DOI: 10.36910/6775-2524-0560-2020-39-21
УДК: 681.3
Гринюк Сергій Васильович, асистент,
https://orcid.org/0000-0002-0080-3167
Поліщук Микола Миколайович, к.т.н., ст. викладач
https://orcid.org/0000-0002-1218-5925
Луцький національний технічний університет

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ШИФРУВАННЯ ІНФОРМАЦІЇ ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ В МЕРЕЖІ

Гринюк С.В., Поліщук М.М. Використання технології шифрування інформації для безпечної передачі в мережі.. Технологія шифрування даних не тільки може шифрувати та дешифрувати дані, але й може реалізувати цифровий підпис, аутентифікацію та автентифікацію та інші функції, забезпечуючи таким чином конфіденційність, цілісність і підтвердження передачі даних по мережі. З метою підвищення безпеки даних у мережевому зв'язку в роботі розглядається гібридна система шифрування, яка використовує для шифрування та дешифрування потрійний алгоритм DES з високою безпекою, і
два ключі шифруються за допомогою алгоритму RSA, забезпечуючи таким чином безпеку потрійного ключа DES та вирішуючи проблему управління ключами.
Ключові слова: безпека мережевого зв'язку, шифрування, алгоритм DES, алгоритм RSA, цифровий підпис.

Гринюк С.В., Полищук Н.Н. Использование технологии шифрования информации для безопасной передачи в сети. Технология шифрования данных не только может шифровать и дешифровать данные, но и может реализовать цифровой подписи, аутентификацию и проверку подлинности и другие функции, обеспечивая таким образом конфиденциальность, целостность и подтверждения передачи данных по сети. С целью повышения безопасности данных в сетевом связи в работе рассматривается гибридная система шифрования, которая использует для шифрования и дешифрования тройной алгоритм DES с высокой безопасностью, и два ключа шифруются с помощью алгоритма RSA, обеспечивая таким образом безопасность тройного ключа DES и решая проблему управления ключами.
Ключевые слова: безопасность сетевой связи, шифрования, алгоритм DES, алгоритм RSA, цифровая подпись.

Hryniuk S.V, Polishchuk M.M. Use information encryption technology for secure network transmission. Data encryption technology can not only encrypt and decrypt data, but can also implement digital signature, authentication and authentication and other functions, thus ensuring the confidentiality, integrity and authentication of data transmission over the network. In order to increase data security in network communication, the paper considers a hybrid encryption system that uses a triple DES algorithm with high security for encryption and decryption, and the two keys are encrypted using the RSA algorithm, thus ensuring the security of the DES triple key and solving the key management problem.
Keywords: network security, encryption, DES algorithm, RSA algorithm, digital signature.

Вступ. Завдяки розвитку комп'ютерних технологій для роботи та життя людей з'явилися великі можливості, а саме спілкування на відстані, обмін інформацією через мережу тощо. Але при цьому виникли проблеми інформаційної безпеки – це стан захищеності інформаційної системи, включаючи інформацію і інфраструктуру самої системи. Інформаційна система знаходиться в стані захищеності, якщо забезпечені її конфіденційність, доступність і цілісність. Конфіденційність (confidentiality) – гарантія того, що секретні дані доступні тільки користувачам, яким доступ дозволений (легальним або авторизованим користувачам). Доступність (availability) – гарантія того, що авторизовані користувачі завжди отримають доступ до даних. Цілісність (integrity) – гарантія збереження даними правильних значень, яка забезпечується забороною неавторизованим користувачам змінювати, модифікувати, видаляти або створювати дані. При цьому загроза – дія, яка направлена на порушення інформаційної безпеки системи, атака – реалізована загроза, а ризик – імовірнісна оцінка величини можливого збитку, який несе власник інформаційного ресурсу в результаті успішно проведеної атаки [3].

