УКРАЇНА

(19) UA (11) 42957 (13) U

(51) МПК (2009)
H04L 9/00

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ШИФРУВАННЯ ДАНИХ

(21) u200902326
(22) 16.03.2009
(24) 27.07.2009
(46) 27.07.2009, Бюл.№ 14, 2009 р.
(72) АВРАМЕНКО ВІКТОР ВАСИЛЬОВИЧ, ЗАБОЛОТНИЙ МИХАЙЛО ІГОРОВИЧ
(73) СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
(57) Спосіб шифрування даних, який полягає в тому, що шифрування здійснюють за допомогою математичних функцій та ключів, що мають випадкову складову k, який **відрізняється** тим, що як ключі використовують m еталонних функцій $f_i(\tau(t)), i=\overline{1...m}$, $f_i(\tau(t))\in R$ та функцію $\tau(t)\in R$, що слугує для генерації аргументів для еталонних функцій $f_i(\tau(t))$, при цьому шифрування здійснюють за допомогою функції суми, яка має вигляд:

$$f_0(t)=\sum_{i=1}^{m} a_i k_i f_i(\tau(t)),$$

де: $f_i(\tau(t)), i=\overline{1...m}$ - m еталонних ключових функцій $f_i(\tau(t))\in R$, $\tau(t)\in R$ - функція генерації аргументів, $t\in R$, a_i - елементи масиву a, який є бінарним кодом повідомлення, представленого у вигляді числа G, k_i - випадкові коефіцієнти, які генеруються під час шифрування повідомлення і невідомі ні відправнику, ні одержувачу, крім того, використовують розшифрування за допомогою функцій непропорційності, які мають вигляд:

$$F_{0i}(t)=@\, d^{(1)}_{f_i(\tau(t))} f_0(t)=\frac{f_0(t)}{f_i(\tau(t))}-\frac{f_0'(t)}{f_i'(\tau(t))},$$

де: $@\, d^{(1)}_{f_i(\tau(t))} f_0(t)$ - позначення непропорційності $f_0(t)$ по $f_i(\tau(t))$ по похідних першого порядку, $f_0(t)$ - функція, що являє собою зашифроване повідомлення, $f_i(\tau(t))$ - еталонна функція, $f_0'(t)$ - похідна від функції $f_0(t)$, $f_i'(\tau(t))$ - похідна від функції $f_i(\tau(t))$.

Корисна модель, що заявляється, відноситься до галузі електрозв'язку і обчислювальної техніки, та систем передачі інформації, а саме до криптографічних способів захисту інформації з використанням симетричного ключа.

В основному алгоритми криптографії з закритими ключами використовують функції перестановок та підстановок і не використовують математичні функції.

Тому в якості аналогу і найближчого аналогу розглядаються асиметричні криптосистеми.

Відомий спосіб шифрування даних, такий як криптосистема RSA, яка відноситься до асиметричних систем.

RSA використовує функцію зведення в ступінь, (див.: С.Коутинхо Введение в теорию чисел. Алгоритм RSA. Москва: Постмаркет, 2001. -с.18-21).

При цьому способі обираються два великих простих числа p і q. Ці числа тримаються в секреті, а публікується число N=p·q, яке називається модулем алгоритму. Крім того отримується шифруюча експонента E, що задовольняє умові

НОД(E,(p-1),(q-1))=1

Пара чисел, що доступна для усіх бажаючих, - це (N, E). Для вибору секретного ключа застосовується розширений алгоритм Евкліда до пари чисел E і (p-1)(q-1). Після чого отримуємо розшифровуючу експоненту d. Знайдена експонента задовольняє співвідношенню

$E\cdot d=1 (\mathrm{mod}(p-1)(q-1))$.

Секретним ключем є трійка (d, p, q).

Для зашифрування повідомлення його представляють у вигляді числа m, яке є менше модуля N алгоритму. Шифротекст C отримується з m за наступним правилом:

$C=m^E (\mathrm{mod}\ N)$.

Розшифрування повідомлення проводиться за наступною формулою:

$m=C^d (\mathrm{mod}\ N)$.

Недоліками цього способу є необхідність вибору ключів довжини не менше 1024-2048 бітів, що значно зменшує швидкість роботи алгоритму, та необхідність вибору двох великих простих чисел, що є досить громіздкою задачею.

