВКИ

В дипломній роботі магістра проведено моделювання та дослідження впливу методів та засобів симетричного шифрування на ефективність систем цифрового зв'язку.

1. Серед наведених алгоритмів шифрування поставленим вимогам відповідає AES з ключем 128 Біт, який має апаратну та програмну реалізацію в багатьох мікроконтролерах фірм Atmel, Mikrochip, Texas Instruments та ін.
2. В багатьох стандартах цифрового зв'язку (Wi-Fi, Wimax, DVB-T2 та ін.) застосовують OFDM модуляцію з використанням одного з типів модуляції BPSK, QPSK, 8-PSK, QAM і ін. Цей стандарт забезпечує високу завадостійкість при високій швидкості передачі даних.
3. Запропонована математична модель каналу зв'язку враховує вплив завад від середовища поширення сигналів та багато променеве поширення радіо хвиль та пов'язані з цим завмирання в каналі зв'язку. Також вона реалізується засобами Matlab.
4. Наведена модель цифрової системи зв'язку на основі OFDM сигналів з використанням квадратурної амплітудної модуляції дозволяє моделювати систему зв'язку засобами Matlab і додавати до неї різні алгоритми шифрування.
5. Результати моделювання цифрової системи зв'язку із застосуванням методу симетричного шифрування AES-128 показують, що бітова помилка для системи зв'язку з OFDM QAM-16 модуляцією не залежить від застосування методів шифрування, але залежить від відношення сигнал/шум.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Лещишин Ю.З. Моделювання методів симетричного шифрування в цифрових системах зв'язку / Ю.З. Лещишин, М.І. Бойко, // Актуальні задачі сучасних технологій Молодих учених та студентів, 16-17 листопада 2017 року – Т.: ТНТУ, 2017 – Том 2. – С. 202.

АНОТАЦІЯ

Бойко Микола Ігорович. Методи та засоби симетричного шифрування. – Рукопис.

Дипломна робота магістра за спеціальністю 123 — “Комп’ютерна інженерія”, Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних систем та мереж, група СІмз-61, Тернопіль, 2018.

Дипломну роботу магістра присвячено дослідженню методів та засобів симетричного шифрування в цифрових системах зв’язку.

На основі аналізу існуючих методів потокового шифрування в цифрових системах зв’язку вибрано метод симетричний шифрування AES-128. Розроблено модель каналу зв’язку із використанням вибраного методу шифрування. За результатами моделювання отримано характеристики ефективності приймання сигналів в цифрових системах зв’язку при застосування методу симетричний шифрування AES-128.

Розроблена модель каналу зв’язку реалізована засобами Matlab.

Ключові слова: симетричне шифрування, цифрові системи зв’язку, AES-128, модель каналу зв’язку.

ANNOTATION

Boyko Nikolai. Methods and means of symmetrical encryption. - Manuscript.

Master's Work, specializing 123 - Computer Engineering, Ivan Pul'uj Ternopil State Technical University, Faculty of Computer Information Systems and Program Engineering, Department of Computer Systems and Networks, a group CImz-61, Ternopil, 2018.

The master's thesis is devoted to the research of methods and means of symmetric encryption in digital communication systems.

Based on the analysis of existing methods of streaming encryption in digital communication systems, the method of symmetric encryption AES-128 is selected. A communication channel model has been developed using the chosen encryption method. According to the results of simulation, the characteristics of the reception of signals in digital communication systems were obtained using the method of symmetric encryption AES-128.

The developed communication channel model is implemented by means of Matlab.

Key words: symmetric encryption, digital communication systems, AES-128, communication channel model.