МЕХАНІЗМ ШИФРУВАННЯ ПОВІДОМЛЕНЬ З МАКСИМАЛЬНОЮ ДОВЖИНОЮ

канд. техн. наук, проф. О.М. Рисований, студ. К.І. Ігнатьєв, студ. Р.В. Рибалка, студ. Д.Р. Рудаковський, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Шифрування інформації є важливим заходом для забезпечення безпеки та конфіденційності в цифровому середовищі. Цей процес полягає в шифруванні даних з метою ускладнення їх зрозуміння. Важливою задачею при шифруванні є дослідження впливу різних ключів на результат.

Основна проблема створення таких програм – це вартість купленого програмного забезпечення та неможливість подальшого внесення змін в доробку при появі нових мікропроцесорів та операційних систем. А якщо програма створена самостійно, то є можливість оперативного внесення відповідних змін й не тільки в функціонал, але й в інтерфейс та його зовнішній вигляд. Існує можливість зміни коду програми. Але така можливість стосується вже реверсного програмування.

У роботі показано, що деякою проблемою при шифруванні повідомлення по модулю є вибір її гами. Розрахунок у програмі ключів займає досить багато часу і це у випадку, якщо максимальний ступінь полінома за модулем два не перевищує 8-10. Але деяким обмеженням вибору максимального ступеня вважатимуться місткість байта. А це 8 біт. Отже, щоб програма шифрування була ефективною і за часом, і швидкістю обробки ключ шифрування повинен дорівнювати байту. Але в цьому випадку довжина послідовності дорівнює 256 символів. Існує кілька різних варіантів виправити це обмеження. Найпростіший – це інкремент попереднього ключа. Переваги цього підходу очевидні, як і недолік – простота злому. Звичайно, можна застосувати псевдовипадкову послідовність, але для 8-го ступеня це – мала довжина.

Проведено дослідження та показано, що програми шифрувальники-здирники, які для європейських користувачів стали дуже актуальними, шифрують невеликі файли, наприклад 862 байт, повністю. Але великі файли, наприклад, 1.8Mb, кодують не до кінця. З цього випливає, що кодування здійснюється циклічно і не більше ніж 1024 символів. Але в цьому випадку кодується, крім початкових 5 байтів, весь PE-заголовок. Висновок напрошується сам собою – за допомогою реверсу поміняти заголовок на інший і очистити дописані вірусом наприкінці файлу блоки однакового розміру 334 = 14Eh байтів.