УДК 681.3.07

MHED — ВИСОКОЕФЕКТИВНИЙ МЕТОД ЗАХИСТУ ДАНИХ НА ОСНОВІ БАГАТОШАРОВОГО ГІБРИДНОГО ШИФРУВАННЯ

Ляшук О. М. , магістрант
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

MHED — HIGHLY EFFICIENT METHOD OF DATA PROTECTION BASED ON MULTILAYER HYBRID ENCRYPTION

Oleksii Liashuk, Undergraduate Student
National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine

Вступ

У сучасному світі, де постійно вдосконалюються технології та зростає об'єм інформації, важливою проблемою постає захист даних. Особливо актуальним питанням є проблема передачі конфіденційних даних незахищеними каналами зв'язку, наприклад, через мережу Інтернет. Тому, щоб убезпечити інформацію, її передають, використовуючи криптографію — науку про методи забезпечення конфіденційності і автентичності інформації.

Сучасні криптографічні алгоритми шифрування даних поділяються на симетричні (з одним ключем для шифрування і дешифрування) та асиметричні (з відкритим ключем). Асиметричні алгоритми використовують відкритий (public) та секретний (private) ключі для шифрування і дешифрування відповідно.

Симетричні алгоритми є досить поширеними і зазвичай використовуються для шифрування великих об'ємів даних, таких як неперервні інформаційні потоки або файли. Сучасні симетричні алгоритми є криптостійкими та швидкодійними [1]. Найбільш відомими та захищеними алгоритмами вважаються AES, Serpent та Twofish.

Мета статті

Розробка методу багатошарового шифрування та дешифрування даних, який дає можливість значно підвищити надійність передачі даних незахищеними каналами.

Симетричні алгоритми

Алгоритм AES (Advanced Encryption Standard), відомий як Rijndael - симетричний алгоритм блочного шифрування, який був розроблений Йоаном Дайменом та Вінсентом Рейменом. Довжина блоку складає 128 біт, довжина ключа може бути 128, 192 та 256 біт.

Початкова версія алгоритму підтримувала широкий діапазон розмірів блоків і ключів. Виправлена версія AES має фіксовану довжину блоку 128 біт і розмір ключа може бути 128, 192 та 256 біт. Через постійний розмір блоку AES оперує масивом байтів 4 × 4, що називається станом (версія алгоритму з великим розміром блоку має додаткові стовпці). У 2006 році AES став одним з найпоширеніших алгоритмів симетричного шифрування.