(19) UA (11) 42957 (13) U

Найбільш близьким за сукупністю ознак до запропонованого є спосіб шифрування даних, що реалізується криптосистемою Ель-Гамаль, яка також використовує функції зведення в ступінь і має випадкове число k у якості складової частини ключа (див.: Н. Смарт Криптография. Техносфера, 2005. -с.200-203).

В цій системі використовуються параметри домену, які є відкриті для великого числа користувачів, і мають вигляд:

P - «велике ціле число», тобто число, що нараховує біля 1024 бітів, таке, що P-1 ділиться на друге, «середнє просте число» Q, що лежить недалеко від 2^{160}.

G - елемент мультиплікативної групи поля F_P^*, порядок якої ділиться на Q, причому

$G^{(P-1)/Q} (\mathrm{mod}\ P) \neq 1$.

Всі параметри домену, тобто P,Q,G, обираються таким чином, щоб елемент $Q^{(P-1)/Q}$ був утворюючою абелевою групою A порядку Q. Інформація про цю групу відкрита і використовується великим числом користувачів.

Після вибору параметрів домену визначають відкритий та секретний ключі. Секретним ключем може бути будь-яке натуральне число x, а відкритий ключ отримується за наступною формулою

$H=G^x (\mathrm{mod}\ P)$

Повідомлення в цій системі представляється ненульовим елементом поля $m \in F_P^*$. Для його шифрування виконуються наступні дії:

- генерується випадковий ефемерний ключ к,
- обчислюється $C_1=G^k$,
- знаходиться $C_2=m \cdot H^k$,

видається отриманий шифротекст в якості пари $C=(C_1, C_2)$.

Для кожного сеансу шифрування використовується свій короткочасний ключ.

Щоб розшифрувати пару даних $C=(C_1, C_2)$, виконуються наступні перетворення:

$$\frac{C_2}{C_1^x} = \frac{m \cdot H^k}{G^{xk}} = \frac{m \cdot G^{xk}}{G^{xk}} = m.$$

Недоліками цього способу також є те, що він базується тільки на множині простих чисел, що приводить до "великих" ключів, які використовуються для підвищення криптостійкості. А це породжує проблеми їх генерації та швидкості роботи алгоритму.

В основу корисної моделі поставлене завдання розробки способу шифрування даних, який дозволить відійти від використання множини простих чисел, складних для обчислення ключів, та для заданого фіксованого секретного ключа забезпечити перетворення вхідного тексту в шифртекст, структура якого не була б визначена на перед, що робить виявлення статистичних властивостей більш складним, завдяки чому підвищується стійкість криптоаналізу на основі підібраних вхідних текстів.

Поставлена задача вирішується тим, що шифрування здійснюють за допомогою математичних функцій та ключів, що мають випадкову складову k, згідно з корисною моделлю, як ключі використовують m еталонних функцій $f_i(\tau(t)), i = \overline{1..m}$, $f_i(\tau(t)) \in R$ та функцію $\tau(t) \in R$, що слугує для генерації аргументів для еталонних функцій $f_i(\tau(t))$, при цьому шифрування інформації здійснюються за допомогою функції суми, яка має вигляд:

$$f_0(t) = \sum_{i=1}^{m} a_i k_i f_i(\tau(t)), \text{ де}$$

$f_i(\tau(t)), i = \overline{1..m}$ - m еталонних ключових функцій $f_i(\tau(t)) \in R$, $\tau(t) \in R$ - функція генерації аргументів, $t \in R$, a_i - елементи масиву a, який є бінарним кодом повідомлення представленого у вигляді числа G, k_i - випадкові коефіцієнти, які генеруються під час шифрування повідомлення і невідомі ні відправнику, ні одержувачу, крім того, використовуються розшифрування за допомогою функцій непропорційності, які мають вигляд:

$$F_{0i}(t) = @ d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0'(t)}{f_i'(\tau(t))}, \text{ де}$$

$@ d^{(1)}_{f_i(\tau(t))} f_0(t)$ - позначення непропорційності $f_0(t)$ по $f_i(\tau(t))$ по похідних першого порядку, $f_0(t)$ - функція, що являє собою зашифроване повідомлення, $f_i(\tau(t))$ - еталонна функція, $f_0'(t)$ - похідна від функції $f_0(t)$, $f_i'(\tau(t))$ - похідна від функції $f_i(\tau(t))$.

