УКРАЇНА

(19) UA (11) 76554 (13) C2

(51) МПК (2006)
H04L 9/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) СПОСІБ БЛОЧНОГО ШИФРУВАННЯ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ

(21) 20040705295
(22) 02.07.2004
(24) 15.08.2006
(46) 15.08.2006, Бюл. № 8, 2006 р.
(72) Нагорняк Юрій Васильович, Дементьєв Юрій Вікторович
(73) Вінницький національний технічний університет
(56) RU 2091983 C1, 27.09.1997
RU 2032990 C1, 10.04.1995
RU 2212108 C1, 10.09.2003
FR 2836311 A1, 22.08.2003
UA 41481 C, 17.09.2001
US 5168521 A, 01.12.1992
US 6249582 A, 19.06.2001

(57) 1. Спосіб блочного шифрування електронної інформації, який включає формування ключа шифрування у вигляді сукупності b-бітових підключів, розбиття вхідного блока даних на два b-бітових підблоки A і B, проведення раундів шифрування шляхом перетворення підблоків під керуванням ключа шифрування за допомогою операцій додавання за модулем 2^b, які виконують над підблоком і підключем, і операцій циклічного зсуву, які виконують над підблоком залежно від іншого підблока, який **відрізняється** тим, що використовують ключ шифрування фіксованої довжини, як перший блок даних використовують випадкове число, здійснюють модифікацію ключа шифрування для кожного наступного блока даних залежно від поточного блока даних, виконують операції циклічного зсуву підблоків залежно від підключів.

2. Спосіб за п. 1, який **відрізняється** тим, що ключ шифрування представляють у вигляді чотирьох b-бітових підключів - K_1, K_2, K_3, K_4.

3. Спосіб за п. 1, який **відрізняється** тим, що під час виконання операцій циклічного зсуву зсув здійснюють на значення просумованих по модулю два байтів керуючого операнда.

4. Спосіб за п. 1, який **відрізняється** тим, що для модифікації ключа шифрування для кожного наступного блока даних залежно від поточного блока даних використовують операції додавання за модулем два, які виконують над підключем і підблоком даних та операції циклічного зсуву, які виконують над підключем залежно від підблока.

(19) UA (11) 76554 (13) C2

Винахід відноситься до галузі електронно-обчислювальної техніки та систем передачі інформації, а саме до криптографічних способів захисту інформації.

Відомим аналогом способу блочного шифрування електронної інформації, що заявляється є DES. Спосіб блочного шифрування DES до недавнього часу був стандартом шифрування в США [National Bureau of Standards. Date Encryption Standard. Federal Information Processing Standards Publication 46. January 1977]. Цей спосіб передбачає представлення ключа шифрування у вигляді сукупності 48-бітових підключів, розбиття вхідного 64-бітового блоку даних на два 32-бітових підблоки L і R та виконання 16 раундів перетворення 32-бітового підблоку даних. Перетворення включають розширення підблоку R до 48 бітів шляхом повторення деяких бітів цього підблоку R $R^{/}$ виконання операції додавання за модулем 2 над підблоком і підключем, перетворення 48-бітового підблоку в 32-бітовий з допомогою таблиць підстановки $R^{/}$ $R^{//}$, здійснення операцій перестановки бітів підблоку $R^{//}$, за певним законом, виконання операції додавання по модулю 2 підблоку $R^{//}$ з підблоком L, перестановку підблоків $R^{//}$ і L.

Розглянутий аналог має наступні недоліки:

1) низька швидкість шифрування під час програмної реалізації, так як спосіб при розробці був розрахований на апаратну реалізацію у вигляді електронних схем і містить операції бітової перестановки, які виконуються на процесорах за неприйнятне великий час;

2) використання короткого 56-бітового ключа, що дозволяє на потужних комп'ютерах розкрити секретний ключ методом підбору можливих значень ключа;

3) використання фіксованих підключів для всіх

можливих вхідних блоків шифруємих даних, що призводить до зниження криптостійкості.

