АНОТАЦІЯ

Алгебраїчний криптоаналіз спрощеного алгоритму AES // Дипломна робота // Крутих Максим Валерійович // Тернопільський національний технічний університет імені Івана Пулюя, Факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних систем та мереж, група СІм-61 // Тернопіль, 2014// с. – 186, рис. – 27, табл. – 8, додат. – 4, кресл. – 7, бібліогр.– 25 .

Ключові слова: AES, S-AES, біт, блок, байт, шифротекст, шифрування, розшифрування, криптоаналіз, алгебраїчний криптоаналіз, S-блок, rijndael, ключ шифрування, лінеаризація, XL-алгоритм, NP-повна задача, поле Галуа.

Робота присвячена дослідженню алгоритму AES з метою проведення його алгебраїчного криптоаналізу.

Алгоритм AES є стійким до всіх атак, в основі яких лежать класичні методи криптоаналізу. Але в 2002 р. Ніколас Куртуа і Йозеф Піпджик висловили припущення про можливості алгебраїчної атаки на шифри з подібною до AES структурою. Алгебраїчна атака націлена на аналіз уразливості в математичних частинах алгоритму і використання його внутрішніх алгебраїчних структур.

Питанням алгебраїчного криптоаналізу алгоритму AES займалися Рафаель Чунг-Вей Фан, Шон Сіммонс, Елізабет Кляйман і Воронін Р. І.. Їхні дослідження обмежились проведенням криптоаналтичної атаки на спрощену версію цього алгоритму. . Розглянуто структуру і алгоритм роботи симетричного блокового алгоритму шифрування Rijndael, описаного в стандарті AES і його спрощеної версії (S-AES). Було розроблено програмне забезпечення для шифрування вхідного тексту і дешифрування зашифрованого тексту, а також для побудови системи рівнянь для здійснення алгебраїчного криптоаналізу і зберігає їх у вигляді текстового файлу з покроковою демонстрацією процесу утворення цих систем. Це дозволяє використовувати дану розробку в навчальних цілях і подальшого дослідження можливості оптимізації даного процесу.