

Винахід стосується шифрування та дешифрування даних, зокрема тих даних, які у сфері дії платних телевізійних систем повинні залишатися недоступними для незареєстрованих осіб або пристроїв. У таких системах дані шифруються в захищеному середовищі, яке має значні обчислювальні потужності і називається підсистемою кодування. Далі ці дані пересилаються, з допомогою відомих засобів, до принаймні однієї децентралізованої підсистеми, де вони дешифруються, зазвичай з допомогою IRD (об'єднаного приймача-декодера) із застосуванням чіп-картки. Ймовірно, що незареєстрована особа може одержати необмежений доступ до цієї чіп-картки і децентралізованої підсистеми, яка працює з нею.

Відомою практикою є зв'язування різних засобів шифрування/дешифрування в ланцюг з утворенням системи шифрування/дешифрування. У подальшому викладі вираз "шифрування/дешифрування" буде вживатися у відношенні окремих засобів шифрування, які використовуються в більшій системі.

Довгий час роботу цих систем намагалися оптимізувати з точки зору трьох параметрів: швидкості, зайнятого простору пам'яті та безпеки. Під швидкістю розуміють час, необхідний для дешифрування прийнятих даних.

Відомі системи шифрування/дешифрування із симетричними ключами. Притаманна їм безпека може бути визначена в залежності від кількох критеріїв.

Першим критерієм є фізична безпека, котра пов'язана з легкістю, чи складністю способу простежування, який здійснюється шляхом добування певних компонентів, після чого можлива їх заміна іншими компонентами. Замінені компоненти, призначенням яких є інформувати незареєстровану особу про природу та спосіб роботи системи шифрування/дешифрування, вибираються цією особою так, щоб вони не були виявленими, або ж були настільки недосяжними для виявлення рештою системи, наскільки це можливо.

Другим критерієм є системна безпека, в межах якої атаки відбуваються без втручання у фізичному сенсі, а здійснюються шляхом аналізу, типового для математики. Зазвичай, такі атаки проводяться з допомогою високопотужних комп'ютерів, що намагаються зламати алгоритми і коди шифрування.

Засобами шифрування/дешифрування із симетричними ключами є, наприклад, системи, відомі, як DES (стандарт шифрування даних). В даний час ці відносно старі засоби всього лише дають уяву про системну безпеку та фізичну безпеку, які повністю взаємопов'язані. Саме з цієї причини, зокрема, стандарт DES, довжина ключів якого досить невелика для задоволення умов безпеки системи, здебільшого замінюється новими засобами шифрування/дешифрування або засобами з довгими ключами. Як правило, ці засоби із симетричними ключами вимагають алгоритмів, що містять кільця дешифрування.

Інші стратегії атак відомі під назвами "простий енергетичний аналіз" та "часовий аналіз". У простому енергетичному аналізі використовується той факт, що мікропроцесор, який задіяний у шифруванні або дешифруванні даних, приєднано до джерела живлення (як правило, напругою 5 Вольт). Коли мікропроцесор знаходиться в стані чекання, через нього тече фіксований струм величиною i . Коли ж він знаходиться в стані активності, миттєве значення струму i залежить не тільки від даних, що надходять, але також від алгоритму шифрування. Простий енергетичний аналіз полягає у вимірювання струму i , як функції часу. З результатів цього вимірювання можна зробити висновок щодо виду алгоритму, виконуваного мікропроцесором.

Аналогічно, метод часового аналізу полягає у вимірювання тривалості розрахунків, як функції зразка, поданого на модуль дешифрування. Так, взаємозв'язок між поданим зразком і часом обрахування результату дає можливість добути такі секретні параметри модуля дешифрування, як ключ. Подібна система описана, наприклад, в документі "Часові атаки на розробки Діффі-Хеллмана, RSA¹, DSS² та інші системи", опублікованому Паулем Кочером у збірнику Cryptography Research, 870 Market St, Suite 1088, Сан-Франциско, Каліфорнія, США.

Для посилення безпеки системи шифрування були запропоновані алгоритми, що мають асиметричні ключі, наприклад, так звані системи RSA (Рівеста, Шаміра та Адлемана). Ці системи передбачають генерування пари узгоджених ключів, один, так званий відкритий ключ, служить для шифрування, а інший, так званий особистий ключ, служить для дешифрування. Ці алгоритми виявляють високий рівень безпеки, як системної, так і фізичної. Проте з іншого боку, вони повільніші за традиційні системи, особливо на етапі шифрування.