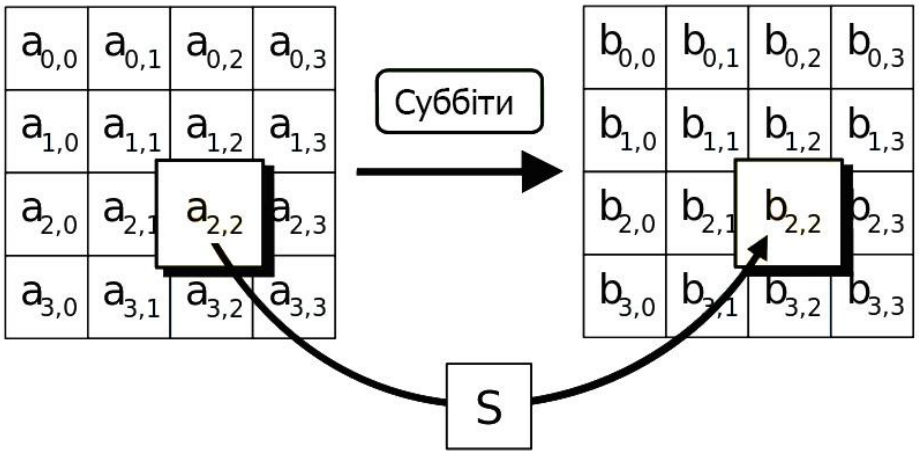

Рис 1. Схема підстановки з використанням S-боксів у алгоритмі AES

Serpent — симетричний алгоритм блочного шифрування, який був розроблений Россом Андерсоном, Ларсом Кнудсеном та Елі Біхамом та став одним з фіналістів другого етапу конкурсу AES. Serpent має довжину блоку 128 біт, а довжина ключа може бути 128, 192 або 256 біт. Алгоритм є 32-раундовим шифром на основі SP-мережі та оперує блоками з чотирьох 32-розрядних слів. Serpent розроблений таким чином, що всі операції можуть виконуватися паралельно, з 32-ма однобітними потоками.

При створенні нового алгоритму автори Serpent дотримуватися консервативних методів проектування, що пояснює використання таблиць підстановки, властивості та характеристики яких вже давно були проаналізовані провідними фахівцями в галузі криптографії [2]. Новий алгоритм аналізувався методами, розробленимими для DES, що також використовує таблиці підстановки. У алгоритмі не використовувалися нові неперевірені технології шифрування. Основною умовою при створенні Serpent було те, що новий алгоритм повинен бути швидше, ніж 3DES і забезпечувати принаймні такий же рівень безпеки: довжина блоку повинна бути 128 біт, а довжина ключа 256 біт. 16-раундовий Serpent має таку саму надійність, як 3DES при двічі більшій швидкості. Тим не менш, автори прийшли до висновку, що для більшої надійності кількість раундів необхідно збільшити до 32. Ставши фіналістом AES, Serpent став другим за результатами голосування.

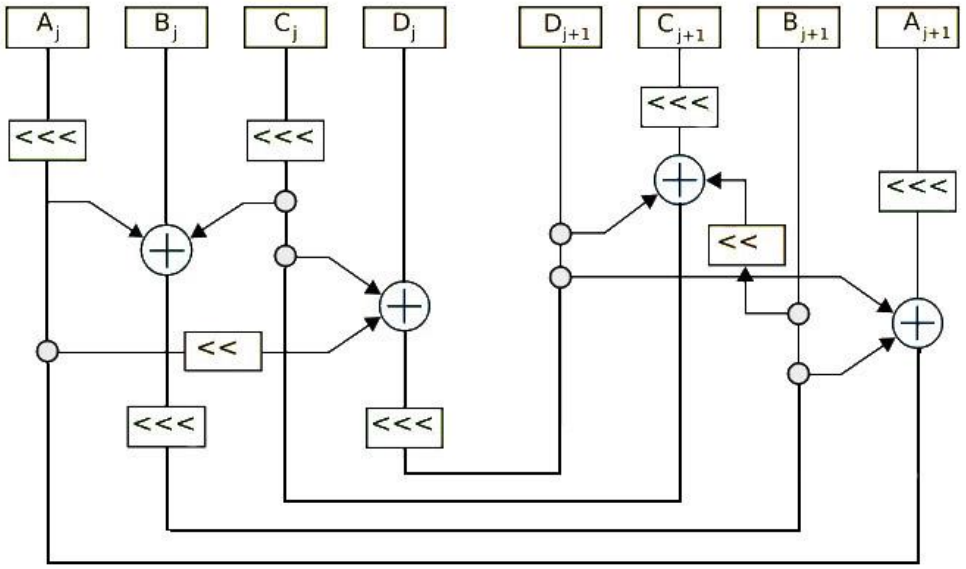

Рис 2. Схема роботи алгоритму Serpent, візуалізація перетворення чотирьох 32-бітних блоків в межах одного раунду.

Twofish — симетричний алгоритм блочного шифрування, розмір блоку якого 128 біт та довжина ключа — до 256 біт; кількість раундів становить 16. Розроблений командою на чолі з Брюсом Шнайером, алгоритм став одним з п'яти фіналістів другого етапу конкурсу AES. Twofish спроектований на основі алгоритму Blowfish.

