МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

ІМА :: 2013

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 22-27 квітня 2013 року)

Суми
Сумський державний університет
2013

Захист даних під час передачі їх по відкритих каналах зв'язку за допомогою методу шифрування MHED

Ляшук О.М., *студ.*
Національний технічний університет України «КПІ», м. Київ

Проблема передачі конфіденційних даних по незахищених каналах зв'язку є важливим питанням сьогодення. Для убезпечення інформації, вона передається з використанням симетричних і асиметричних криптографічних алгоритмів.

Найчастіше конфіденційні дані передаються з використанням гібридного алгоритму, де асиметричний алгоритм використовується для шифрування ключа, а симетричний для шифрування даних. Симетричні алгоритми є досить надійними, проте є випадки компроментації, як це трапилося в 1993 році, коли був зламаний DES – стандарт Національної безпеки США.

З метою вирішення зазначеної проблеми розроблено методологію захисту даних на основі багатошарового гібридного шифрування і дешифрування даних - MHED (багатошарове гібридне шифрування і дешифрування).

Особливістю запропонованого методу є те, що асиметричний алгоритм використовується разом з симетричними алгоритмами, кожен з яких застосовується послідовно, шар за шаром. Тому, якщо буде скомпроментовано один з симетричних алгоритмів, дані будуть захищені іншим.

У розробленому методі в якості симетричних алгоритмів використовуються AES, Serpent і Twofish, та асиметричний алгоритм RSA. При дешифрації даних, ключ зчитується з початку зашифрованих даних, розшифровується секретним ключом і використовується для дешифрування даних шар за шаром.

Використання MHED значно підвищує надійність передачі даних по незахищеним каналам. Застосування гібридного шифрування вирішує проблему з передачею ключів іншій стороні та забезпечує прийнятну швидкодію роботи комплексу з чотирьох алгоритмів. У запропонованому методі дані залишаються захищеними навіть при компроментації одного з використаних алгоритмів.

1. Б. Шнайєр, *Практическая криптография* (Москва: Вільямс: 2005).