2 Забезпечення комп'ютерної безпеки в інформаційних системах

Анатолій Кочубінський, Володимир Синявський, Олександр Шаталов
Інститут кібернетики імені В. М. Глушкова НАН України
УДК 002:651.928(083.73)

АЛГОРИТМ АСИМЕТРИЧНОГО ШИФРУВАННЯ, ЗАСНОВАНИЙ НА ЕЛІПТИЧНИХ КРИВИХ

Анотація: **Запропоновано алгоритм асиметричного шифрування даних, що ґрунтується на криптографічному перетворенні, визначеному національним стандартом України ДСТУ 4145-2002. Цей алгоритм призначено для направленого шифрування невеликих за обсягом даних, головним чином, ключів та інших таємних параметрів криптографічних перетворень в системах розподілу ключової інформації в незахищених каналах зв'язку.**
Summary: **An algorithm of the asymmetric encryption is presented, that is based on the cryptographic transformation defined by the national standard of Ukraine DSTU 4145-2002. This algorithm is intended for public key encryption of small information blocks, mainly, keys and other secret parameters of cryptographic transformations in key distribution systems.**
Ключові слова: **Асиметричне шифрування, еліптичні криві.**

Вступ

Наразі в України як ДСТУ існує усього один криптографічний алгоритм власної розробки. Це алгоритм електронного цифрового підпису ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння». Авторами цього алгоритму є вчені Інституту кібернетики імені В. М. Глушкова НАН України.

Натомість сучасні інформаційні технології часто вимагають створення структур типу цифрових конвертів.

На цей час не існує нормативно затвердженого алгоритм асиметричного шифрування власної розробки, але криптографічне перетворення, визначене в ДСТУ 4145-2002 дає можливість розробити такий алгоритм, що матиме високу стійкість і достатню швидкодію. Такий алгоритм розроблено і саме він використовується як складова частина створення цифрового конверту. Стійкість цього алгоритму перевершує стійкість алгоритму ДСТУГОСТ 28147:2009 і тому він забезпечує адекватну криптографічну стійкість цифрового конверту в цілому. Цей алгоритм пройшов широку апробацію в прикладних розробках і має позитивні відгуки.

В даній роботі запропоновано алгоритм асиметричного шифрування даних, що ґрунтується на криптографічному перетворенні, визначеному національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» [1]. Цей алгоритм призначено для направленого шифрування невеликих за обсягом даних, головним чином, ключів та інших таємних параметрів криптографічних перетворень в системах розподілу ключової інформації в незахищених каналах зв'язку і системах управління доступом до ключових даних і розподілу повноважень користувачів в таких системах.

I Терміни, визначення та позначення

В роботі використовуються терміни та визначення понять з розділу 3 [1] а також наступні.

Параметри алгоритму асиметричного шифрування, що є загальними для довільного числа користувачів алгоритму. До загальних параметрів алгоритму асиметричного шифрування належать:

- параметри основного поля $GF\left(2^m\right)$: степінь розширення m і примітивний многочлен $f(t)$ (тричлен, п'ятичлен), що визначає поліноміальний базис;
- еліптична крива виду

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in GF\left(2^m\right), B \neq 0, A \in \{0,1\}$;

- базова точка еліптичної кривої P;
- функція гешування згідно до 6.2 ДСТУ 4145;

- порядок базової точки *n*.

Загальні параметри алгоритму задаються відповідно до цієї статті та розділу 7 [1], а зображуються відповідно до розділу 5 [1].

Ключ зашифрування - є індивідуальним параметром алгоритму асиметричного шифрування. Вважається, що в процесі зашифрування є доступ до автентичної копії ключа зашифрування.

Q - точка еліптичної кривої.

Ключ розшифрування - це індивідуальний параметр алгоритму асиметричного шифрування, що обчислюється згідно з процедурою, наведеною нижче.

Разовий ключ зашифрування - ціле число e, обчислене згідно з цією роботою.

Криптограма**Ошибка! Ошибка связи.**пара елементів основного поля (f_r, f_s).

Автентифікатор повідомлення T - двійковий рядок $\tilde{h}$ (T).

В роботі використовуються позначення з розділу 4 [1], а також позначення наведені в таблиці 1.

Таблиця 1

d	ключ розшифрування, ціле число, $0 < d < n$
Q	ключ зашифрування, точка еліптичної кривої
e	разовий ключ зашифрування, ціле число, $0 < e < n$
(f_r, f_s)	криптограма, $f_r, f_s \in GF(2^m)$
$\tilde{h}$ (T)	автентифікатор повідомлення *T*, двійковий рядок, $L(\tilde{h}(T)) = 64$

Математичні об'єкти, що використовуються в цьому алгоритмі, зображуються згідно з розділом 5 [1]. Крім того, використовуються такі формати даних.

