MHED 2 – модифікований метод шифрування даних для їх захисту під час передачі по мережі Інтернет

Товкач І.О., *студент*; Піддубний В.О., *доцент*
Київський політехнічний інститут, м. Київ

Інтернет на сьогоднішній день є найбільш доступним каналом зв'язку для широкого загалу, проте через свою незахищеність, при пересиланні конфіденційних даних потребує застосування різних способів для їх захисту.

Одним з таких способів, який спроможний вирішити проблему ефективного захисту, є використання методу гібридного шифрування – MHED (Multilayer Hibrid Encryption and Decryption), в якому здійснюється комплексна обробка даних за допомогою симетричних алгоритмів AES, Serpent, Twofish (кожен з яких накладається послідовно, шар за шаром), та асиметричного алгоритму RSA [1].

В результаті здійсненого аналізу функціонування кожної комбінації задіяних алгоритмів у даному методі, було з'ясовано, що від послідовності розташування їх в шарі залежить в цілому швидкість роботи MHED. Також встановлено, що послідовність розташування симетричних алгоритмів має бути різною – в залежності від типу даних: текст, графіка (фото), аудіо, відео.

На основі проведених досліджень виконана оптимізація взаємодії алгоритмів шифрування: дані, які мають бути зашифрованими, спочатку надходять до програмного модулю, де відбувається їхня селекція за типом файлу, після цього вони пересилаються на обробку тими симетричними алгоритмами, послідовність розташування котрих є найбільш оптимальною для конкретних типів файлів (текстових, графічних, аудіо та відео). Для кожної такої послідовності (шару), генерується новий випадковий пароль, який зашифровується асиметричним алгоритмом та записується у початок зашифрованих даних.

MHED-2 впроваджено в електронній мережі архівів Київщини.

1. О.М. Ляшук, *Вісник національного технічного університету України «КПІ». Серія Радіотехніка, радіоапаратобудування.* **56,** 144 (2014).