АНОТАЦІЯ

Тема дипломного проекту: “Програмна система криптоаналізу методом неможливих диференціалів на основі технологій паралельного програмування OpenMP та MPI”.

Мета роботи полягає в розробці послідовних і паралельних алгоритмів аналізу стійкості блокових шифрів методом неможливих диференціалів (МНД) і виявлення особливостей реалізації його основних етапів.

Предмет дослідження. Предметом дослідження є особливості використання диференціального криптоаналізу та методу неможливих диференціалів при оцінювання стійкості АБШ.

Об'єкт дослідження. Об'єктом дослідження є блоковий алгоритм шифрування AES, зокрема, елементи, що входять до раунду алгоритму.

Програма, яка розробляється в даному проекті, призначена для проведення криптоаналізу методом неможливих диференціалів блокового симетричного шифру AES, а саме – над елементами раунду

Пояснювальна записка складається з шести розділів.

Перший розділ є постановочний. Тут дається короткий огляд сучасних методів криптоаналізу, проводиться теоретичний аналіз предметної області, формулюються цілі та завдання роботи над дипломною роботою магістра, а також основні шляхи їх вирішення. Крім того, у першому розділі розглянуто аналіз БСШ і сферу застосування AES, актуальність криптоаналізу, як такого, методи криптоаналізу, метод повного перебору, парадокс дня народження, паралелізм у задачах криптоаналізу, сформульовані висновки згідно вибору методів, які краще підходять для створення програмної системи.

Другий розділ присвячений алгоритмам, які використані у роботі. До них належить повний огляд алгоритму шифрування AES (Rijndael), включаючи раундове перетворення, алгоритм створення ключів, функцію шифрування,

функцію зворотнього дешифрування, функцію прямого дешифрування. Крім того, в другому розділі описані методи криптоаналізу, а саме, диференціальний криптоаналіз та МНД. Останнім розглядається в розділі застосування MPI для розпаралелювання криптоаналізу. Висновками до другого розділу підсумовується той чи інший вибір алгоритму, і наведені основні характеристики методів, чи алгоритмів.

Третій розділ передбачає написання програмного забезпечення. Тут описані основні елементи AES, та проведення криптоаналізу МНД над ними. Також розглянута паралелізація вихідного коду за допомогою MPI, та тестування написаного програмного забезпечення.

Четвертий розділ - економічний. Головною метою розділу є встановлення економічної доцільності проведення даної розробки.

Пятий розділ – розділ охорони праці та техніки безпеки. В ньому розглянуто забезпечення безпеки, при роботі з ЕОМ, та безпеку при надзвичайних ситуаціях.

Шостий розділ – розділ екології.

Рік виконання – 2013.

Рік захисту – 2013.

Ключові слова: метод неможливих диференціалів, криптоаналіз, AES.

Дипломна робота містить 143 сторінки, 14 таблиць,23 рисунки, список літератури містить 22 найменування.