Економічні втрати, спричинені вразливістю безпеки інформаційної системи, з кожним роком зростають, а проблема безпеки стає все більш серйозною. Ризик інформаційної безпеки обмежує ефективне використання інформації, що в свою чергу впливає на економіку, національну оборону та навіть несе загрози національній безпеці. Іншими словами, інформаційна безпека має важливий вплив на розвиток сучасного суспільства, захист національної безпеки та соціальної стабільності, та має вирішальний вплив на успіх чи провал інформаційної революції.

Криптовалюта є ядром технологій інформаційної безпеки. Це ключ до реалізації конфіденційності та цілісності. [4]

Постановка проблеми. Популяризація комп'ютерних мережно-комунікаційних технологій є проявом інформатизації сучасного суспільства. Це дає змогу різним сферам діяльності змінити традиційний спосіб передачі та швидкість розповсюдження інформації, яка сприяє покращенню

ефективності роботи. Технологія шифрування даних є головною складовою при передачі інформації через комп'ютерні мережі та спрямована на підвищення її безпеки [5]. В даний час існує багато проблем, пов'язаних із безпекою мережі:

По-перше, різноманітні мережеві хакери використовують власну технологію та інші переваги для комп'ютерної мережі як носія якогось прямого порушення нормального робочого процесу, крадіжка інформації про користувачів та інші дії;

По-друге, деякі злочинці використовують комп'ютерні вразливості для мережевого вірусу, який не тільки впливає на використання комп'ютерних функцій, але й через руйнівну силу самого вірусу, внаслідок чого користувачі комп'ютерної мережі паралізовані, що робить інформацію про користувача або файли повністю відкритою;

По-третє, завдяки швидкому розвитку комп'ютерних технологій з'явилися різноманітні веб-ресурси, що привертають велику кількість користувачів, які будуть з різних причин публікувати деякі помилкові негативні новини та дискредитувати інших і при цьому впливати на життя та роботу інших людей. Щоб цього уникнути почали використовувати технологію шифрування даних при передачі через мережу [6].

Виклад основного матеріалу. Шифрування – практичний засіб забезпечення секретності інформації. Сучасні методи шифрування є математичними перетвореннями (алгоритми), в яких повідомлення розглядаються як числа або алгебраїчні елементи в деякому просторі. Ці алгоритми відображають область «змістовних повідомлень» і область «беззмістовних повідомлень». Повідомлення, з числа «змістовних», також є вихідними даними алгоритму шифрування та називаються відкритим текстом (cleartext), беззмістовні повідомлення, які є результатом роботи алгоритму шифрування, називаються зашифрованим текстом (ciphertext). Якщо знехтувати сенсом повідомлення, то вхідні дані алгоритму шифрування зручно називати вихідним текстом (plaintext), який не зобов'язаний бути осмисленим [2].

Існує два класи криптосистем – симетричні і асиметричні. У симетричних схемах шифрування (класична криптографія) секретний ключ шифрування збігається з секретним ключем дешифрування (рис. 1).