Завдяки такому рішенню збільшується кількість можливих ключів, тим самим зростає стійкість системи при атаці методом підбору. Також шляхом використання разом з еталонними функціями випадкових коефіцієнтів, які генеруються під час шифрування випадковим чином, досягається те, що одне й те ж повідомлення, з однаковими ключами, кожного разу дає різну шифровку. І ще одна з задач, яка розв'язується за допомогою корисної моделі, це більш простий вибір ключів.

Спосіб здійснюється таким чином.

Для сеансу передачі даних як ключ обираються m еталонних функцій $f_i(\tau(t)), i = \overline{1..m}$, $f_i(\tau(t)) \in R$ та функція $\tau(t) \in R$, що слугує для генерації аргументів для еталонних функцій $f_i(\tau(t))$.

$t \in R$ і можуть обиратись будь-яким чином. Наприклад, як t може використовуватись позиція символу в повідомленні.

Для зашифрування повідомлення, його представляють у вигляді числа G, яке розкладають в m- розрядний бінарний код a. Повідомлення представляють у вигляді такого числа G, що його бінарний код місить більше ніж одну одиницю.

Шифртекст $f_0(t)$ отримується з a за наступним правилом

$$f_0(t) = \sum_{i=1}^{m} a_i k_i f_i(\tau(t)), \text{ де}$$

$f_i(\tau(t)), i = \overline{1..m}$ - m еталонних ключових функцій $f_i(\tau(t)) \in R$, що задовольняють заданим обмеженням:

1. Функція повинна належати до області дійсних чисел.

2. Функція повинна мати похідні до порядку m включно.

3. Функція і її похідна будь-якого порядку (у тому числі і m) не повинна бути константою.

4. Функція не повинна містити відрізків, на яких, при декількох контрольних обчисленнях, вона практично дорівнює константі (наприклад функція $x^{-\alpha}$ при великих значеннях x).

5. Набір функцій повинний бути підібраний таким чином, щоб не було ситуацій, у яких значення одної функції в одній і тій же точці буде дуже близьким до нуля у порівнянні зі значенням іншої функції, тобто кожна функція повинна вносити досить вагомий "внесок" у суму значень функцій, що відповідає зашифрованому повідомленню.

$\tau(t)\in R$ - функція генерації аргументів.

t - аргумент функції $\tau(t)$. Наприклад, як аргумент може виступати місцеположення символу в повідомленні.

a_i - елементи масиву a, який є бінарним кодом повідомлення G.

k_i - випадкові коефіцієнти, які генеруються під час шифрування повідомлення і невідомі а ні відправнику, а ні одержувачу.

Розшифрування виконується наступним чином.

Перебираються всі можливі з m - розрядних бінарних кодів повідомлень. В залежності від кількості одиниць в бінарному коді поточного можливого повідомлення визначається вид функції непропорційності.

Якщо в бінарному коді одна одиниця, то функція непропорційності має вигляд:

$$F_{0i}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0'(t)}{f_i'(\tau(t))}.$$

Якщо кількість одиниць дорівнює дві, то функція непропорційності має вигляд:

$$F_{0iji}(t) = @\, d^{(1)}_{fji(t)} f_{0i}(t) = \frac{f_{0i}(t)}{f_{ji}(t)} - \frac{f_{0i}'(t)}{f_{ji}'(t)},$$

де $F_{ji}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_j(\tau(t)) = \frac{f_j(\tau(t))}{f_i(\tau(t))} - \frac{f_j'(\tau(t))}{f_i'(\tau(t))}$.

Аналогічно формується вид функції непропорційності при більшій кількості одиниць в бінарному коді.

У випадку коли функція непропорційності дорівнює нулю, вважається, що повідомлення розшифровано, якщо функція непропорційності не дорівнює нулю, то продовжується перебирання бінарних кодів повідомлень.

Приклад роботи способу шифрування даних.

1. Вибір ключів сеансу:

$f_i(\tau(t)), i = \overline{1..m}$ - m функцій $f_i(\tau(t))\in R$ і задовольняють вказаним вище обмеженням на ключові функції.