Відмінною особливістю алгоритму є використання заздалегідь обчислюваних S-боксів, які залежать від ключа, та використання складної схеми розгортки підключення шифрування. Перша половина n-бітового ключа використовується як фактичний ключ шифрування, а друга половина — для модифікації алгоритму, від якого залежать S-бокси [3].

Алгоритм Twofish з'явився в результаті спроб модифікації алгоритму Blowfish для 128-бітного вхідного блоку. Новий алгоритм легко реалізується апаратно та має досконалішу систему розширення ключа.

В результаті алгоритм реалізували у вигляді змішаної мережі Фейстеля з чотирма гілками, котрі змінюють одна одну використовуючи перетворення Адамара. Алгоритм зайняв третє місце по результатам голосування у конкурсі AES.

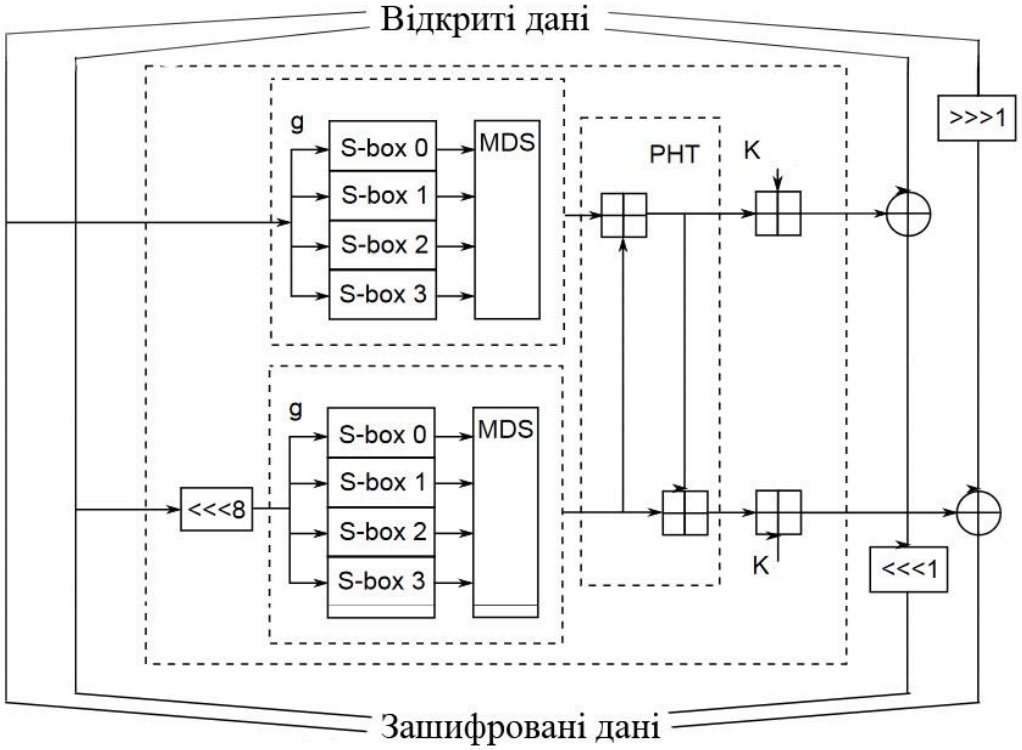

Рис. 3. Схема роботи алгоритму Twofish, ілюструється вплив ключа на формування S-боксів та на перетворення даних.

Асиметричний алгоритм RSA

У перерахованих алгоритмах для обміну зашифрованими даними обидві сторони повинні мати ключ, яким потрібно попередньо обмінятися захищеним каналом. При широкому розповсюдженні мережі Інтернет постає проблема передачі ключа довіреній стороні по незахищеним каналом, бо симетричний ключ може бути перехоплений і третя сторона може розшифрувати повідомлення.

Вказана проблема вирішується за допомогою асиметричного шифрування, де найчастіше використовується алгоритм RSA з довжиною ключа 1024, 2048 або 4096 біта.

