РЕФЕРАТ

Актуальність теми. Сьогодні існує велика потреба у забезпеченні шифрування інформації в режимі реального часу, але існуючі стандарти алгоритмів шифрування є дуже повільними для вирішення цієї задачі. Тому постає гостра необхідність у розробці алгоритмів шифрування, які могли це здійснювати на порядок швидше. В даній магістерській дисертації досліджуються способі генерації ключів алгоритмів шифрування на базі лінійних структур.

Об'єктом дослідження алгоритми шифрування на базі лінійних структур.

Предметом дослідження є способи генерації ключів алгоритмів шифрування на базі лінійних структур.

Мета роботи полягає у розробці способів генерації ключів алгоритмів шифрування на базі лінійних структур.

Методи дослідження. В даній роботі проведено аналіз існуючих алгоритмів шифрування, проаналізовано ключі алгоритму шифрування на базі лінійних структур, їх вразливості та недоліки, розроблені способи генерації ключів.

Наукова новизна роботи полягає у подальшому розвитку алгоритмів шифрування на базі лінійних структур та способів генерації секретних даних алгоритмів (ключів).

Практична цінність отриманих в роботі результатів полягає в тому, що розроблені алгоритми шифрування на базі лінійних структур є швидшими за існуючі стандарти і можуть використовуватися у тих випадках, де необхідно забезпечити шифрування в режимі реального часу.

Апробація роботи. Результати роботи пройшли апробацію на наукових конференціях:

– XI конференція молодих вчених «Прикладна математика та комп’ютинг» ПМК-2018-2;

– XX міжнародна науково-технічна конференція SAIT 2018.

Структура та обсяг роботи. *Магістерська дисертація складається з вступу, трьох розділів, висновків та додатків.*

У вступі охарактеризовано стан проблеми, обґрунтовано актуальність напрямку досліджень, визначено завдання дослідження, описано виконану роботу.

У першому розділі виконано аналіз сучасних стандартів шифрування та виконано порівняння швидкості стандартів з алгоритмом на базі лінійних структур.

У другому розділі розроблено можливі апаратні, на базі ПЛІС, та програмні реалізації алгоритму на базі лінійних структур.

У третьому розділі сформульовано три можливих варіанти секретних ключів, проведено теоретичний аналіз криптоатак на ключі та розроблено модифікації до алгоритмів генерації ключів.

У висновках підведено підсумок зроблених досліджень.

У додатках наведено фрагменти програмного коду, що реалізує алгоритми генерації ключів, копії публікацій, довідки про впровадження та копії графічних матеріалів.

Робота виконана на 77 аркушах, містить 4 додатки та посилання на список використаних літературних джерел з 32 найменувань. У роботі наведено 26 рисунків та 6 таблиць.

Ключові слова: алгоритми шифрування, способи генерації ключів алгоритмів шифрування, алгоритми шифрування на базі лінійних структур, ключі алгоритмів шифрування.