Прототипом даного винаходу є спосіб блочного шифрування RC-5 [R. Rivest, The RC5 Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994) Lecture Notes in Computer Sciens, v.1008. Springer-Verlag, 1995 pp. 86-96]. В цьому способі ключ шифрування представляють у вигляді сукупності підключів – $K_0,K_1,...,K_{2r+2}$, де r - кількість раундів шифрування. Вхідний блок даних розбивають на два b-бітових підблоки -A і B. Шифрування заключається в почерговому перетворенні підблоків за допомогою операцій додавання за модулем 2^b, які виконують над підблоком і підключем, операцій додавання за модулем 2, які виконують над двома підблоками, і операції циклічного зсуву, які виконують над підблоком в залежності від іншого підблоку. Варіанти операцій циклічного зсуву відрізняються величиною зсуву від 0 до b-1 біт. Для вибору конкретної модифікації операції циклічного зсуву використовується $\log_2$ b молодших розрядів керуючого блока. На кожному раунді шифрування використовують нову пару ключів, тому для різної кількості раундів шифрування застосовують ключі різної довжини. Проте для кожного нового блоку використовують той самий набір підключів.

Спосіб здійснюється наступним чином:

1. Задають число раундів r і довжину підблоку b;

2. Формують ключ шифрування у вигляді сукупності підключів –$K_0,K_1,...,K_{2r+2}$.

3. Вхідний блок даних розбивають на два b-бітових підблока - A і B.

4. Виконують перетворення:

$A:=(A+K_0)\bmod 2^b$;

$B:-(B+K_1)\bmod 2^b$;

5. Проводять r раундів перетворень:

$A :- ([(A \oplus B] \ll B) + K_{2i} \bmod 2^b$

$B :- ([(B \oplus A] \ll A) + K_{2i+1} \bmod 2^b$

де i є [1 ..r] - номер раунду шифрування.

Розглянутому способу властиві наступні недоліки:

1) для будь яких вхідних блоків даних використовуються ті самі підключі, тому спосіб не має достатньої стійкості до диференційного і лінійного криптоаналізу;

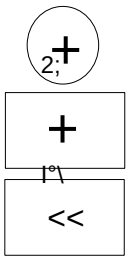
2) при малій кількості раундів шифрування, є можливість часткового розкриття зашифрованого тексту при використанні ключа близького до таємного;

3) на керовану операцію циклічного зсуву мають вплив лише $\log_2 b$ молодших бітів керуючого блоку, що призводить до зменшення криптостійкості.

В основу винаходу покладено задачу створення способу блочного шифрування електронної інформації, в якому за рахунок введення нових та модифікації існуючих в прототипі операцій буде забезпечуватись більша стійкість до лінійного та диференційного криптоаналізу при меншій кількості операцій перетворень, що підвищить швидкодію та надійність способу.

Поставлена задача досягається тим, що у способі блочного шифрування електронної інформації, який включає формування ключа шифрування у вигляді сукупності b-бітових підключів, розбиття вхідного блоку даних на два b-бітових підблока A і B, проведення раундів шифрування шляхом перетворення підблоків під керуванням ключа шифрування за допомогою операцій додавання за модулем 2^b, які виконують над підблоком і підключем і операцій циклічного зсуву, які виконують над підблоком в залежності від іншого підблоку використовують ключ шифрування фіксованої довжини. Ключ шифрування представляють у вигляді чотирьох b-бітових підключів – K_1,K_2,K_3,K_4. В якості першого блоку даних використовують випадкове число. Здійснюють модифікацію ключа шифрування для кожного наступного блоку даних в залежності від поточного блоку даних, за допомогою операцій додавання за модулем 2 та операції циклічного зсуву, які виконують над підключем в залежності від підблоку. Виконують операції циклічного зсуву підблоків в залежності від підключів. В операціях циклічного зсуву, зсув здійснюють на значення просумованих по модулю 2 байтів керуючого операнда, таку операцію циклічного зсуву будемо позначати « .

На фігурі 1 показана структура представлення даних для шифрування. Фігура 2 відображає структурну схему одного раунду шифрування блоку даних. На фігурі 3 показано структурну схему міжблокової модифікації ключа. На фігурах використано наступні позначення:



- операція додавання за модулем

- операція додавання за модулем

- операція циклічного зсуву на значення просумованих по модулю 2 байтів керуючого операнда;

лініями позначено передачу b-бітового сигналу.

Спосіб здійснюється наступним чином:

1. Задають довжину підблока b та кількість раундів шифрування r.

1. Вхідні дані розбивають на n-1 блоків, довжиною 2b біт.

2. Генерують випадковий блок даних, та вставляють його перед блоками вихідних даних.

3. Представляють початковий ключ шифрування як сукупність чотирьох b-бітових підключів K_1,K_2,K_3,K_4.

4. Проводять шифрування n блоків даних.

Шифрування блоку даних здійснюється в наступній послідовності:

1. Вхідний блок даних розбивають на два b-бітових підблока - A і B.