Алгоритм RSA побудований за принципом складності факторизації [4]. В основу даного алгоритму покладено використання двох ключів — відкритого і секретного, які будучи разом створеними утворюють пари ключів. Відкритий ключ використовується для шифрування даних і не зберігається в таємниці. Повідомлення, яке було зашифровано відкритим ключем, можливо розшифрувати тільки відповідним секретним ключем.

Послідовність дій при використанні даного алгоритму для шифрування та дешифрування є наступною: сторона X, якій необхідно отримати конфіденційні дані від сторони Y через незахищений канал, надсилає стороні Y публічний (відкритий) ключ, яким сторона Y шифрує дані та надси-

лає їх стороні X, яка дешифрує їх за допомогою приватного (секретного) ключа.

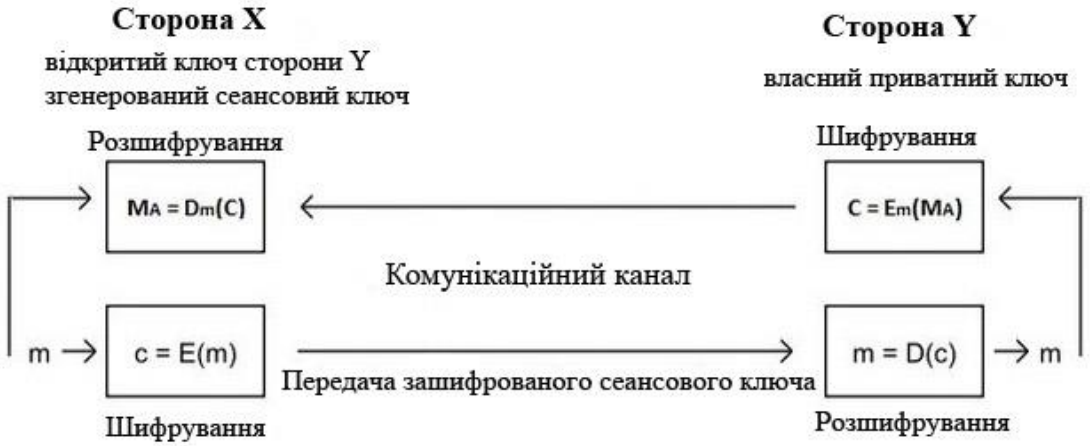

Рис 4. Схема передачі даних незахищеним каналом з використанням RSA.

Гібридний алгоритм шифрування

Асиметричні алгоритми зазвичай мають набагато більшу довжину ключа та використовують математичні операції, які неефективно виконуються на сучасних комп'ютерах, тому працюють дуже повільно.

Для досягнення оптимальної швидкодії використовують гібридний метод шифрування, який поєднує в собі переваги асиметричного та симетричного шифрування. Вказаний метод дозволяє двом сторонам передавати зашифровані дані також без використання захищеного каналу для передачі ключів. Метод використовується у відомій криптографічній системі PGP [5] і його алгоритм зводиться до наступної послідовності дій:

1. Стороною X генерується пара з відкритого та секретного ключа.
2. Відкритий ключ передається незахищеним каналом стороні Y, яка має надсилати конфіденційні дані стороні X.
3. Сторона Y генерує випадковий ключ для симетричного криптографічного алгоритму та зашифровує ним інформацію.
4. За допомогою відкритого ключа на стороні X ініціалізується асиметричний алгоритм, ним шифрується згенерований випадковий симетричний ключ, який додається до зашифрованої інформації.
5. Сторона X отримує кодовану інформацію від сторони Y та ініціалізує асиметричний алгоритм. Симетричний ключ екстрагується з прийнятої інформації та дешифрується секретним ключем.
6. Решта даних розшифровується симетричним алгоритмом за допомогою дешифрованого симетричного ключа стороною X.

