



УКРАЇНА

(19) UA

(11) 50199

(13) A

(51) 6 H04L9/06

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС

ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВІНАХІДВИДАЄТЬСЯ ПІД
ВІДПОВІДАЛЬНІСТЬ
ВЛАСНИКА
ПАТЕНТУ

(54) СПОСІБ ШИФРУВАННЯ ДАНИХ ДЛЯ СИСТЕМ ОБРОБКИ В ЕОМ

1

2

(21) 2001117911

(22) 20 11 2001

(24) 15 10 2002

(46) 15 10 2002, Бюл. № 10, 2002 р.

(72) Лисицька Ірина Вікторівна, Руженцев Віктор Ігорович

(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

(57) Спосіб шифрування даних для систем обробки в ЕОМ, який полягає у тому, що послідовність двійкових символів відкритого тексту розбивають на n бітні блоки, кожний з котрих розбивають у свою чергу на правий R_0 та лівий L_0 півблоки по $n/2$ біти, які розміщують у відповідних накопичувачах, зашифрування котрих включає в себе l циклів, при цьому дані R_{j-1} з виходу накопичувача N_j правого півблока і дані відповідного підключа K_j кожного циклу надходять на вхід циклової функції перетворення $f(R_{j-1}, K_j)$, який відрізняється тим, що вихідне значення даних правого півблока R_{j-1} також використовують для обчислення різниці за модулем m зі значенням даних лівого півблока L_{j-1} , і цю різницю заносять у накопичувач правого півблока наступного циклу, так що $R_j = R_{j-1} - L_{j-1} \pmod m$, вихідні дані циклової функції заносять у накопичувач лівого півблока, тобто $L_j = f(R_{j-1}, K_j)$, при цьому як циклову функцію перетворення використовують модульне множення значення R_{j-1} накопичувача N_j правого півблока на ключ зашифрування $K_j \equiv (K_j)^E \pmod m$, так що у накопичувач N_j лівого півблока наступного циклу заносять число $L_j \equiv R_{j-1} \cdot (K_j)^E \pmod m$, тобто $f(R_{j-1}, K_j) \equiv R_{j-1} \cdot (K_j)^E \pmod m$, а при розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, у кожному циклі в основному режимі значення L_{j-1} накопичувача N_{j-1}

лівого півблока подають на вхід циклової функції перетворення $g(L_{j-1}, K_{j+1})$, при цьому як циклову функцію перетворення використовують модульне множення значення L_{j-1} накопичувача N_{j-1} лівого півблока на ключ розшифрування $K_{j+1}^* \equiv (K_{j+1})^{-E} \pmod m$, так що у накопичувач N_j правого півблока наступного циклу заноситься число $R_j \equiv L_{j-1} \cdot K_{j+1}^* \pmod m$, тобто

$R_j \equiv f^*(L_{j-1}, K_{j+1}) \equiv L_{j-1} \cdot (K_{j+1})^{-E} \pmod m$, а значення накопичувача правого півблока R_{j-1} сумують за модулем m зі значенням виходу циклової функції перетворення $g(L_{j-1}, K_{j+1})$ і результат заносять в накопичувач N_j лівого півблока наступного циклу, тобто $L_j = R_{j-1} + g(L_{j-1}, K_{j+1}) \pmod m$, а в режимі використання лівілки обчислюють піднесення значення L_{j-1} накопичувача N_{j-1} лівого півблока до степеня D за модулем m , тобто обчислюють $X_{j-1} \equiv (L_{j-1})^D \pmod m$, і потім з отриманого числа обчислюють корінь степеня D за модулем m , і в накопичувач N_j правого півблока заносять число $R_j \equiv \sqrt[D]{X_{j-1}}$, тобто циклова функція перетворення має вигляд $h(L_{j-1}, L(m)) \equiv \sqrt[D]{X_{j-1}} \pmod m$, 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_j лівого півблока наступного циклу, тобто $L_j \equiv R_{j-1} + h(L_{j-1}, L(m)) \pmod m$, де $m = pq$ - модуль перетворення, котрий є добутком двох простих чисел p і q , $L(m)$ - узагальнена функція Ейлера числа m , показники степенів E і D пов'язані умовою $ED \equiv 0 \pmod L(m)$