2. Визначають ключ, що буде використовуватися для наступного блоку даних по таким співвідношенням:

$K_1(t+1):= (K_1(t) \oplus A) \ll B$

$K_2(t+1):= (K_2(t) \oplus B) \ll A$

$K_3(t+1) := (K_3(t) \oplus A) << B$

$K_4(t+1) := (K_4(t) \oplus B) << A$

де t є [1 ..n] - номер блоку даних.

3. Проводять r раундів перетворень підблоків A і B за співвідношеннями:

$A := ((A + K_1) \bmod 2^b) \lll (K_1 \oplus K_3)$;

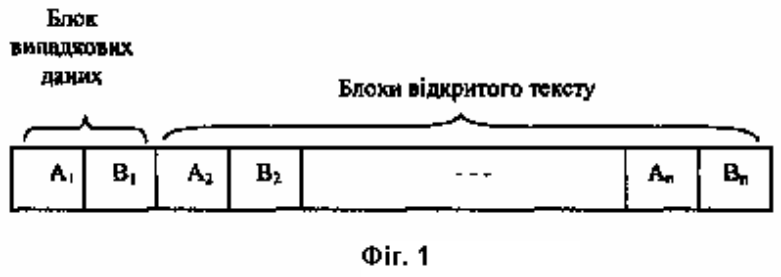
$B := ((B + K_2) \bmod 2^b) \lll (K_2 \oplus K_4)$;

$A := ([(A \lll B] + K_3) \bmod 2^b$;

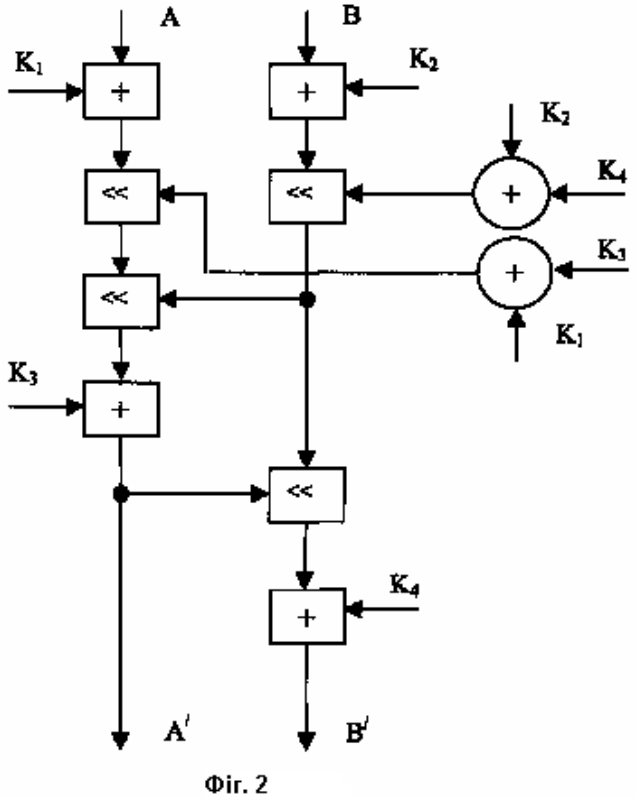
$B := ([(B \lll A] + K_4) \bmod 2^b$.

Принцип роботи винаходу пояснюється на фіг. 1-3.

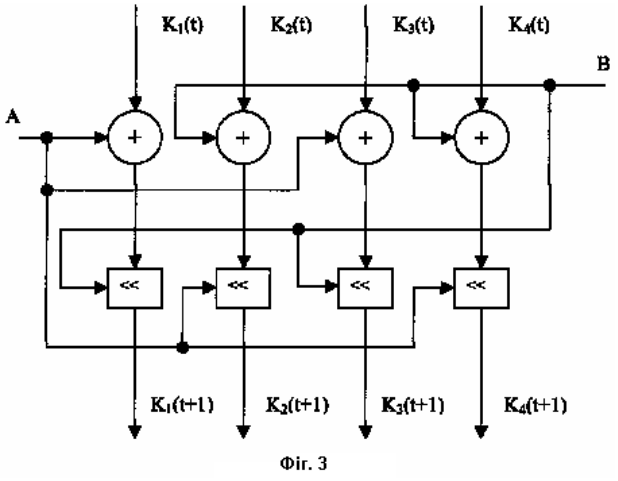
Описаний спосіб може бути реалізований у вигляді спеціалізованих електронних схем, на базі встроєних мікроконтролерів та у вигляді програм для комп'ютерів.



Фіг. 1



Фіг. 2



Фіг. 3

Комп'ютерна верстка М. Клюкін Підписне Тираж 26 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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