$\tau(t)\in R$ - функція, що слугує для генерації аргументів для функцій $f_i(\tau(t))$ і також використовується як ключ.

$t\in R$. Наприклад як t може використовуватись місцеположення символу в тексті.

m - кількість функцій $f_i(\tau(t))$, обраних як ключ, одночасно є довжиною масиву a.

2. Шифрування.

Повідомлення представляється у вигляді числа G, яке розкладають в m - розрядний бінарний код a. Повідомлення представляють у вигляді такого числа G, що його бінарний код місить більше ніж одну одиницю. Це необхідно для підвищення кріпкостійкості.

Шифрування здійснюється за формулою:

$$f_0(t) = \sum_{i=1}^{m} a_i k_i f_i(\tau(t)) \qquad (1)$$

Генерування коефіцієнтів k_i за випадковим законом може виконуватися, наприклад, шляхом вимірювання імовірнісного фізичного процесу або вимірювання сигналу датчику шуму, у ролі якого часто використовуються спеціально сконструйовані електронні пристрої.

В іншому варіанті способу замість генератора випадкових чисел може бути використаний генератор псевдо випадкових чисел, на вхід якого подається випадково вибране число, отримуючи на виході необхідне псевдо випадкове число. Відомий ряд способів побудови генераторів псевдо випадкових чисел (див. наприклад B. Schneider, "Applied Cryptography", Second Edition, John Wiley & Sons, Inc., New York 1966, pp.416-418), які можуть бути використані в способі за корисною моделлю. Використання генератора псевдовипадкових чисел дозволяє реалізувати спосіб, який пропонується, програмним шляхом, беручи як початкове випадкове число, наприклад, значення інтервалу часу між натисненнями кнопки миші.

В результаті чого ми отримуємо шифровку $f_0(t)$.

Після цього перш, ніж передавати, повідомлення розшифровується і перевіряється, чи співпадає отриманий результат з незашифрованим текстом повідомлення. Якщо так, то зашифроване повідомлення відправляється одержувачу, якщо ні, то перед неправильно розшифрованими символами в початковому тексті треба поставити службові символи. Це робиться з метою змінити значення аргументу для еталонних функцій і виключити співпадіння значень їхніх сум. Після цього повторюється процедура шифрування з пункту 2.

При числовій реалізації алгоритму передаються функції $f_0(t)$ в дискретній формі. Тобто у вигляді масиву. Довжина масиву не повинна бути сталою. Змінюватися довжина масиву буде по заздалегідь обумовленому користувачами правилу.

Як приклад такої схеми можна визначити наступний алгоритм: довжина масиву визначається як $60 + \left(\sum_{i=1}^{m} a_i \cdot i\right) \bmod 30$.

3. Розшифрування

Після отримання зашифрованого повідомлення задача розшифрування зводиться до знаходження бінарного коду повідомлення $f_0(t)$. Для цього за допомогою функцій непропорційності визначається, які саме еталонні функцій складають зашифрований блок повідомлення. Оскільки кожна з еталонних функцій відповідає певному розряду двоїчного числа, то це дозволяє визначити бінарний код зашифрованого символу.

Для знаходження еталонних функцій які увійшли в суму $f_0(t)$ використовуємо нижче описаний алгоритм.

Послідовно перебираються всі можливі з m - розрядних бінарних кодів повідомлень. Робиться припущення, що елемент з вибірки і є розшифровкою зашифрованого повідомлення. Для перевірки цього твердження виконуються наступні дії.

В залежності від місцеположення одиниць у бінарному коді визначається з яких еталонних функцій складається поточний елемент вибірки. Наприклад, якщо бінарний код 10110000, то в цей елемент шифрується за допомогою еталонних функцій f_1, f_3, f_4.

В залежності від кількості одиниць і еталонних функцій визначається вид функції непропорційності.

Якщо в бінарному коді одна одиниця, то функція непропорційності має вигляд:

$$F_{0i}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0'(t)}{f_i'(\tau(t))}$$

Якщо кількість одиниць дорівнює дві, то функція непропорційності має вигляд:

$$F_{0iji}(t) = @\, d^{(1)}_{F_{ji}(t)} F_{0i}(t) = \frac{F_{0i}(t)}{F_{ji}(t)} - \frac{F_{0i}'(t)}{F_{ji}'(t)},$$

$$\text{де } F_{ji}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_j(\tau(t)) = \frac{f_j(\tau(t))}{f_i(\tau(t))} - \frac{f_j'(\tau(t))}{f_i'(\tau(t))}$$

Аналогічно формується вид функції непропорційності при більшій кількості одиниць в бінарному коді.