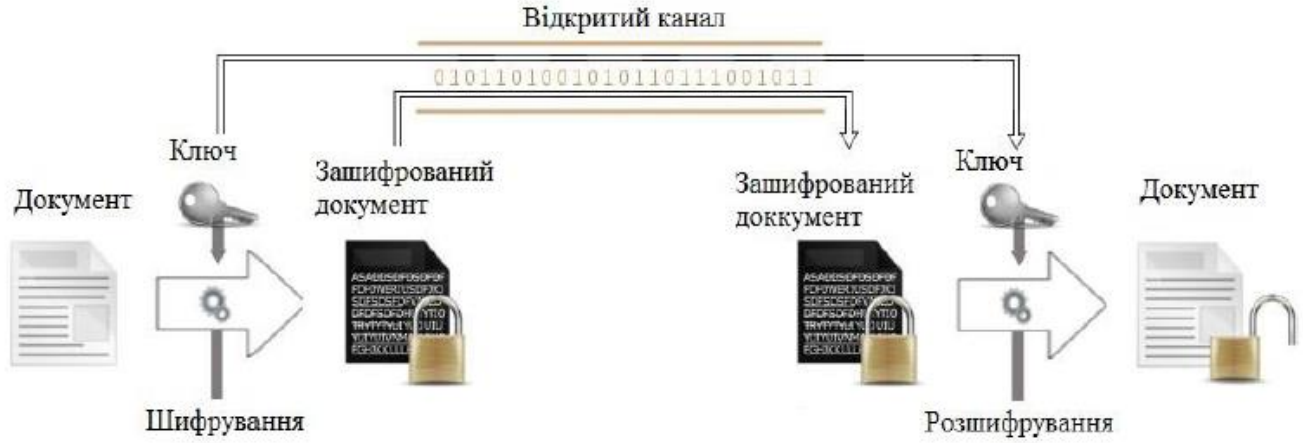

Рис. 1. Схема роботи симетричних алгоритмів

Популярні стандартні симетричні алгоритми шифрування даних є DES (Data Encryption Standard) та AES (Advanced Encryption Standard). AES забезпечує кращий захист, використовує 128-бітові ключі (працює з 192- і 256- бітними ключами) і має високу швидкість роботи, кодуючи за один цикл 128-бітний блок на відміну від 64-бітного блоку DES. В даний час AES є найбільш поширеним симетричним алгоритмом шифрування [1].

У симетричних алгоритмах проблема у ключі. По-перше, криптостійкість багатьох симетричних алгоритмів залежить від якості ключа, це висуває підвищені вимоги до служби генерації ключів. По-друге, важливою є надійність каналу передачі ключа другому учаснику секретних переговорів. Проблема з n ключами виникає навіть у системі з двома абонентами, а в системі з абонентами, охочим обмінюватися секретними даними за принципом «кожен з кожним», потрібно $n * (i - 1)2$ ключів, які

повинні бути згенеровані і розподілені надійним чином. Тобто кількість ключів пропорційна квадрату кількості абонентів, що при великій кількості абонентів робить задачу 13 надзвичайно складною. Несиметричні алгоритми, які засновані на використанні відкритих ключів, знімають цю проблему [3]. В асиметричних схемах шифрування (криптографія з відкритим ключем) відкритий ключ шифрування не збігається з секретним ключем дешифрування (рис. 2).