Найбільш останні технології проведення атак використовують так звану концепцію DPA, що означає "диференційний енергетичний аналіз". Ці методи базуються на припущеннях, які можуть бути доведеними після великого числа проб, про наявність 0 або 1 в заданій позиції ключа шифрування. Вони майже неруйнівні, що робить їх недосяжними для виявлення, і використовують як компонент фізичного втручання, так і компонент математичного аналізу. Спосіб їх роботи нагадує методику дослідження нафтоносних районів, де на поверхні здійснюється вибух відомої потужності і де з допомогою телефонних навушників і зондів, розміщених на також відомих відстанях від місця вибуху, робляться висновки щодо стратиграфічного складу нижніх горизонтів без необхідності проведення значних земляних робіт, а завдяки відбиттю ударних хвиль від границь осадових шарів у цих нижніх горизонтах. Атаки за концепцією DPA описані, зокрема, в §2.1 документа "Застереження стосовно визначення кандидатів AES за смарт-картками", опублікованого 1 лютого 1999 авторами Суреш Чарі, Чаранджіт Джатла, Джосюла Р. Рао та Панкай Рохатті, співробітниками фірми IBM T.J.Watson Research Center, Yorktown Heights, NY.

Необхідність мати протидію атакам типу DPA примушує використовувати так звані системи поставлення умисних "вибільюючих" перешкод, або у вхідній інформації, або на виході алгоритму шифрування/дешифрування. Методика вибілювання описана в § 3.5 згаданого вище документа.

Крім того, факт обмеженості обчислювальних потужностей в децентралізованій підсистемі платної телевізійної системи створює проблему, яка ще ніколи не була задовільно розв'язана і яка стосується формування описаного вище ланцюга достатньої довжини.

Задача даного винаходу полягає в тому, аби запропонувати спосіб шифрування/дешифрування, який був би стійким проти сучасних методів простежування, подібних до описаних вище.

Розв'язання задачі, яка є метою даного винаходу, досягається з допомогою способу, описаного в розпізнавальній частині пункту 1 формули.

Характерна особливість способу полягає в тому, що проміжний модуль починає працювати не тоді, коли отримано результат від попереднього (розташованого вище по потоку даних) модуля, а підключається, як тільки вже надійшла частина інформації. Тому сторонній спостерігач не має можливості встановити вхідні або вихідні умови для цього модуля.

Оскільки дешифрування проводиться в децентралізованій підсистемі, що працює з чіп-карткою, а ця чіп-картка адаптована лише до відносно обмежених обчислювальних потужностей, якщо порівнювати з підсистемою кодування, то вигідно користуватись, наприклад, відкритим асиметричним ключем, який протягом останніх кроків дешифрування працює відносно швидко. Це дає можливість, з одного боку, зберегти невраженими характеристики системи при завершенні виконання цієї процедури, а з іншого боку, сконцентрувати обчислювальні потужності, які в основному пов'язані з шифруванням за допомогою особистого ключа, у підсистемі кодування.

Виявилося, що за рахунок можливості зчеплення, або часткового інтерлівінгу, двох засобів шифрування/дешифрування, які розташовані послідовно один за одним, можна додатково підвищити безпеку. Це зчеплення або частковий інтерлівінг слід розуміти, як процес, котрий полягає в тому, що початок обробки даних другим засобом шифрування/ дешифрування припадає на момент, коли перший засіб шифрування/дешифрування ще не закінчив своєї роботи над цими ж самими даними. Це дає можливість маскувати ті дані, які могли б бути результатом роботи першого модуля, перед тим, як вони будуть піддані обробці другим модулем.

Формування ланцюга може початися, як тільки вираховані першим модулем дані стають частково доступними на його виході для обробки другим модулем.

Винахід дає можливість захиститися від згаданих вище атак шляхом поєднання різних засобів шифрування/дешифрування в системі шифрування/дешифрування і можливо шляхом асоціювання зчеплення або часткового інтерлівінгу з послідовністю, в якій ці засоби ідуть один за одним.

