ОПТИМІЗАЦІЯ ВЗАЄМОДІЇ АЛГОРИТМІВ ШИФРУВАННЯ В MHED-МЕТОДІ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ПРИ ПЕРЕДАЧІ ЇХ ПО ВІДКРИТИХ КАНАЛАХ ЗВ'ЯЗКУ

Товкач І. О., магістрант; Піддубний В. О., к.т.н., доц.
Національний технічний університет України
«Київський політехнічний інститут», Київ, Україна

Поширення глобальної інформатизації, зокрема в діловодну сферу та стрімке впровадження електронного врядування — на сьогодні є одним з важливих чинників розвитку сучасного суспільства, де визначальним є його трансформація в інформаційне суспільство. Одна з провідних функцій такого суспільства — це забезпечення зв'язку між державними органами влади, приватним сектором та громадянським суспільством [1].

Найбільш доступним комунікаційним засобом між суб'єктами зв'язку на сьогодні є мережа Інтернет, за допомогою якої відбувається обмін даними. Проте, дана мережа є незахищеним каналом зв'язку.

Тому стабільно актуальною залишається проблема захисту конфіденційних даних, до числа яких відноситься банківська інформація, персональні дані громадян, комерційна та службова інформація та інші різновиди закритої інформації. Щоб убезпечити таку інформацію від несанкціонованого доступу використовують програмні методи захисту, до числа яких належить криптографія.

Криптографічний захист базується на використанні математичних методів перетворення інформації за допомогою спеціальних алгоритмів. Вони поділяються на симетричні, які використовують один ключ для шифрування та дешифрування, та асиметричні, які мають пару споріднених ключів – відкритий та секретний [2].

Останнім часом все частіше використовуються методи гібридного шифрування, які поєднують переваги вище вказаних методів шифрування.

Об'єктом нашого дослідження є метод 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* [3].

Авторами проводилося порівняння витрат часу на шифрування та дешифрування різних типів файлів (текстових, графічних, аудіо та відео) при різних комбінаціях симетричних алгоритмів, при чому розглядалися такі комбінації симетричних файлів, як *Serpent–Twofish–AES, Twofish–Serpent – AES, AES–Twofish–Serpent*.

В результаті аналізу функціонування кожної комбінації задіяних алгоритмів метода, було встановлено, що від послідовності їх розташування в шарі залежить в цілому швидкість роботи методу *MHED*.

Крім того було встановлено, що послідовність розташування симетричних алгоритмів має бути різною — в залежності від типу даних: текст, графіка (фото), аудіо, відео.

На основі проведених досліджень витрат часу здійснена оптимізація взаємодії алгоритмів шифрування, що відображено на структурній схемі (рис. 1).