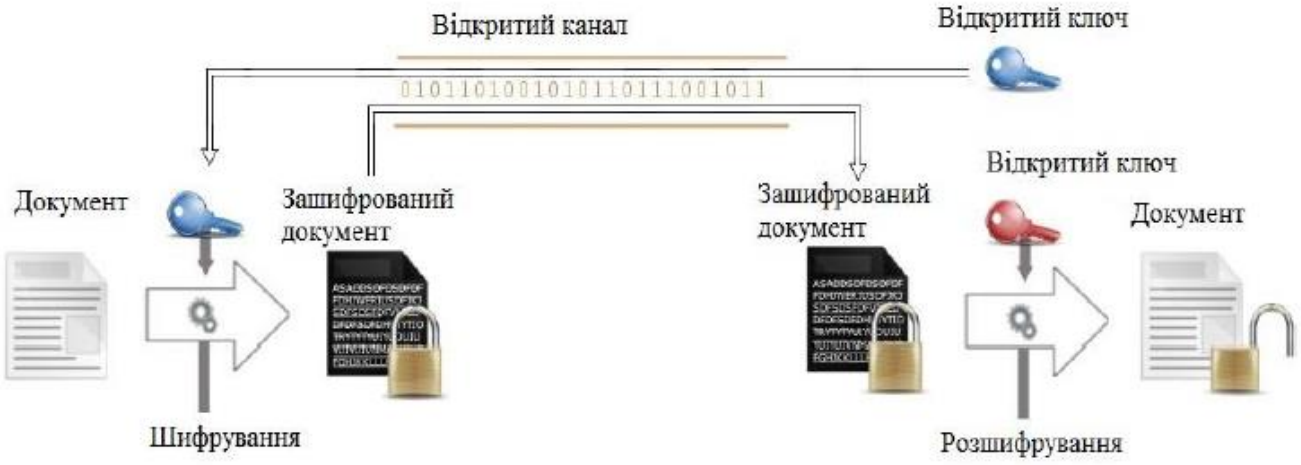

Рис. 2. Схема роботи асиметричних алгоритмів

Особливість шифрування з відкритим ключем в тому, що одночасно генерується унікальна пара ключів. Текст, зашифрований одним ключем, розшифровується тільки з використанням другого. У моделі кріптосхеми з відкритим ключем три учасники: відправник, отримувач і зловмисник. Завдання відправника в тому, щоб по відкритому каналу зв'язку передати повідомлення в захищеному вигляді. Одержувач генерує на своєму боці два ключа: відкритий E і D закритий . Закритий ключ D (особистий) абонент зберігає в захищеному місці, а відкритий ключ E він може передати всім, з ким хоче підтримувати захищені відносини. Для шифрування тексту служить відкритий ключ, але розшифрувати цей текст можна тільки за допомогою закритого ключа. Тому відкритий ключ передається відправнику в незахищеному вигляді. Відправник, використовуючи відкритий ключ одержувача, шифрує повідомлення X і передає його одержувачу. Одержувач розшифровує повідомлення своїм закритим ключем D . Очевидно, що числа, одне з яких служить для шифрування тексту, а інше - для дешифрування, не можуть бути незалежними один від одного, а значить, є теоретична можливість обчислення закритого ключа з відкритого. Однак це пов'язано з величезним обсягом обчислень, які вимагають відповідно величезного часу [3].

Для того щоб в мережі усі n абонентів мали можливість не тільки приймати зашифровані повідомлення, але і самі посилати такі, кожен абонент повинен мати власну парою ключів E і D . В мережі буде $2n$ ключів: n відкритих ключів для шифрування і n секретних ключів для дешифрування. Так вирішується проблема масштабованості – квадратична залежність кількості ключів від числа абонентів в симетричних алгоритмах замінюється лінійною залежністю в несиметричних.

Хоча інформація про відкритий ключ не є секретною, її потрібно захищати від підробок, щоб зловмисник під ім'ям легального користувача не нав'язав свій відкритий ключ, після чого за допомогою свого закритого ключа він зможе розшифровувати всі повідомлення, що посилаються легальному користувачеві, і відправляти свої повідомлення від його імені.

З огляду на особливості технології шифрування симетричного ключа та відкритого ключа, у практичних додатках їх буде два види технології шифрування в поєднанні з гібридною системою шифрування, тобто поєднанням DES та RSA, для передачі мережі шифрування даних за допомогою DES та шифрування за допомогою RSA

Цей спосіб не тільки забезпечує безпеку даних та підвищує швидкість шифрування та дешифрування. Комбінація DES та RSA показана на рис. 3.