В одному з варіантів здійснення винаходу система шифрування/дешифрування містить підсистему кодування, де послідовно застосовуються три алгоритми:

а) асиметричний алгоритм A_1 з особистим ключем d_1 . Алгоритм A_1 застосовує сигнатуру до незашифрованих даних, що прийшли у повідомленні t , даючи цією операцією першу криптограму c_1 . Це здійснюється з допомогою математичних операцій, які в математиці зазвичай виражаються формулою: $c_1 = t^{\text{exponent } d_1} \text{ modulo } n_1$. В даній формулі n_1 утворює частину відкритого ключа асиметричного алгоритму A_1 , modulo є добре відомим математичним оператором порівняння по модулю в межах множини взаємно простих чисел, а d_1 - це особистий ключ алгоритму A_1 .

б) симетричний алгоритм S , в якому використовується секретний ключ K . Цей алгоритм перетворює криптограму c_1 у криптограму c_2 .

в) асиметричний алгоритм A_2 з особистим ключем d_2 . Цей алгоритм A_2 перетворює криптограму c_2 в криптограму c_3 , з допомогою математичної операції, яка, як і раніше, має вираз: $c_3 = c_2^{\text{exponent } d_2} \text{ mod } n_2$. У цій формулі n_2 утворює частину відкритого ключа асиметричного алгоритму A_2 , а d_2 є особистим ключем алгоритму A_2 .

Криптограма c_3 покидає підсистему кодування і з допомогою відомих засобів надходить до децентралізованої підсистеми. У випадку систем платного телебачення вона може містити також відеоінформацію або повідомлення.

Децентралізована підсистема використовує, у порядку, зворотному до зазначеного вище, три алгоритми A_1' , S' і A_2' . Ці три алгоритми утворюють частину трьох засобів шифрування/дешифрування A_1-A_1' , $S-S'$ та A_2-A_2' , які розподілені між підсистемою кодування та децентралізованою підсистемою і які складають систему шифрування/дешифрування.

г) алгоритм A_2' виконує математичну операцію над c_3 , яка відновлює c_2 і має вираз: $c_2 = c_3^{\text{exponent } e_2} \text{ mod } n_2$. У цій формулі множина, що складається з e_2 і n_2 , є відкритим ключем асиметричного алгоритму A_2-A_2' .

д) симетричний алгоритм S' , в якому використовується секретний ключ K , відновлює криптограму c_1 .

є) асиметричний алгоритм A_1' із відкритим ключем e_1 , n_1 відновлює t шляхом виконання математичної операції, що має вираз: $t = c_1^{\text{exponent } e_1} \text{ mod } n_1$.

В децентралізованій підсистемі зчеплення полягає в тому, що етап декодування д) починається в той час, коли попереднім етапом г) ще повністю не відновлено c_2 , а етап декодування е) починається в той час, коли етапом д) ще повністю не відновлено c_1 . Перевагою способу є те, що створюються перешкоди для здійснення атаки, спрямованої, наприклад, спочатку для добування, в децентралізованій підсистемі, криптограми c_1 в кінці етапу д) для того, щоб порівняти її з незашифрованими даними t , а потім з допомогою c_1 і t атакувати алгоритм A_1' , і далі поступово вздовж ланцюга кодування здійснювати пошук із зворотом.

Зчеплення не є необхідним у підсистемі кодування, яка встановлена в захищеному фізичному середовищі. З іншого боку в децентралізованій підсистемі воно корисне. У випадку платного телебачення IRD (об'єднаний приймач-декодер) фактично встановлюється у приміщенні абонента і може стати предметом атаки описаного вище виду.

Слід врахувати, що атака комбінації трьох зчеплених алгоритмів дешифрування A_1' , S' і A_2' має набагато менше шансів на успіх, ніж у випадку, якби криптограми c_1 і c_2 повністю відновлювалися між кожним етапом г), д) і є). Крім того, той факт, що алгоритми A_1' і A_2' використовуються із відкритими ключами e_1 , n_1 та e_2 , n_2 , означає, що обчислювальні засоби, які потрібні для децентралізованої підсистеми, набагато менші порівняно із засобами підсистеми кодування.

Для прикладу, а також для констатації факту відмітимо, що етапи а) і в), тобто етапи шифрування з допомогою особистих ключів, у 20 разів довші, ніж етапи г) і є) дешифрування з допомогою відкритих ключів.

В одному з варіантів здійснення винаходу, який витікає з попереднього, алгоритми A_1 і A_2 подібні до своїх аналогів A_1' і A_2' .

