УКРАЇНА

(19) UA (11) 121345 (13) U

(51) МПК
H04L 9/14 (2006.01)
G06F 21/72 (2013.01)
G06F 21/60 (2013.01)

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 09187**

(22) Дата подання заявки: **18.09.2017**

(24) Дата, з якої є чинними права на корисну модель: **27.11.2017**

(46) Публікація відомостей про видачу патенту: **27.11.2017, Бюл.№ 22**

(72) Винахідник(и):
Янковський Ігор Миколайович (UA),
Цапко Денис Петрович (UA)

(73) Власник(и):
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ІННОВЕЙШН ДЕВЕЛОПМЕНТ ХАБ",
пров. Охтирський, 7, корп. 3, м. Київ, 03680 (UA)

(74) Представник:
Матата Юлія Миколаївна

(54) СПОСІБ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ МІЖ МОДУЛЕМ КРИПТОГРАФІЧНИХ ТА ТЕХНОЛОГІЧНИХ ПЕРЕТВОРЕНЬ І МОДУЛЕМ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

(57) Реферат:

Спосіб захищеного обміну даними між модулем криптографічних та технологічних перетворень (МКТП) і модулем криптографічних перетворень (МКП) полягає у тому, що генерують першу пару приватного та публічного ключів у МКТП та генерують другу пару приватного та публічного ключів у МКП, генерування здійснюють відповідно до ДСТУ ETSI EN 119 312:2015. Здійснюють обмін публічними ключами з першої та другої пари приватного та публічного ключів між МКТП та МКП. Генерують перший спільний секретний ключ у МКТП і другий спільний секретний ключ в МКП та здійснюють обмін згенерованими першим і другим секретними ключами між МКТП та МКП. При здійсненні обміну першим і другим спільними секретними ключами їх шифрують та дешифрують за допомогою згенерованих першої та другої пари приватного та публічного ключів, а перший та другий спільні секретні ключі періодично замінюють новими шляхом їх повторного генерування відповідно до попередньо встановленого часового періоду. Генерують пакет даних для захищеного обміну між МКТП та МКП. Генерують випадкове значення за допомогою генератора випадкових чисел; здійснюють шифрування пакета даних за допомогою згенерованого випадкового значення та першого і другого спільних секретних ключів відповідно до стандарту симетричного алгоритму блочного шифрування (AES), передають зашифрований пакет даних каналом зв'язку між МКТП та МКП, після чого здійснюють дешифрування пакета даних. Першу та другу пару приватного та публічного ключів періодично замінюють новими шляхом їх повторного генерування відповідно до попередньо встановленого часового періоду. Генерують третю пару приватного та публічного ключів у МКТП та генерують четверту пару приватного та публічного ключів у МКП, здійснюють генерування відповідно до стандарту ДСТУ ETSI EN 119 312:2015. Здійснюють обмін публічними ключами третьої та четвертої пари ключів між МКТП та МКП. При здійсненні обміну публічними ключами третьої та четвертої пари ключів їх шифрують та дешифрують за допомогою чинних першої та другої пари приватного та публічного ключів, а після здійснення обміну першу та другу пару приватного та публічного ключів визначають нечинними.

UA 121345 U

Корисна модель належить до галузі криптографічного захисту інформації (КЗІ) і може бути використана у складі засобів КЗІ, у тому числі для накладання електронного цифрового підпису (ЕЦП), верифікації накладення підпису за допомогою модуля криптографічних перетворень (МКП), такого як смарт-карта, SIM-карта, що імплементує стандарт криптографічного захисту ДСТУ ETSI EN 119 312:2015.

Криптографічні алгоритми, що використовуються у запропонованому способі захищеного обміну даних, базуються на використанні згенерованих ключових пар приватного та публічного ключів, що захищено зберігаються в пам'яті МКП та спільних секретних ключів.

З рівня техніки відома криптографічна служба у вигляді програмного забезпечення (патент № US 6412069 B1, 25.06.2002), яке розташовується на жорсткому або гнучкому диску та зв'язано зі стандартною операційною системою (ОС) комп'ютера. ОС має простір застосувань та простір ядра. Програмне забезпечення (ПЗ) криптографічних служб виконує криптографічні операції у просторі ядра ОС. Це ПЗ включає в себе програмний інтерфейс рівня застосувань простору ядра та модуль криптографічних служб, що має бібліотеку криптографічних алгоритмів.

Недоліками відомої служби є її низький рівень стійкості до зламу, низька швидкодія, а також те, що бібліотека криптографічних алгоритмів не використовує сучасний стандарт криптографічного захисту ДСТУ ETSI EN 119 312:2015 і є застарілою.