Винахід відноситься до галузі обчислювальної техніки, де використовуються блочні шифри, такі як, наприклад, стандарт шифрування даних DES та інші симетричні алгоритми-шифрування

Відомий спосіб шифрування даних, такий як

ГОСТ 28147-89, що використовується у режимах простої заміни, гамування з зворотним зв'язком по виходу та інших. При цьому способі інформацію розбивають на 64-розрядні блоки T_0 , зашифрування котрих включає в себе 32 цикли ($j = 1, 2, \dots, 32$)

(19) UA (11) 50199 (13) A

У ключовий запам'ятовуючий пристрій (КЗП) вводять 256 біт ключа K в вигляді восьми 32-ох розрядних підключів (K_0, K_1, \dots, K_7). Кожний блок бітів, наприклад, у режимі простої заміни, розбивають на ліві, або старші біти і праві, або молодші біти, які вводять відповідно у накопичувачі N_1 і N_2 . Біти з виходу накопичувача N_2 разом з 32 розрядним підключем K_0 , зчитаним з КЗП проходять циклове перетворення, в ході якого виконується їх сумування за модулем 2^{32} і результат сумування подається на блок підстановок. Далі виконують детермінований циклічний зсув вихідної послідовності бітів за допомогою регістра зсуву, результат підсумовують за модулем 2 з змістом накопичувача N_1 і записують у накопичувач N_2 , а старе значення N_2 переписують у накопичувач N_1 . Перший цикл завершений. В другому циклі використовують нове значення N_2 і з КЗП зчитують заповнення - підключ K_1 , у третьому циклі - підключ K_2 і т.д. Так продовжується 24 цикли. В останніх восьми циклах розглянута процедура повторюється як і раніше, тільки порядок зчитування підключів з КЗП зворотний K_7, K_6, \dots, K_0 .

Найбільш близьким по сукупності ознак до заявленого є спосіб шифрування даних для систем обробки в ЕОМ, який полягає в тому, що послідовність двійкових символів відкритого тексту розбивається на n бітні блоки, кожен з яких розбивають на правий та лівий півблоки по $n/2$ біти, які розміщують у відповідних накопичувачах півблоків, зашифрування котрих включає і, наприклад, 1 цикл. При цьому дані з виходу накопичувача правого півблока і дані відповідного циклового підключу кожного циклу надходять на вхід циклової функції перетворення, вихідні дані котрої підсумовують у відповідному побітному суматорі за модулем 2 з даними лівого півблока, дані накопичувача правого півблока теперішнього циклу переносять у накопичувач лівого півблока чергового циклу, а результатом підсумовування заповнюють накопичувач правого півблока чергового циклу (див. заявку на патент України №2001032062 від 28.03.2001).

Однак, ці шифри не мають можливості санкціонованого доступу до зашифрованої інформації при втраті ключової інформації.

В основу винаходу поставлена задача створення такого способу шифрування даних для систем обробки в ЕОМ, при котрому санкціонований користувач ЕОМ при втраті ключової інформації має можливість розшифрувати зашифровану інформацію, що призводить до поширення функціональних можливостей симетричних способів шифрування.