В іншому варіанті здійснення винаходу, який також витікає з попереднього, на етапі в) використовується

відкритий ключ e_2 , n_2 асиметричного алгоритму A_2 тоді, як на етапі г) криптограма c_3 дешифрується з допомогою особистого ключа d_2 цього алгоритму. Цей варіант здійснення винаходу являє собою можливу альтернативу, коли ресурси децентралізованої підсистеми щодо обчислювальних потужностей аж ніяк не досягнуті.

Хоча чіп-картки використовуються, головним чином, для дешифрування даних, існують також чіп-картки, що мають потужності, які потрібні для проведення операцій шифрування. У цьому випадку описані вище атаки будуть стосуватися також і тих карток для шифрування, які працюють за межами захищених місць, таких, як центр управління. Саме з цієї причини спосіб згідно з винаходом застосовується також до послідовних операцій шифрування, тобто модуль, що знаходиться нижче по потоку інформації, починає свою операцію шифрування, як тільки з'явиться частина інформації, що надходить від модуля вище по потоку. Перевага такого процесу полягає в інтерлівінгу різних модулів шифрування, внаслідок чого в заданий момент часу не є повністю доступним результат, який надходить від модуля, вищого по потоку інформації. Крім того, нижчий по потоку інформації модуль починає проводити свої операції не з повним результатом, а з його частинами, що робить невіддатливим для розкриття спосіб роботи модуля щодо відомого стану на вході або виході.

Даний винахід стане зрозумілим детальніше завдяки наступним ілюстраціям, які подані у вигляді прикладу, що не вносить обмежень, і в яких:

на Фіг.1 показані операції шифрування,

на Фіг.2 показані операції дешифрування,

на Фіг.3 показано альтернативний спосіб шифрування.

На Фіг.1 показано, що в ланцюг шифрування вводиться множина m даних. Перший елемент A_1 проводить операцію шифрування, використовуючи так званий особистий ключ, який складається з показника степеня d_1 та модуля n_1 . Результат цієї операції представляється, як C_1 . Згідно із способом роботи, запропонованим у винаході, як тільки з'являється частина результату C_1 , починає працювати наступний модуль. Цей наступний модуль S виконує свою операцію шифрування з допомогою секретного ключа. Як тільки результат C_2 з'являється частково, він передається до модуля A_2 для проведення третьої операції шифрування з використанням так званого особистого ключа, який складається з показника степеня d_2 та модуля n_2 . Кінцевий результат, позначений тут через C_3 , готовий для передавання відомими шляхами, як, наприклад, теле- і радіомовленням або по кабелю.

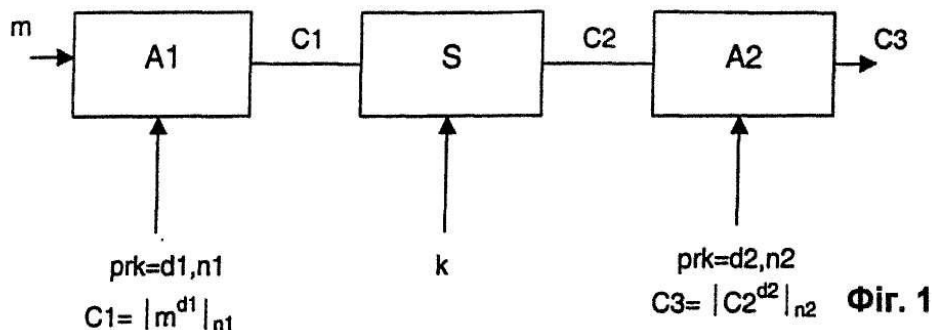
На Фіг.2 показана система дешифрування, що складається з трьох модулів дешифрування A_1' , S' , A_2' , які подібні до модулів, що служать для шифрування, але розміщені у зворотному порядку. Так, спершу маємо справу з модулем A_2' , який проводить свою операцію дешифрування на основі так званого відкритого ключа, що складається з показника степеня e_2 та модуля n_2 . Так само, як і у випадку шифрування, як тільки на виході модуля A_2' з'являється частина результату C_2 , вона передається до модуля S' для другої операції дешифрування. Для завершення дешифрування модуль A_1' виконує свою операцію на основі так званого відкритого ключа, який складається з показника степеня e_1 та модуля n_1 .