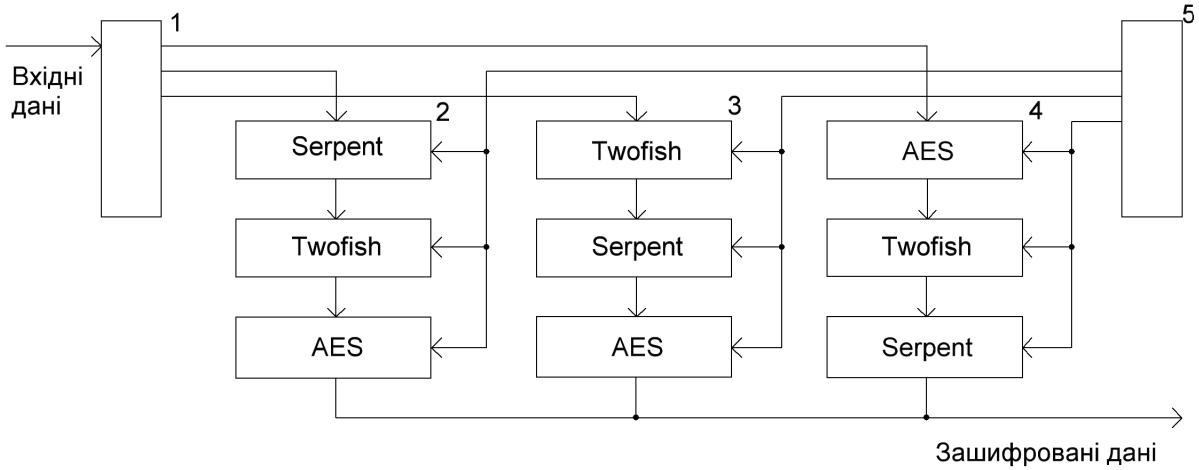

Рисунок 1. Структурна схема взаємодії алгоритмів шифрування в модифікованому методі гібридного шифрування MHED: 1 — програмний модуль, 2, 3, 4 — модулі обробки симетричними алгоритмами, 5 — модуль обробки несиметричним алгоритмом

Вхідні дані, які мають бути зашифрованими, спочатку надходять до програмного модулю 1, 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: 2 — текстових (*Serpent–Twofish–AES*), 3 — графічних (*Twofish–Serpent–AES*), 4 — аудіо та відео (*AES–Twofish–Serpent*). Для кожної такої послідовності (шару), генерується новий випадковий пароль, який зашифровується асиметричним алгоритмом 5 та записується у початок зашифрованих даних.

При дешифрації даних ключ зчитується з початку зашифрованих даних, розшифровується секретним ключем та використовується для дешифрування даних шар за шаром [3].

Завдяки модифікації методу *MHED* авторам вдалося зменшити витрати часу на шифрування та дешифрування: текстової інформації — на 21%, графічної — на 19%, аудіо — на 12%, відео — на 9%. Порівняння проводились при обробленні модифікованим та звичайним методом *MHED* одних і тих файлів різного типу.

Таким чином, здійснена модифікація методу гібридного шифрування *MHED* шляхом оптимізації взаємодії застосованих алгоритмів шифрування, дозволила створити новий програмний продукт — *PolsdarCriptor*, який вже впроваджено в архівній галузі. Він інтегрований в службові сторінки офіційних сайтів архівних установ Київської області, де за його допомогою

конфіденційні дані можуть оброблятись для пересилання між установами, які входять до «Електронної мережі архівів Київщини» [4].

Література

1. Вишневський А., Електронне урядування: досвід упровадження в Головдержслужбі України. /А. Вишневський, В. Дунаєв// Вісник державної служби України. — 2008. — №4.

2. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко — К. : ООО «Полиграф-Консалтинг», 2005. — 215 с.

3. Ляшук О. М. MHED – високоефективний метод захисту даних на основі багатошарового гібридного шифрування /О. М. Ляшук// Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали та системи». Київ, 11 — 15 березня 2013 р.: матеріали конференції — Київ, 2013. — С. 220—221.

4. Веб-сайт Електронної мережі архівів Київщини [Електронний ресурс]. — Режим доступу: http://archives.kiev.ua — Назва з екрану (6.02.2014).

Анотація

Запропоновано більш ефективну взаємодію симетричних алгоритмів шифрування *AES, Serpent, Twofish* та асиметричного алгоритму *RSA* в *MHED*–методі захисту конфіденційних даних при передачі їх по відкритих каналах зв'язку, що дозволило зменшити затрати часу на обробку даних.

Ключові слова: Захист конфіденційних даних, алгоритми, відкриті канали зв'язку, *MHED*-метод шифрування.

Аннотация

Предложено более эффективное взаимодействие симметричных алгоритмов шифрования *AES, Serpent, Twofish* и асимметричного алгоритма *RSA* в *MHED*–методе зщты конфиденцийних данных при передаче их по открытым каналам связи, что позволило уменьшить затраты времени на обработку данных.

Ключевые слова: Защита конфиденциальных данных, алгоритмы, открытые каналы связи, *MHED*-метод шифрования.

Abstract

A more effective interaction symmetric encryption algorithms AES, Serpent, Twofish algorithm and asymmetric RSA in MHED–protection methods confit-dentsiynyh data when transferring them to open channels of communication, thus reducing the cost of time for processing.

Keywords: Protecting sensitive data, algorithms, open communication channels, MHED-encryption method.