УКРАЇНА

(19) UA (11) 38795 (13) U

(51) МПК (2009)
H04L 9/06

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ШИФРУВАННЯ ДАНИХ ДЛЯ СИСТЕМ ОБРОБКИ В ЕОМ

(21) u200714931
(22) 27.12.2007
(24) 26.01.2009
(46) 26.01.2009, Бюл.№ 2, 2009 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, UA, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ, UA
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, UA
(57) Спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n-бітні блоки, кожний з яких послідовно розміщують в накопичувачі, зашифрування яких складається з чотирьох циклів, при цьому дані r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_i з виходу і-го накопичувача секретного ключа кожного циклу надходять на вхід циклової функції перетворення $f(r_{i-1},K_i)$, яка є множенням значення даних r_{i-1} на першу складову підключа зашифрування за модулем, який **відрізняється** тим, що в кожному циклі використовують окремий модуль m_i, який є другою складовою підключа K_i, які розміщують в і-му накопичувачі секретного ключа, а циклову функцію $f(r_{i-1},K_i) \equiv r_{i-1} \cdot A_i \bmod m_i$ реалізують за допомогою блока множення за модулем, на входи якого додатково подають значення модуля m_i з і-го накопичувача секретного ключа, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, у кожному циклі дані r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_{5-i} з виходу (5-i)-го накопичувача секретного ключа подають на вхід циклової функції перетворення $f(r_{i-1},K_{5-i}) \equiv r_{i-1} \cdot A_{5-i}^{-1} \bmod m_{5-i}$, яка є множенням значення r_{i-1} з (i-1)-го накопичувача тексту на першу складову підключа розшифрування за модулем, який є другою складовою підключа розшифрування, які подають з (5-i)-го накопичувача секретного ключа і реалізують за допомогою блока множення за модулем.

1 2

Корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в електронно-обчислювальній техніці та у системах передачі інформації.

Відомим є спосіб блокового симетричного шифрування базовою операцією якого є операція множення за модулем. Зашифрування блоку відкритого тексту здійснюється за правилом $C=((((M\times K_1)_{mod2^n}\oplus K_2)\times K_3)_{mod2^n}+K_4)_{mod2^n}$, де K_1, K_2, K_3, K_4 - підключі, які отримуються з секретного ключа К шляхом використання процедури розгортання. Для розшифрування блоку закритого тексту С необхідно виконати обчислення за таким правилом $M=((((C-K_4)_{mod2^n}/K_3^{-1})_{mod2^n}\oplus K_2)/K_1^{-1})_{mod2^n}$, де K_1^{-1}, K_3^{-1} - числа, що є оберненими відповідно до K_1 та K_3 за модулем 2^n. [Сокирук В.В., Лужецький В.А. Побудова статистично безпечного БСШ на основі арифметичних операцій за модулем //Інформаційні технології та комп'ютерна інженерія. -2006. -№1. -С.158-163].

Недоліком цього способу є недостатня надійність за рахунок того, що на всіх етапах обчислення криптографічних перетворень використовується одне значення модуля 2^n.

Найбільш близьким за сукупністю ознак до запропонованого є спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n бітні блоки, кожний з котрих розбивають у свою чергу на правий R_o та лівий L_0 півблоки по n/2 біти, які розміщують у відповідних накопичувачах, зашифрування котрих включає в себе 1 циклів, при цьому дані правого півблока R_{i-1} використовують для обчислення різниці за модулем m зі значенням лівого півблока L_{i-1} і цю різницю заносять у накопичувач правого півблока наступного циклу так, що $R_i=R_{i-1}-L_{i-1}$ (mod m), ви-