Такий технічний результат може бути досягнутий за способом шифрування даних для систем обробки в ЕОМ, який укладається у тому, що послідовність двійкових символів відкритого тексту розбивають на n бітні блоки, кожен з яких розбивають у свою чергу на правий R_0 та лівий L_0 півблоки по $n/2$ біти, які розміщують у відповідних накопичувачах, зашифрування котрих включає в себе і циклів, при цьому дані R_{i-1} з виходу накопичувача N_1 правого півблоку і значення відповідного підключу K_i кожного циклу надходять на вхід циклової функції перетворення $f(R_{i-1}, K_i)$, згідно з

винаходом, вихідне значення даних правого півблоку R_{i-1} також використовується для обчислення різниці за модулем m зі значенням даних лівого півблоку L_{i-1} і цю різницю заносять у накопичувач правого півблоку наступного циклу, так що $R_i = R_{i-1} - L_{i-1} \pmod{m}$, вихідні дані циклової функції заносять у накопичувач лівого півблоку, тобто $L_i = f(R_{i-1}, K_i)$, при цьому в якості циклової функції перетворення використовують модульне множення значення R_{i-1} накопичувача N_1 правого півблоку на ключ зашифрування $K_i' = (K_i)^E \pmod{m}$, так що у накопичувач N_1 лівого півблоку наступного циклу заносять число $L_i = R_{i-1} * (K_i)^E \pmod{m}$, тобто $f(R_{i-1}, K_i) = R_{i-1} * (K_i)^E \pmod{m}$.

При розшифруванні, яке проводять в оберненому порядку по відношенню до зашифрування, у кожному циклі в основному режимі значення L_{i-1} накопичувача N_1 лівого півблоку подають на вхід циклової функції перетворення $g(L_{i-1}, K_{i+1})$, при цьому в якості циклової функції перетворення використовують модульне множення значення L_{i-1} накопичувача N_1 лівого півблоку на ключ розшифрування $K_{i+1}' = (K_{i+1})^E \pmod{m}$, так що у накопичувач N_1 правого півблоку наступного циклу заносять число $R_i = L_{i-1} * K_{i+1}' \pmod{m}$, тобто $R_i = f(L_{i-1}, K_{i+1}) = L_{i-1} * (K_{i+1})^E \pmod{m}$, а значення накопичувача правого півблоку R_{i-1} сумують за модулем m зі значенням виходу циклової функції перетворення $g(L_{i-1}, K_{i+1})$ результат заносять в накопичувач N_1 лівого півблоку наступного циклу, тобто $L_i = R_{i-1} + g(L_{i-1}, K_{i+1}) \pmod{m}$, а в режимі використання лазівки беруть іншу функцію циклового перетворення $h(L_{i-1}, L(m))$, а саме обчислюють піднесення значення L_{i-1} накопичувача N_1 лівого півблоку до степеня D за модулем m , тобто обчислюють $X_{i-1} = (L_{i-1})^D \pmod{m}$ і потім з отриманого числа обчислюють корінь степеня D за модулем m , і в накопичувач N_1 правого півблоку заносять число $R_i = \sqrt[D]{X_{i-1}}$,

тобто циклова функція перетворення має вигляд $h(L_{i-1}, L(m)) = \sqrt[D]{X_{i-1}} \pmod{m}$, а значення накопичувача правого півблоку R_{i-1} сумують за модулем m зі значенням виходу тепер вже циклової функції перетворення $h(L_{i-1}, L(m))$, і результат заносять в накопичувач N_1 лівого півблоку наступного циклу, тобто $L_i = R_{i-1} + h(L_{i-1}, L(m)) \pmod{m}$, де $m = pq$ - модуль перетворення, котрий є добутком двох простих чисел p і q , $L(m)$ - узагальнена функція Ейлера числа m (найменше спільне кратне функцій Ейлера простих співмножників числа m) показники степенів E і D пов'язані умовою $ED \equiv 0 \pmod{L(m)}$.

На фіг. 1 зображена схема процедури шифрування, на фіг. 2 - схема процедури розшифрування в основному режимі, на фіг. 3 - схема розшифрування в режимі використання лазівки.