Також з рівня техніки відома система (заявка № US 2005005101 A1, 06.01.05), що має блок перевірки підпису модуля ядра та спосіб його використання. Цей модуль автоматично контролює шлях підпису та отримує інформацію про підпис, яка надається кожним модулем при намаганні завантаження у ядро. Відомості про підпис, що одержують зі шляху модуля ядра, добуваються за допомогою криптографічної інфраструктури ядра для перевірки відомостей про підпис, наданих службою криптографічної інфраструктури ядра, коли той же модуль ядра намагається зареєструвати процедури та механізми у криптографічній інфраструктурі ядра. Застосовується лише в ОС Unix.

Недоліками відомої системи є її висока ресурсоємність, обмежена галузь застосування, оскільки криптографічне ПЗ системи може працювати виключно у просторі застосувань ОС Unix і не може функціонувати у просторі ядра інших систем, а також низький ступінь криптографічної стійкості.

Задачею корисної моделі є створення способу захищеного обміну даними між модулем криптографічних та технологічних перетворень (МКТП) та МКП, який міг би забезпечувати високий ступінь КЗІ, використовуватись як окремо так і в складі інших засобів КЗІ та який би забезпечував реалізацію криптографічного алгоритму відповідно до вимог ДСТУ ETSI EN 119 312:2015.

Технічний результат запропонованого об'єкта корисної моделі полягає у забезпеченні надійного обміну даними по захищеному каналу шифрування між МКП і МКТП, підвищенні криптостійкості, запобіганні перехопленню публічних ключів, що ним передаються шляхом їх шифрування відповідно до алгоритму шифрування RSA, а також у виключенні можливості несанкціонованого дешифрування захищених даних, що передаються захищеним каналом зв'язку.

Ще одним технічним результатом є те, що завдяки запропонованій послідовності дій способу підвищується швидкість передачі даних по каналу шифрування і знижується ресурсоємність, необхідна для шифрування та дешифрування переданих даних.

Ще одним технічним результатом є забезпечення реалізації криптографічного алгоритму відповідно до вимог ДСТУ ETSI EN 119 312:2015 для КЗІ, що передається захищеним каналом шифрування.

Поставлена задача вирішується запропонованим способом захищеного обміну даними між МКТП і МКП, що включає такі дії:

- генерують першу пару приватного та публічного ключів у МКТП та генерують другу пару приватного та публічного ключів у МКП, причому генерування здійснюють відповідно до вимог ДСТУ ETSI EN 119 312:2015,
- здійснюють обмін публічними ключами з першої та другої пари приватного та публічного ключів між МКТП та МКП,
- генерують перший спільний секретний ключ у МКТП і другий спільний секретний ключ в МКП та здійснюють обмін згенерованими першим і другим секретними ключами між МКТП та МКП, причому при здійсненні обміну першим і другим спільними секретними ключами їх шифрують та дешифрують за допомогою згенерованих першої та другої пари приватного та публічного ключів, а перший та другий спільні секретні ключі періодично замінюють новими шляхом їх повторного генерування відповідно до попередньо встановленого часового періоду,

- генерують пакет даних для захищеного обміну між МКТП та МКП,

- генерують випадкове значення за допомогою генератора випадкових чисел,

- здійснюють шифрування пакета даних за допомогою згенерованого випадкового значення та першого і другого спільних секретних ключів відповідно до стандарту симетричного алгоритма блочного шифрування (AES), передають зашифрований пакет даних каналом зв'язку між МКТП та МКП, після чого здійснюють дешифрування пакета даних,

причому першу та другу пару приватного та публічного ключів періодично замінюють новими шляхом їх повторного генерування у відповідності до попередньо встановленого часового періоду, при цьому процес заміни включає етапи на яких:

- генерують третю пару приватного та публічного ключів у МКТП та генерують четверту пару приватного та публічного ключів у МКП, причому генерування здійснюють відповідно до вимог ДСТУ ETSI EN 119 312:2015,

- здійснюють обмін публічними ключами третьої та четвертої пари ключів між МКТП та МКП, причому при здійсненні обміну публічними ключами третьої та четвертої пари ключів їх шифрують та дешифрують за допомогою чинних першої та другої пари приватного та публічного ключів, а після здійснення обміну першу та другу пару приватного та публічного ключів визначають нечинними.

Як МКП використовується смарт-картка (smart-card), що містить інтегральну схему та пам'ять і призначена для ідентифікації, автентифікації, авторизації користувачів, зберігання ключової інформації і проведення криптографічних операцій в довіреному середовищі та інших операцій.

