ABSTRACT

The thesis is presented in 64 pages. It contains 2 appendixes and bibliography of 13 references. 29 figures and 2 tables are given in the thesis.

The goal of the thesis is to develop mathematical and software tools for creating cryptographic system for encrypting messages in order to send messages safely in the Internet.

Symmetric encryption methods like Substitution cipher, Vernamn ciper, One time pad method, IDEA, RC4, DES, Triple DES, AES; asymmetric encryption methods like Diffi-Hellman, RSA, El Gamal, DSA, elliptic curves algorithms; gibrid encryption methods, like Pretty Good Privacy are discussed.

Different network systems for sending messages like WhatsApp, Telegram, Viber, Apple iMessage, Microsoft Skype, Google Hangouts, Threema, Silent Text were discussed.

According to the formulated criteria, AES (as a symmetric encryption method) and RSA (as asymmetric encryption method) are chosen for solving the task.

Cryptographic system for encrypting and sending messages has been developed.

Keywords: encryption, RSA, AES, safety in the web, message system, chat, communication.