АНОТАЦІЯ

Дипломну роботу виконано на 64 аркушах, вона містить 2 додатки та перелік посилань на використані джерела з 13 найменувань. У роботі наведено 29 рисунків та 2 таблиці.

Метою даної дипломної роботи є створення математичного та програмного забезпечення, що представляє собою криптографічну ситему шифрування повідомлення при його надсиланні в Інтернеті.

Розглянуто методи симетричного шифрування, такі як підстановочні шифри, шифр Вернама, шифри одноразового блокноту, IDEA, RC4, DES, Triple DES, AES, асиметричного шифрування, такі як алгоритми обміну ключами Діффі-Хелмана, алгоритм RSA, алгоритм Ель-Гамаля, алгоритм цифрового підпису DSA, шифрування з допомогою еліптичних кривих, а також описано гібрині методи шифрування та описано метод під назвою Pretty Good Privacy.

Розглянуто такі рішення, як відкриті мережеві системи для надсилання повідомлень: WhatsApp, Telegram, Viber, Apple iMessage, Microsoft Skype, Google Hangouts, Threema, Silent Text.

На основі сформульованих критеріїв для розв’язання поставленої задачі вибрано метод AES для реалізації симетричного шифрування, метод RSA для реалізації асиметричного шифрування.

Розроблено систему, що реалізує обрані методи та виконує надсилання повідомлень між користувачами. Виконано тестування розробленої системи.

Ключові слова: шифрування, RSA, AES, безпека у мережі, система надсилання повідомлення, чат, спілкування.