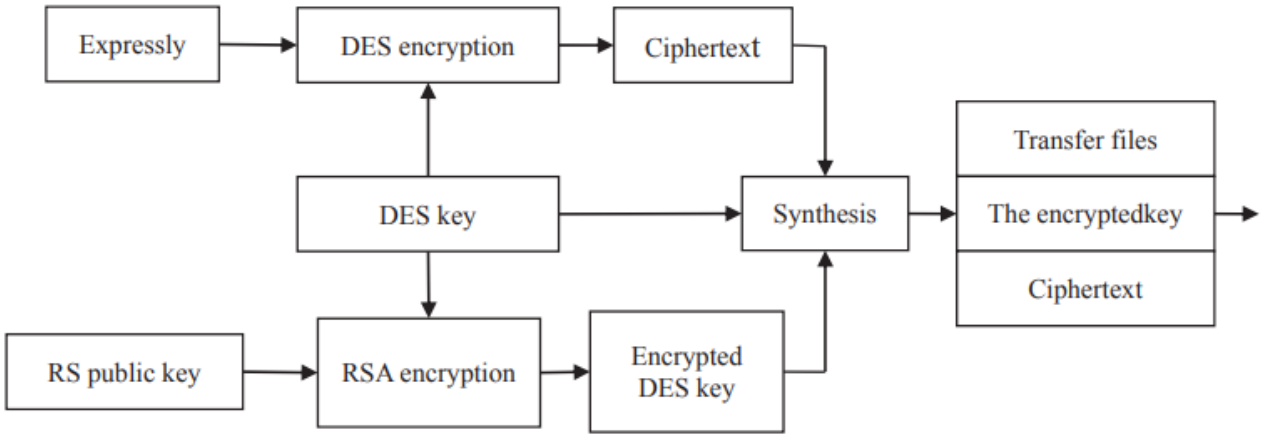

Рис. 3. DES та RSA поєднані за діаграмою технології шифрування

По-перше, відправник використовує алгоритм DES для шифрування інформації plaintext симетричним ключем для отримання знака ciphertext, а потім шифрує симетричний ключ, використовуючи відкритий ключ RSA приймача для отримання зашифрованого DEA або ключ IDEA, зашифровує ciphertext та зашифрований ключ разом із мережею до приймача. Після отримання інформацію про ciphertext приймач розшифровує ключ власним ключем, щоб отримати ключ DES, а потім розшифровує ciphertext за допомогою ключа і, нарешті, отримує інформацію про plaintext, відіграючи, таким чином, роль захисту конфіденційної інформації.

Хоча DES має широкий спектр застосувань і його можна легко отримати з різних джерел. Ключова довжина DES - це лише 56 біт, тому легко атакувати, надійність шифрування не може відповідати сучасним потребам безпеки. Тому використання двох 56-бітових змішувань ключа шифрування та дешифрування, довжина ключа 112, надійність шифрування значно зросла, що є потрійним шифрування DES (3DES). Принципова схема алгоритму 3DES показана на hbc/ 4, де ключ K1, K2 генерується випадковим чином.

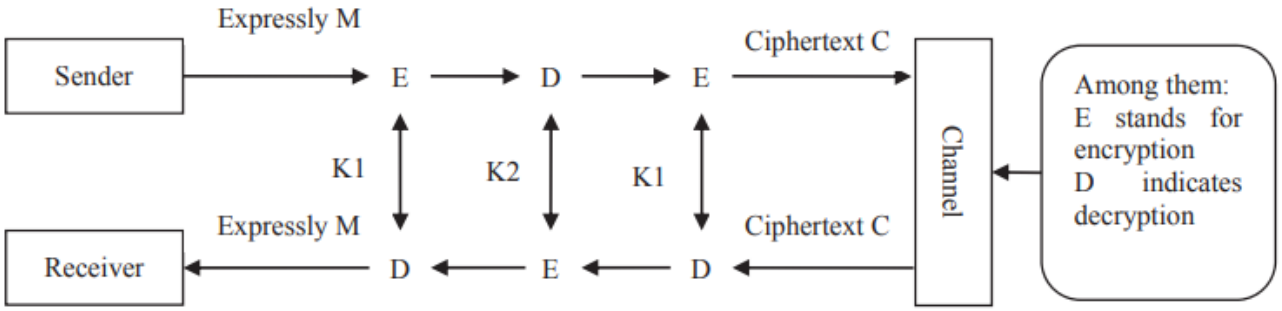

Рис.4. Схема алгоритму 3DES

Потрійна реалізація алгоритму DES включає два класи: DES клас та ТРИ клас. Основні функції класу DES:

```
public staticbyte[ ]encrypt(byte[ ]oword64, int[ ][ ]iSubKeys)//encryption
public static byte[ ]decrypt(byte[ ]bCipher-text, int[ ][ ]SubKeys)//
decryption
THREE main categories of functions:
public static byte[ ]encrypt(byte[ ]oword, int[ ][ ]SubKeysl, int[ ][
]SubKeyS2)// decryption
public static byte[ ]decrypt(byte[ ]sword,int[ ][ ]SubKeysl, int[ ][
]SubKeyS2)//encryption
return plaintext
```