Суть запропонованого способу полягає у створенні захищеного каналу шифрування, яким передають дані між користувачами у зашифрованому вигляді із застосуванням різних алгоритмів. Таким чином, у разі несанкціонованого перехоплення трафіку, що передається захищеним каналом шифрування, його зміст неможливо буде розшифрувати та зрозуміти. Поряд із цим, користувачі повинні мати легкий і швидкий спосіб передачі великих об'ємів даних, а шифрування всього каналу зв'язку є досить ресурсоємним процесом, що значно знижує швидкодію.

Спосіб захищеного обміну даними між МКТП і МКП здійснюють таким чином.

У МКТП для першого користувача генерують першу пару (RSA) приватного PrKey1 та публічного PubKey1 ключів, а у МКП для другого користувача генерують другу пару приватного PrKey2 та публічного PubKey2 ключів. Далі здійснюють обмін публічними ключами PubKey1, PubKey2 між користувачами, PubKey1 надсилають до МКП другому користувачу, а PubKey2 надсилають до МКТП першому користувачу. Після цього у МКТП та у МКП генерують перший спільний секретний ключ SharedSecret1 та другий спільний секретний ключ SharedSecret2, які необхідні для шифрування даних, що передаються захищеним каналом шифрування і здійснюють обмін ними між користувачами. Для того, щоб провести захищений обмін ключами SharedSecret1 і SharedSecret2, їх шифрують за допомогою раніше згенерованих пар приватного та публічного ключів. Спільний секретний ключ SharedSecret1 при передачі шифрують за допомогою пари ключів PrKey1, PubKey2, а розшифровують на стороні приймання за допомогою пари ключів PrKey2, PubKey1. Спільний секретний ключ SharedSecret2 аналогічно шифрують при передачі за допомогою PrKey2, PubKey1, а розшифровують на стороні приймання за допомогою PrKey1, PubKey2.

Проте, постійне використання одних і тих самих спільних секретних ключів протягом довгого періоду часу може призвести до можливості його розшифрування сторонніми особами, які можуть перехоплювати дані, що передаються захищеним каналом шифрування і розшифрувати спільні секретні ключі. Для запобігання цьому у способі передбачена періодична заміна спільних секретних ключів, наприклад, один раз на день, що не дає можливості стороннім особам накопичити необхідній об'єм інформації для розшифровування спільних секретних ключів.

Далі генерують випадкове значення за допомогою генератора випадкових чисел, формують пакет даних, що підлягає передачі захищеним каналом шифрування та здійснюють шифрування пакета даних за допомогою згенерованого випадкового значення та першого і другого спільних секретних ключів відповідно до стандарту симетричного алгоритму блочного шифрування (AES) та передають зашифрований пакет даних каналом зв'язку між МКТП та МКП, після чого здійснюють дешифрування пакета даних на стороні приймання.

Дешифрування отриманих пакетів даних на стороні приймання здійснюють в зворотному порядку від процедури шифрування.

В одному з варіантів здійснення способу випадкове значення, що генерують, є псевдовипадковим значенням.

Для підвищення криптостійкості захищеного каналу шифрування та запобіганню теоретично можливого розшифровування пар приватного та публічного ключів сторонніми особами, у способі передбачена також періодична заміна пар приватного та публічного ключів, наприклад, один раз на рік. Процес заміни пар приватного та публічного ключів відбувається аналогічного до їх першого генерування. У МКТП для першого користувача генерують нову третю пару (RSA) приватного PrKey1_2 та публічного PubKey1_2 ключів, а у МКП для другого користувача генерують нову четверту пару приватного PrKey2_2 та публічного PubKey2_2 ключів. Далі здійснюють обмін новими публічними ключами PubKey1_2, PubKey2_2 між користувачами, PubKey1_2 надсилають до МКП другому користувачу, а PubKey2_2 надсилають до МКТП першому користувачу. Для запобігання несанкціонованому перехопленню нових згенерованих ключів при їх передачі між користувачами їх шифрують відповідно до алгоритму RSA з використанням ще чинних старих першої PrKey1, PubKey1 та другої PrKey2, PubKey2 пар приватного та публічного ключів. Після успішного обміну новими публічними ключами PubKey1_2, PubKey2_2 між користувачами, старі першу та другу пару приватного та публічного ключів визначають нечинними.

Далі в процесі роботи способу захищеного обміну даними між МКТП і МКП його дії циклічно повторюють.

В одному з варіантів здійснення способу генерування пар приватного та публічного ключів здійснюють відповідно до вимог RFC 3447 "Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1".