(19) UA (11) 38795 (13) U

хідні дані циклової функції заносять у накопичувач лівого півблока, тобто $L_i=f(R_{i-1},K_i)$, при цьому як циклову функцію перетворення використовують модульне множення значення R_{i-1} накопичувача N_{i-1} правого півблока на ключ зашифрування $K_i \equiv (K_i)^E (\mathrm{mod}\, m)$, так що у накопичувач N_i лівого півблока наступного циклу заносять число $L_i \equiv R_{i-1} \cdot (K_i)^E (\mathrm{mod}\, m)$, тобто $f(R_{i-1},K_i) \equiv R_{i-1} \cdot (K_i)^E (\mathrm{mod}\, m)$, а при розшифруванні, яке проводиться в оберненому порядку по відношенню до зашифрування, у кожному циклі в основному режимі значення L_{j-l} накопичувача N_{j-l} і лівого півблока подають на вхід циклової функції перетворення $g(L_{i-l},K_{l-j+1})$, при цьому як циклову функцію перетворення використовують модульне множення значення L_{j-l} накопичувача N_{i-1} лівого півблока на ключ розшифрування $K_j \equiv (K_{l-j+1})^{-E} (\mathrm{mod}\, m)$, так що у накопичувач Ni правого півблока наступного циклу заноситься число $R_j \equiv L_{j-1} \cdot (\mathrm{mod}\, m)$, тобто $R_j \equiv f'(L_{j-1},K_{l-j+1}) \equiv L_{j-1} \cdot (K_{l-j+1})^{-E} (\mathrm{mod} m)$, а значення накопичувача правого півблока R_{j-1} сумують за модулем m зі значенням виходу циклової функції перетворення $g(L_{j-1}, K_{l-j-1})$ і результат заносять в накопичувач Ni лівого півблока наступного циклу, тобто $L_i=R_{j-1}+g(L_{j-1},K_{l-j+1})(\mathrm{mod} m)$ а в режимі використання лазівки обчислюють піднесення значення L_{j-1} накопичувача N_{j-1} лівого півблока до степеня D за модулем m, тобто обчислюють $X_{j-1}=(L_{j-1})^D (\mathrm{mod} m)$, і потім з отриманого числа обчислюють корінь степеня D за модулем m, і в накопичувач Ni правого півблока заносять число $R_j = \sqrt[D]{X_{j-1}}$, тобто циклова функція перетворення має вигляд

$$h(L_{j-1}, L(m)) = \sqrt[D]{X_{j-1}} (\mathrm{mod}\, m),$$

а значення накопичувача правого півблока R_{j-1} сумують за модулем m зі значенням виходу тепер вже циклової функції перетворення $h(L_{j-1}, L(m))$, і результат заносять в накопичувач N_i лівого півблока наступного циклу, тобто $L_j \equiv R_{j-1} + h(L_{j-1}, L(m)) (\mathrm{mod}\, m)$, де m=pq - модуль перетворення, котрий є добутком двох простих чисел p і q, L(m) - узагальнена функція Ейлера числа т, показники степенів E і D пов'язані умовою $ED \equiv 0 (\mathrm{mod} L(m))$ [Патент України №50199, МПК H04L9/06, Бюл. №10, 2002р.].

Недоліком цього способу є недостатня швидкодія роботи шифру, за рахунок великої обчислювальної складності отримання ключа зашифрування циклових функцій, а також використання великої кількості циклів.

В основу корисної моделі поставлена задача створення способу шифрування даних для систем обробки в ЕОМ, в якій за рахунок використання арифметичних операції за модулем досягається можливість зменшення кількості циклів шифрування, що приводить до підвищення швидкодії виконання шифрування і збільшення криптографічної стійкості за рахунок використання секретних ключів шифрування, до складу яких входить модуль.