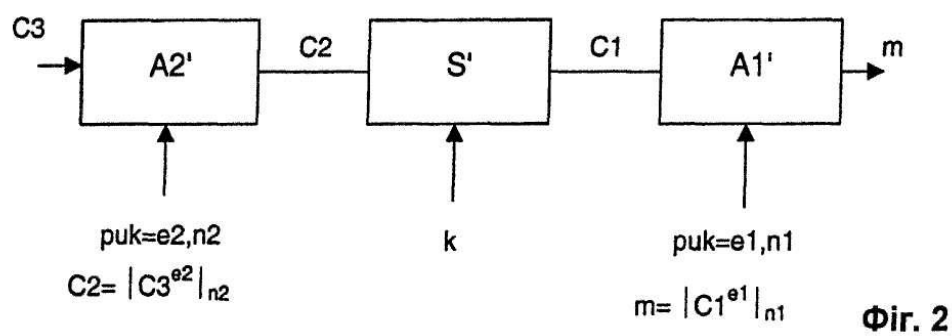
В одному з варіантів здійснення винаходу ключі двох модулів A_1 і A_2 ідентичні, тобто з боку шифрування $d_1=d_2$ і $n_1=n_2$. Аналогічно, при дешифруванні $e_1=e_2$ і $n_1=n_2$. У цьому випадку говорять про особистий ключ d , n та про відкритий ключ e , n .

В іншому варіанті здійснення винаходу, як показано на Фігурах 3 і 4, в модулі A_2 використовується так званий відкритий ключ замість так званого особистого ключа. При шифруванні в модулі A_2 використовується відкритий ключ e_2 , n_2 (див. Фіг.3), а при дешифруванні (див. Фіг.4) для роботи модуля A_2' використовується відкритий ключ d_2 , n_2 . Хоча ця конфігурація передбачає великий обсяг роботи для системи дешифрування, використання особистого ключа посилює безпеку, гарантовану модулем A_2 .

Приклад, показаний на Фігурах 3 і 4, не вносить обмежень щодо інших комбінацій. Наприклад, конфігурацію модуля A_1 можна встановити такою, щоб він виконував операцію шифрування з допомогою відкритого ключа, а дешифрування з допомогою особистого ключа.

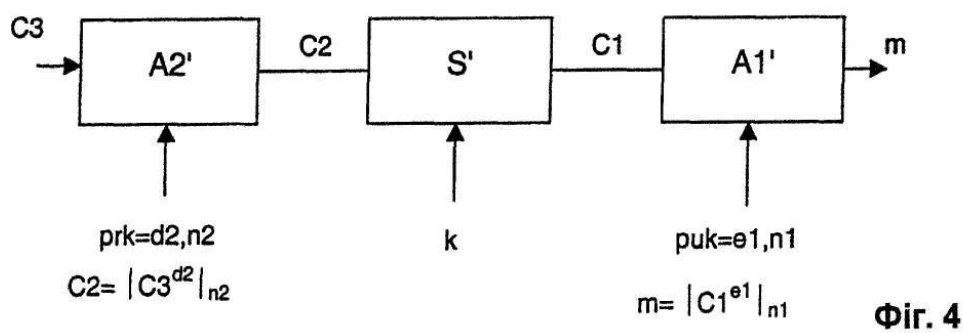
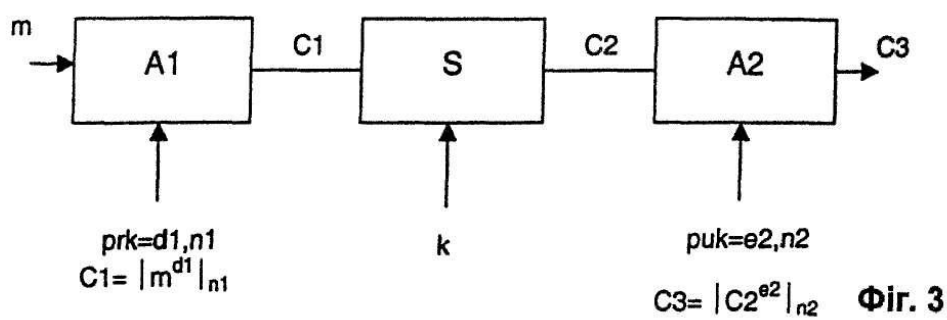
Можна також замінити модуль шифрування/дешифрування, який має секретний ключ S , модулем з асиметричними ключами, такого ж виду, як модулі A_1 і A_2 .





prk – особистий ключ

puk – відкритий ключ



prk – особистий ключ

puk – відкритий ключ