Таким чином досягається прийнятна швидкість обробки даних при використанні блочного симетричного алгоритму та вирішується проблема з передачею ключа незахищеними каналами.

Симетричні алгоритми є досить надійними, проте існують випадки їх компроментації, як це трапилось у 1993 році, коли було зламано симетричний алгоритм національної безпеки США DES [1]. Тому неможливо гарантувати, що нові досягнення в галузі криптоаналізу та постійне підвищення обчислювальної потужності комп'ютерів не виявлять вразливість у симетричному алгоритмі, через що захищені дані зможуть бути дешифровані третьою стороною. Для вирішення цієї проблеми постійно удосконалюють алгоритми, збільшують довжину ключа.

Покращення алгоритмів не завжди вирішує проблему, оскільки дані можуть бути перехоплені, а потім — у недалекому майбутньому, коли технічні засоби це дозволять, при необхідності буде проведений злом алгоритму та дешифрування даних.

Опис розробленого методу — MHED

Для вирішення вище зазначених проблем був розроблений метод захисту даних на основі багатошарового гібридного шифрування та дешифрування даних — MHED (Multilayer Hybrid Encryption and Decryption).

Особливість методу полягає в тому, що задіяні всі вищезгадані алгоритми для комплексної обробки даних: разом з асиметричним алгоритмом використовується декілька симетричних алгоритмів, кожен з яких накладається послідовно, шар за шаром. Тому, в разі компроментації одного з симетричних алгоритмів, дані будуть захищені іншим. З точки зору швидкодії оптимально використовувати 3 шари симетричних алгоритмів [6].

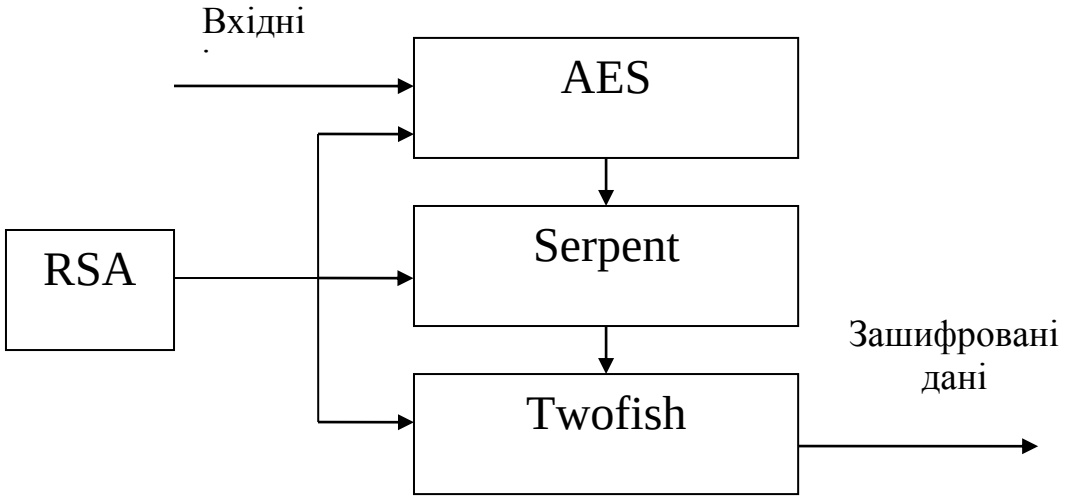

Рис. 5. Процес шифрування даних за допомогою методу MHED

В запропонованому методі, в частині використання симетричних алгоритмів, були обрані AES, Serpent та Twofish, як асиметричний алгоритм використовується RSA. Для кожного шару генерується новий надійний випадковий пароль, який зашифровується RSA. Такий ключ вирівнюється до 512 біт та записується в початок зашифрованих даних. При дешифрації

даних ключ зчитується з початку зашифрованих даних, розшифровується секретним ключем та використовується для дешифрування даних шар за шаром.