Поставлена задача вирішується тим, що в спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивають на n бітні блоки, кожний з яких послідовно розміщують в накопичувач, зашифрування яких складається з чотирьох циклів, при цьому дані r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_i з виходу i-го накопичувача секретного ключа кожного циклу надходять на вхід циклової функції перетворення $f(r_{i-1}, K_i)$, яка є множенням значення даних r_{i-1} на першу складову підключа зашифрування за модулем, відповідно до винаходу в кожному циклі використовують окремий модуль m_i, який є другою складовою підключа K_i які розміщують в і-му накопичувачі секретного ключа, а циклову функцію $f(r_{i-1},K_i) \equiv r_{i-1} \cdot A_i \mathrm{mod} m_i$ реалізують за допомогою блока множення за модулем, на входи якого додатково подають значення модуля m_i з і-го накопичувача секретного ключа, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, у кожному циклі дані r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_{5-1} з виходу (5-і)-го накопичувача секретного ключа подають на вхід циклової функції перетворення $f(r_{i-1},K_{5-i}) \equiv r_{i-1} \cdot A_{5-i}^{-1} \mathrm{mod} m_{5-i}$, яка є множенням значення r_{i-1} з (i-1)-го накопичувача тексту на першу складову підключа розшифрування за модулем, який є другою складовою підключа розшифрування, які подають з (5-і)-го накопичувача секретного ключа і реалізують за допомогою блока множення за модулем.

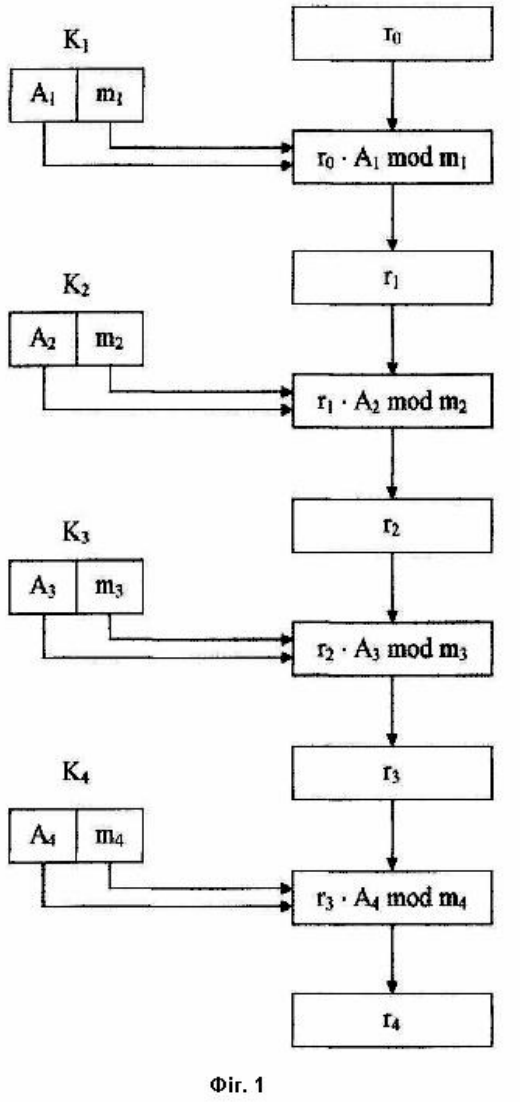
На Фіг.1 зображена структурна схема зашифрування блоку даних;

на Фіг.2 - структурна схема розшифрування блоку шифротексту.

