АНОТАЦІЯ

Дана дипломна робота присвячена створенню пакету прикладних програм для шифрування інформації з використанням схеми Ель-Гамаля.

В рамках даного дипломного проекту проведено аналіз алгоритму шифрування та формування цифрового підпису схеми Ель-Гамаля, і виділено операції в скінченних полях які потрібні для їх реалізації.

На етапі формування ключів необхідно виконувати пошук примітивного елемента поля Галуа, для цього реалізовано три алгоритми для пошуку первісного кореня. Для виконання операції піднесення до степеня реалізовано алгоритми двійкового потенціювання зправа наліво, зліва направо, а також віконний метод. При дешифруванні повідомлень виникає необхідність виконувати операцію ділення, яка реалізується через пошук мультиплікативно-оберненого елемента за розширеним алгоритмом Евкліда. При реалізації схеми Ель-Гамаля виникає необхідність генерувати великі прості числа, тому додатково були реалізовані алгоритми пошуку простого цілого числа, а саме: простого перебору, Ферма, Міллера та Міллера-Рабіна.

Так як криптостійкість системи Ель-Гамаля базується на обчислювальній складності задачі дискретного логарифмування, то також було реалізовано алгоритми обчислення логарифму в скінченних полях, а саме: простого перебору, узгодження та Шенкса. Проведено додатково аналіз роботи цих алгоритмів, для визначення шляхів покращення криптостійкості схеми Ель-Гамаля.

Дане програмне забезпечення призначено для навчальних цілей. Це дозволяє реалізацію криптосистеми Ель-Гамаля, а також розглянути і проаналізувати роботу алгоритмів в скінченних полях, які використовуються для даної криптосистеми.

Пояснювальну записку виконано на 118 аркушах, вона містить 2 додатки та посилання на список використаних літературних джерел із 10 найменувань. У роботі наведено 1 таблиця та 19 рисунків.

Ключові слова: шифрування, дешифрування, криптостійкість, поле Галуа, схема Ель-Гамаля, дискретне лоарифмування