Спосіб може бути здійснений таким чином. Модуль m , за котрим ведуться обчислення у кожному циклі, вибирається з умови $2^{n/2} < m < 2^{n/2+1}$, так що накопичувачі всіх циклів окрім першого мають додатний бітовий розряд (вхідний $n/2$ бітний півблок відкритого тексту завжди не перевищує значення m , в той час коли в інших циклах при виконанні операцій за модулем m можуть бути

отримані числа, що перевищують $2^{n/2}$. Далі виконуються однотипні операції зашифрування (Фіг 1), котрі повторюються l разів (l циклів), у результаті чого формується зашифроване повідомлення. На кожний n бітний блок відкритого тексту процедура формує зашифрований блок, довжина якого є $n + 2$.

Процедуру дешифрування в математичному сенсі є оберненою до процедури зашифрування.

Працездатність запропонованого способу підтверджується наступними математичними співвідношеннями. Шифрування у кожному циклі виконується за формулами

$$L_i = R_{i-1} * (K_i)^E \pmod{m}, R_i = R_{i-1} - L_{i-1} \pmod{m}$$

Зашифроване повідомлення, таким чином, складається з двох півблоків з $n/2 + 1$ бітів кожний, причому, відповідно до першого порівняння, якщо з лівого пів блоку (виходу) мати можливість випусти значення R_{i-1} попереднього циклу, то з останнього порівняння сумуванням значення правого півблоку R_i (виходу) з випущеним значенням правого півблоку попереднього циклу можна отримати значення лівого півблоку попереднього циклу і т.д., тобто виконуючи процедуру обернену до процедури шифрування можна прийти до вихідного повідомлення. Залишається упевнитись, що зі значення L_i півблоку даного циклу можна випустити значення правого півблоку R_{i-1} попереднього циклу, який був при шифруванні. Дійсно це так бо при дешифруванні обчислюється $R_i^* = L_{i-1} - K_i^E \pmod{m}$. З урахуванням того, що номери циклів при шифруванні і дешифруванні пов'язані умовою $j = l - i + 1$, причому для ключів шифрування та дешифрування виконується умова $K_i^E = K_{l-i+1}$, маємо

$$R_i^* = L_{i-1} * (K_{l-i+1})^E = R_{i-1} * (K_{l-i+1})^E * (K_{l-i+1})^E = R_{i-1} \pmod{m},$$

тобто приходимо до тексту R_{i-1} , який був при шифруванні на вході функції циклового перетворення попереднього циклу. Але ж тоді при сумуванні цього результату зі значенням накопичувача лівого півблоку отримаємо

$$R_{i-1}^* = L_{i-1} \pmod{m}$$

В режимі застосування лазівки (фіг 3) на кожному циклі виконується операція

$$X_{j-1} = (L_j)^D = (R_{j-1}^* * K_j^E)^D = (R_{j-1}^*)^D * (K_j)^{ED}$$

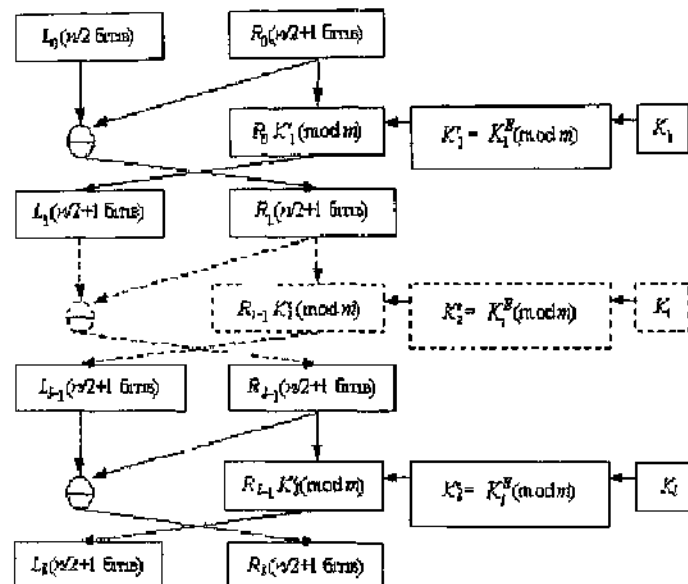
З урахуванням того, що числа E і D підкоряються умові $ED = 0 \pmod{L(m)}$, маємо очевидний результат $X_{j-1} = (R_{j-1}^*)^D \pmod{m}$ і тому що в цьому випадку $(K_j)^{ED} = 1 \pmod{m}$. Але ж тоді на виході циклової функції $h(L_{j-1}, L(m))$ отримуємо результат