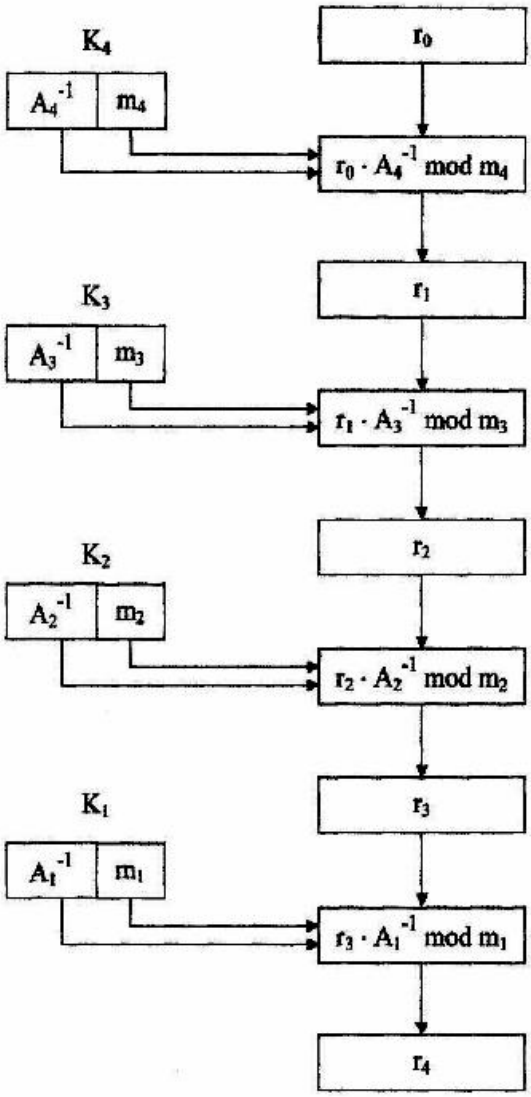
Спосіб здійснюється таким чином, n бітні блоки даних r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_i з виходу і-го накопичувача секретного ключа кожного циклу надходять на вхід циклової функції зашифрування $f(r_{i-1},K_i) \equiv r_{i-1} \cdot A_i \mathrm{mod} m_i \quad (i = \overline{1 \div 4})$, яка є множенням значення даних r_{i-1} з виходу (i-1)-го накопичувача тексту на першу складову підключа зашифрування за модулем, який є другою складовою підключа K_i, які розміщують в і-му накопичувачі секретного ключа та реалізують за допомогою блока множення за модулем, циклова функція розшифрування $f(r_{i-1},K_{5-i}) \equiv r_{i-1} \cdot A_{5-i}^{-1} \mathrm{mod} m_{5-i}$, на входи якої у кожному циклі подають дані r_{i-1} з виходу (i-1)-го накопичувача тексту і дані відповідного підключа K_{5-i} з виходу (5-і)-го накопичувача секретного ключа, є множенням значення r_{i-1} з (i-1)-го накопичувача тексту на першу складову підключа розшифрування за модулем, який є другою скла-

довою підключа розшифрування, які подають з (5-і)-го накопичувача секретного ключа і реалізують за допомогою блока множення за модулем, в яких підключі зашифрування формують з складових A_i та m_i, тобто $K_i=A_i||m_i$, які розміщують у (2n+2)-розрядні накопичувачі, де A_i розміщують в старші (n+1) розряди та m_i в молодші (n+1) розряди, а підключі розшифрування використовують складові A_i^{-1} та m_i, тобто $K_i=A_i^{-1}||m_i$. за якими проводять обчислення у кожному циклі, де A_i^{-1} - число, що є оберненим до A_i за модулем m_i, де A_i^{-1} розміщують в старші (n+1) розряди та m_i в молодші (n+1) розряди (2n+2)-розрядного накопичувача, які вибирають з таких умов $m_i<m_{i+1}$, $2A_i>m_i$, $A_i \cdot A_{i+1}>m_{i+1}$, причому розрядність m_i вибирають з умови, що $2^n<m_i<2^{n+1}$, тому накопичувачі всіх циклів, окрім першого, мають додатковий бітовий розряд (вхідний n бітовий блок відкритого тексту завжди не перевищує значення 2^n, в той час коли в інших циклах при виконанні арифметичних операцій за модулем m_i можуть бути отримані числа, що перевищують 2^n). Далі виконують однотипні операції зашифрування, які повторюють чотири цикли у результаті чого формують зашифроване повідомлення. На кожний n бітовий блок відкритого тексту процедура формує зашифрований блок, довжина якого складає n+1 бітів і який заносять в останній накопичувач.

Процедура розшифрування є оберненою до процедури зашифрування, на вхід першого накопичувача подають n+1 бітовий блок зашифрованого тексту, а після завершення розшифрування на виході останнього накопичувача отримують n бітовий блок відкритого тексту, причому секретні підключі розшифрування використовують в оберненому порядку по відношенню до секретних ключів зашифрування.



Фіг. 1



Фіг. 2

Комп'ютерна верстка С.Литвиненко Підписне Тираж 28 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