Обчислюємо функцію непропорційності.

Якщо функція непропорційності дорівнює нулю, то це означає, що зашифроване повідомлення складається з тих же еталонних функцій, що і бінарний код поточного повідомлення з вибірки. Таким чином, вважається, що припущення вірне.

Якщо функція непропорційності не дорівнює нулю, то виконується перехід до іншого елементу вибірки.

У якості прикладу розглядається алгоритм визначення виду функції непропорційності та розпізнавання еталонних функцій, що увійшли в $f_0(t)$ у випадку коли $\sum_{i=1}^{m} a_i = 3$, тобто кількість одиниць у бінарному коді дорівнює три. Кількість одиниць у бінарному коді дорівнює кількості еталонних функцій, що увійшли в суму $f_0(t)$. А і - це номер першої одиниці у бінарному коді, j - номер другої одиниці, q - третьої.

Етап перший. Знаходиться непропорційність функції $f_0(t)$ по одній будь-якій функції $f_i(t)$. Яка позначається через $F_{0i}(t)$.

$$F_{0i}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0'(t)}{f_i'(\tau(t))} \qquad (2)$$

Замість $f_0(t)$ в (2) підставляється його вираз в (1).

Отримаємо:

$$F_{0i}(t) = \sum_{j \neq i} k_j \left(\frac{f_j(\tau(t))}{f_i(\tau(t))} - \frac{f_j'(\tau(t))}{f_i'(\tau(t))} \right) = \sum_{j \neq i} k_j F_{ji}(t) \qquad (3),$$

де

$$F_{ji}(t) = @\, d^{(1)}_{f_i(\tau(t))} f_j(\tau(t)) \qquad (4)$$

Етап другий. Знаходиться непропорційність по похідній першого порядку функції $f_{0i}(t)$ по одній з будь-яких функцій $F_{ji}(t)$. Яка позначається через $F_{0iji}(t)$.

$$F_{0iji}(t) = @\, d^{(1)}_{F_{ji}(t)} F_{0i}(t) = \frac{F_{0i}(t)}{F_{ji}(t)} - \frac{F_{0i}'(t)}{F_{ji}'(t)} \qquad (5)$$

З огляду на формулу (3)

$$F_{0iji}(t) = \sum_{q \neq j} k_q F_{qiji}(t) \qquad (6),$$

де

$$F_{qiji}(t) = @\, d^{(1)}_{F_{ji}(t)} F_{qi}(t) \qquad (7).$$

Етап третій. Знаходиться непропорційність по похідній першого порядку функції $F_{0iji}(t)$ по одній з будь-яких функцій $F_{qiji}(t)$ з (7). Яка позначається через $F_{0ijiqiji}(t)$.

$$F_{0ijiqiji}(t) = @\, d^{(1)}_{F_{qiji}(t)} F_{0iji}(t) \qquad (8).$$

Якщо функція непропорційності (8) дорівнює нулю, то вважається, що зашифроване повідомлення при розшифруванні дорівнює поточному елементу з вибірки можливих повідомлень.

За аналогічною схемою розшифровуються інші можливі повідомлення коли $\sum_{i=1}^{m} a_i \neq 3$. Кількість етапів обчислення відповідає $\sum_{i=1}^{m} a_i$.

Як було сказано вище, індекси при обчисленні функцій непропорційності залежать від положення одиниці в бінарному коді. Наприклад, бінарний код можливого повідомлення з вибірки має вигляд 11100000. Відповідний набір індексів має вигляд ijqklmnp.

Тоді i=1, j=2, q=3, k=4, l=5, m=6, n=7, p=8.

При числовій реалізації алгоритму отримуються функції, що відповідають зашифрованому повідомленню, в дискретній формі. Тобто у вигляді масиву. Довжина масиву обчислюється за тим же правилом, що і при зашифруванні. Після розшифрування виключаємо з розшифрованого тексту службові символи.

Комп'ютерна верстка Н. Лисенко 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