Висновки

При використанні методу MHED значно підвищується надійність передавання даних незахищеними каналами, такими як мережа Інтернет. Завдяки використанню гібридного шифрування вирішується проблема з передачею ключів іншій стороні та забезпечується прийнятна швидкодія роботи всього комплексу з чотирьох задіяних алгоритмів. В розробленому методі використання декількох шарів шифрування симетричними алгоритмами забезпечує захист даних навіть при компроментації одного з них.

Література

1. Мао В. Современная криптография: теория и практика / В. Мао. — М. : Видавничий дім «Вільямс». — 2005. — 763 с.

2. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайєр. — М. : Издательский дом "Вильямс", 2005. — 424 с.

3. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е.Б. Маховенко. — М. : НПО «Профессионал». — 2004. — 490 с.

4. Лєвін М. PGP: Кодирование и шифрование информации с открытым ключом / М. Лєвін. — М. : Бук–пресс. — 2006. — 166 с.

5. Використання криптографічних алгоритмів у системі «Truecrypt» [Електроний ресурс]. — Режим доступу: http://www.truecrypt.org/docs/cascades#aes–serpent–twofish.

References

1. Wenbo Mao (2003) *Modern Cryptography: Theory and Practice*. Prentice Hall Professional Technical Reference.

2. Ferguson N. and Schneier B. (2005) Practical Cryptography: Designing and Implementing Secure Cryptographic Systems

3. Rostovcev A. G. and Mahovenko E. B. (2004) *Teoreticheskaja kriptografija* [Theoretical cryptography]. Moskow, NPO «Professional» Publ., 490 p.

4. Levin M. (2006) *PGP: Kodirovanie i shifrovanie informacii s otkrytym kljuchom* [The encoding and encryption of information with a public key]. Moskow, Buk–press Publ., 166 p.

5. Vykorystannia kryptohrafichnykh alhorytmiv u systemi «Truecrypt» [The use of cryptographic algorithms in the system «Truecrypt»]. Available at: http://www.truecrypt.org/docs/cascades#aes–serpent–tshhofish

Ляшук О. М. ***MHED — високоефективний метод захисту даних на основі багатошарового гібридного шифрування.*** *У роботі розглянуті сучасні алгоритми шифрування та проблеми, які виникають при їх використанні; описано метод гібридного шифрування. Запропоновано метод багатошарового гібридного шифрування, який розроблено для безпечного обміну інформацією у мережі Інтернет, з використанням асиметричного та n-кількості симетричних алгоритмів.*

Ключові слова: *криптографія, симетричний алгоритм, гібридне шифрування, AES, RSA.*

Ляшук А. Н. ***MHED — высокоэффективный метод защиты данных на основе многослойного гибридного шифрования****. В работе рассмотрены современные алгоритмы шифрования и проблемы, возникающие при их использовании; описан метод*

гибридного шифрования. Предложен метод многослойного гибридного шифрования, который разработан для безопасного обмена информацией в сети Интернет, с использованием асимметричного и n-количества симметричных алгоритмов.

Ключевые слова: *криптография, симметричный алгоритм, гибридное шифрование, AES, RSA.*

Liashuk O. M. ***Highly efficient method of data protection based on multilayer hybrid encryption.***

Introduction. The paper deals with modern encryption algorithms and problems associated with their use. Hybrid encryption method was developed for secure communication over the Internet.

Principal part. Symmetric algorithms used in method are AES, Serpent and Twofish, asymmetric algorithm is RSA. For each layer new secure random key is generated and encrypted by RSA. This key is aligned and written in the beginning of the encrypted data. On decryption key is read from the beginning of encrypted data and decrypted by RSA secret key. Then symmetric key is used to decrypt data layer by layer.

Conclusions. Use of multilayer hybrid encryption allows to transmit both keys and data by unsecure channel and ensure that data will be protected and at least one symmectric algorithm is not compromised.

Keywords*: cryptography, symmetric algorithm, hybrid encryption, AES, RSA.*