Криптосистема відкритого ключа може використовуватися в технології цифрового підпису. В системі цифрового підпису RSA є однією з найпоширеніших технологій цифрового підпису. Вимоги до технології цифрового підпису повинні бути: жодна інша особа не може підробити підпис, підпис може бути перевірений, і підписувач не може заперечити власний підпис.Цифровий підпис RSA використовує модель аутентифікації в криптосистемі відкритого ключа, як показано на рис. 5. Схема підпису RSA та алгоритм RSA дуже схожа на шифр, не однакова з приватним ключем для підписання відкритий ключ для перевірки, таким чином гарантуючи, що інші люди не можуть підробити підпис, всі власники підписів відкритого ключа можуть бути перевірені, і підписувач не може заперечувати підпис згодом. Для створення можна використовувати: класи, визначені в Java, публічні та приватні ключі RSA, клас підпису в Javax. Пакет безпеки, крім того, що використовується для підписання, може також використовуватися для перевірки цифрових підписів. Метод initverfy () об'єкта підпису передається у відкритий ключ, виконує метод підтвердження () та перевіряє вихідні дані з інформацією про підпис у своєму підписі.

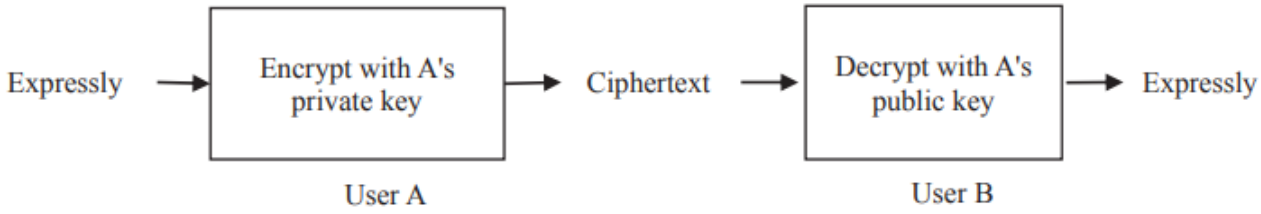

Рис. 5. Модель аутентифікації, що використовується для цифрових підписів

Висновки. Технологія комп'ютерних інформаційних мереж у світі швидко розвивається, що робить інформаційну мережу популярною, люди активно користуються послугами інтернету. Питання безпеки також є серйозною загрозою. Проблема безпеки комп'ютерної мережі - це довгий шлях, який потрібно пройти для вирішення проблеми Завдання та технологія шифрування даних для вирішення цієї проблеми є основним засобом підтримки безпеки комп'ютерної мережі. З розвитком інформаційної ери, комп'ютерне шифрування даних та технології також зробили більш поглиблене дослідження, дослідники повинні продовжувати здійснювати технологічні інновації, а технологія шифрування даних стала ефективною гарантією підтримки безпеки комп'ютерної мережі Система шифрування даних, розроблена в цій статті повністю використовує технологію шифрування даних і цифрову технологія підпису, яка не тільки вирішує ключову проблему управління, але й забезпечує цілісність і достовірність даних**.**

Список бібліографічних посилань

1. Баричев С.Г. Основи сучасної криптографії / С.Г. Баричев, Р.Е. Серов. // Учбовий посібник. – М.: Горячая линия, Телеком, 2002. – 152с.:іл.
2. Мао В. Сучасна криптографія. Теорія і практика / В. Мао. – М.: Вильямс, 2005. – 768 с.
3. Олифер В. Г. Комп'ютерні мережі. Принципи, технології, протоколи / В. Г. Олифер, Н. А.Олифер. // Підручник для вузів. – 5-е вид. – СПб.: Питер, 2016. – 922с.: іл.

References

4. S.H. Yin. Computer network security in the data encryption technology [J]. Electronic Technology and Software Engineering, 2015, 18: 214
5. W. Tang. Cryptography and network security technology foundation [M]. Beijing: Mechanical Industry Press. 2004.
6. David A. Solomon, Mark E. Russinovieh. Inside Microsoft Windows 2000. Microsoft Press. 2000. 8.