$$R_j^* = \sqrt[D]{(R_{j-1}^*)^D} = R_{j-1} \pmod{m}$$

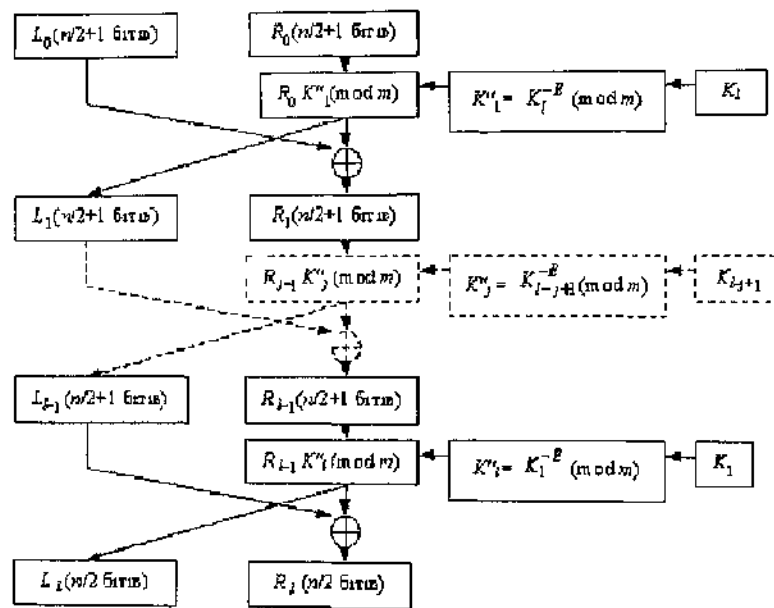
тобто і в цьому разі незалежно від ключів шифрування і дешифрування ми отримуємо текст R_{j-1} , який був при шифруванні на вході функції циклового перетворення попереднього циклу.

Лазівка повинна не зменшувати стійкості шифру. Тому параметри лазівки p, q, E і D виступають секретними (установчими) параметрами шифру.

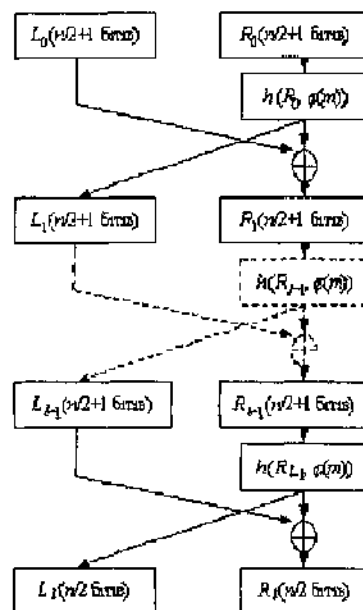
Помітимо, що операція обчислення кореня неоднозначна. Наприклад, при $D = 2$ будемо мати чотири кореня. Відповідно кожний цикл розшифрування приводить до чотирьох варіантів розшифрованих блоків, а для l циклів число варіантів розшифрованих текстів становитиме 4^l (для $l = 4$ для знаходження дійсного відкритого блока необхідно буде переглянути 256 варіантів блоків).



Фіг 1



Фиг 2



Фиг 3

ДП «Український інститут промислової власності» (Украпатент)
вул. Сим'ї Хохлових, 15, м. Київ, 04119, Україна
(044) 456 – 20 – 90

ТОВ «Міжнародний науковий комітет»
вул. Артема, 77, м. Київ, 04050, Україна
(044) 216 – 32 – 71