Запропонований спосіб захищеного обміну даними між МКТП і МКП, завдяки запропонованій послідовності дій, забезпечує надійний обмін даними по захищеному каналу шифрування між модулем криптографічних та технологічних перетворень і модулем криптографічних перетворень, підвищення криптостійкості, запобігання перехопленню публічних ключів, що ним передаються шляхом їх шифрування відповідно до алгоритму шифрування RSA, а також забезпечує унеможливлення несанкціонованого дешифрування захищених даних, що передаються захищеним каналом зв'язку.

Крім цього, заявлений спосіб забезпечує підвищення швидкості передачі даних по каналу шифрування і зниження ресурсоємності, необхідної для шифрування та дешифрування переданих даних, а також забезпечує реалізацію криптографічного алгоритму відповідно до вимог ДСТУ ETSI EN 119 312:2015 для КЗІ, що передається захищеним каналом шифрування.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

1. Спосіб захищеного обміну даними між модулем криптографічних та технологічних перетворень (МКТП) і модулем криптографічних перетворень (МКП), що включає етапи, на яких:
- генерують першу пару приватного та публічного ключів у МКТП та генерують другу пару приватного та публічного ключів у МКП, причому генерування здійснюють відповідно до ДСТУ ETSI EN 119 312:2015,
- здійснюють обмін публічними ключами з першої та другої пари приватного та публічного ключів між МКТП та МКП,
- генерують перший спільний секретний ключ у МКТП і другий спільний секретний ключ в МКП та здійснюють обмін згенерованими першим і другим секретними ключами між МКТП та МКП, причому при здійсненні обміну першим і другим спільними секретними ключами їх шифрують та дешифрують за допомогою згенерованих першої та другої пари приватного та публічного ключів, а перший та другий спільні секретні ключі періодично замінюють новими шляхом їх повторного генерування відповідно до попередньо встановленого часового періоду,
- генерують пакет даних для захищеного обміну між МКТП та МКП,
- генерують випадкове значення за допомогою генератора випадкових чисел,
- здійснюють шифрування пакета даних за допомогою згенерованого випадкового значення та першого і другого спільних секретних ключів відповідно до стандарту симетричного алгоритму блочного шифрування (AES), передають зашифрований пакет даних каналом зв'язку між МКТП та МКП, після чого здійснюють дешифрування пакета даних,
причому першу та другу пару приватного та публічного ключів періодично замінюють новими шляхом їх повторного генерування відповідно до попередньо встановленого часового періоду, при цьому процес заміни включає етапи, на яких:
- генерують третю пару приватного та публічного ключів у МКТП та генерують четверту пару приватного та публічного ключів у МКП, причому генерування здійснюють відповідно до стандарту ДСТУ ETSI EN 119 312:2015,

- здійснюють обмін публічними ключами третьої та четвертої пари ключів між МКТП та МКП, причому при здійсненні обміну публічними ключами третьої та четвертої пари ключів їх шифрують та дешифрують за допомогою чинних першої та другої пари приватного та публічного ключів, а після здійснення обміну першу та другу пару приватного та публічного ключів визначають нечинними.

2. Спосіб за п. 1, який **відрізняється** тим, що генерування пар приватного та публічного ключів здійснюють відповідно до стандарту RFC 3447 "Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1".

3. Спосіб за будь-яким з попередніх пп. 1, 2, який **відрізняється** тим, що попередньо встановлений період заміни спільних секретних ключів складає один день.

4. Спосіб за будь-яким з попередніх пп. 1-3, який **відрізняється** тим, що попередньо встановлений період заміни пар приватного та публічного ключів складає один рік.

5. Спосіб за будь-яким з попередніх пп. 1-4, який **відрізняється** тим, що згенероване випадкове значення є псевдовипадковим значенням.

6. Спосіб за будь-яким з попередніх пп. 1-5, який **відрізняється** тим, що шифрування першого спільного секретного ключа здійснюють за допомогою приватного ключа з першої пари приватного та публічного ключів і публічного з ключа з другої пари приватного та публічного ключів, а шифрування другого спільного секретного ключа здійснюють за допомогою приватного ключа з другої пари приватного та публічного ключів і публічного ключа з першої пари приватного та публічного ключів.

7. Спосіб за будь-яким з попередніх пп. 1-6, який **відрізняється** тим, що дешифрування першого спільного секретного ключа здійснюють за допомогою приватного ключа з другої пари приватного та публічного ключів і публічного ключа з першої пари приватного та публічного ключів, а дешифрування другого спільного секретного ключа здійснюють за допомогою приватного ключа з першої пари приватного та публічного ключів і публічного ключа з другої пари приватного та публічного ключів.

8. Спосіб за будь-яким з попередніх пп. 1-7, який **відрізняється** тим, що дешифрування пакета даних здійснюють в зворотному порядку від процедури шифрування.

Комп'ютерна верстка В. Мацело

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601