УДК 681.325

МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ПОВІДОМЛЕНЬ

Савіцький В.А.
Науковий керівник – доц., к.т.н. Огородник К.В.

З розвитком інформаційного суспільства великим державам стали доступні технологічні засоби тотального нагляду за мільйонами людей. Тому криптографія стає одним з основних інструментів, що забезпечують конфіденційність, довіру, авторизацію, електронні платежі, корпоративну безпеку і безліч інших важливих речей, а дослідження, пов'язані з розробкою нових методів та засобів криптографічного захисту, є досить актуальними.

Було розроблено алгоритм криптографічного захисту повідомлень, у основі якого лежить попіксельна перестановка вихідного повідомлення згідно певного введеного ключа. Даний алгоритм було реалізовано програмно. На рис.1 наведено загальний вигляд робочого вікна програми під час кодування.

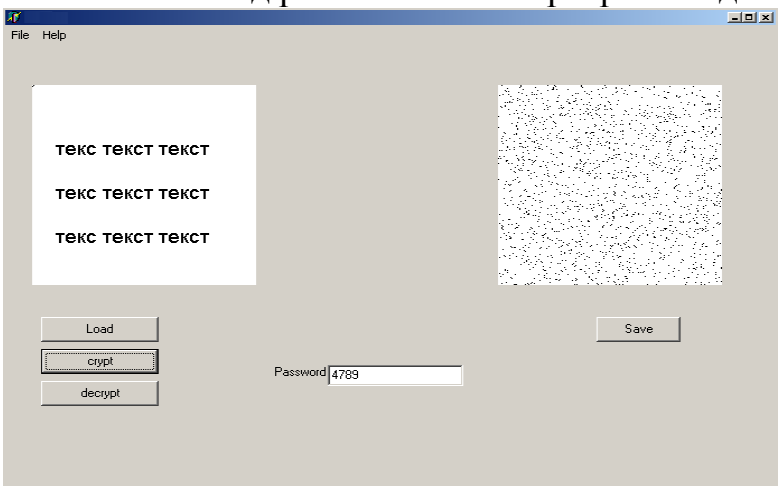

Рисунок 1 – Загальний вигляд робочого вікна програми кодування повідомлень

Програма має зручний інтерфейс який дозволяє бачити початкове та закодоване повідомлення. В робочому вікні розміщене поле для вводу ключа, який може набувати довільного значення розміром до 32 бітів, згідно якого генератор псевдовипадкових чисел генерує послідовність перестановки пікселів. Початкове зображення вноситься в масив для обробки a[i,j]. Пікселі з основного масиву зображення a[i,j] почергово заносяться в масив кінцевого зображення b[x,y] (x,y-випадкові величини), з якого формується закодоване зображення. Розкодування відбувається в зворотному порядку згідно заданого ключа. В випадку вводу вірного ключа ми отримаємо початкове повідомлення, а у випадку коли ключ невірний – шумове зображення.

Таким чином, було розроблено алгоритм та програму криптографічного захисту повідомлень, яка забезпечує високий рівень криптозахисту внаслідок великої кількості можливих попіксельних перестановок. Повторне закодування повідомлення взагалі унеможливлює розкодування прямим підбором ключа.