Криптограма зображується як пара елементів основного поля (f_r, f_s). Елементи основного поля f_r та f_s зображуються згідно з 5.3 [1].

Автентифікатор $\tilde{h}$ (T) повідомлення T зображується як двійковий рядок, довжина якого дорівнює 64: $\tilde{h}(T) = (\tilde{h}_{63}, \ldots, \tilde{h}_0)$.

II Обчислювальні алгоритми

В алгоритмі асиметричного шифрування використовуються обчислювальні алгоритми, визначені в розділі 6 [1].

Нижче встановлюється алгоритм обчислення автентифікатора повідомлення.

Вхідні дані алгоритму: повідомлення *T*, $L_T > 0$, функція гешування *H* згідно з 6.2 [1].

Результат виконання алгоритму: автентифікатор повідомлення $\tilde{h}(T)$.

Алгоритм обчислення автентифікатора:

1. Обчислюється геш-код повідомлення $H(T) = (h_{L_H - 1}, \ldots, h_0)$;
2. Приймається $\tilde{h}_i = h_i$ для $i = 0, \ldots, 63$.

Двійковий рядок $\tilde{h}(T) = (\tilde{h}_{63}, \ldots, \tilde{h}_0)$ є зображення автентифікатора повідомлення *T*.

Далі встановлюємо алгоритм форматування повідомлення *T*, тобто алгоритм перетворення оригінального повідомлення *T* на форматоване повідомлення $\tilde{T}$, до якого потім застосовується криптографічне перетворення.

Вхідні дані: повідомлення $T = (T_{L_T - 1}, \cdots, T_0)$, довжина якого L_T кратна 8 та задовольняє нерівність $0 < L_T < m - 72$.

Результат виконання алгоритму: форматоване повідомлення $\widetilde{T} = \left(\widetilde{T}_{L_{\widetilde{T}}-1}, \ldots, \widetilde{T}_0\right)$, довжина якого дорівнює $L_{\widetilde{T}} = L_T + 8$.

Алгоритм форматування повідомлення:

1. Приймається $l = {L_T}/{8} = \left(l_{L(l)-1}, \ldots, l_0\right)$;
2. Приймається $\widetilde{T}_i = l_i$ для $i = 0, \ldots, L(l) - 1$;
3. Якщо $L(l) < 8$, то приймається $\widetilde{T}_i = 0$ для $i = L(l), \ldots, 7$;
4. Приймається $\widetilde{T}_{i+8} = T_i$ для $i = 0, \ldots, L_T - 1$.

Двійковий рядок $\widetilde{T}$ зображує форматоване повідомлення.

III Обчислення загальних параметрів алгоритму асиметричного шифрування

Основне поле обирається згідно з підрозділом 7.1 [1]. В алгоритмі асиметричного шифрування використовуються виключно основні поля, що визначаються поліноміальним базисом. Крім основних полів, наведених в таблиці 1 розділу 7.1 [1], в цьому алгоритмі можна використовувати поля, наведені в табл. 2.

Таблиця 2

№ п/п	Степінь поля *m*	Рекомендований примітивний многочлен
1	571	$x^{571}+x^{10}+x^5+x^2+1$
2	701	$x^{701}+x^{16}+x^4+x^2+1$

Еліптична крива обирається згідно з 7.2 [1]. Базова точка обчислюється згідно з 7.3 [1]. Перевіряння правильності загальних параметрів алгоритму асиметричного шифрування виконується згідно з розділом 8 [1]. Крім рекомендованих еліптичних кривих, наведених в таблиці Г.1 додатку Г до [1], дозволяється використовувати еліптичні криві, наведені в таблиці 3.

Таблиця 3

№ п/п	*m*	Еліптична крива
1	571	*A*=0 *B*=1 *n*=200000000000000000000000000000000000000000000000000000000000000000000131850E1F19A63E4B391A8DB917F4138B630D84BE5D639381E91DEB45CFE778F637C1001
2	701	*A*=1 *B*=1 *n*=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAD5CAB03B27B328085FC98875979E92940BD75F057C949D183ED24984CCCC47EFD300B7412AC4F44F067627B

IV Обчислення ключів алгоритму асиметричного шифрування

В цьому розділі встановлюється порядок обчислення ключа розшифрування *d* та ключа зашифрування *Q* алгоритму асиметричного шифрування.

Ключ розшифрування *d* обчислюється наступним чином.

1. Обчислюється випадкове ціле число *d* згідно з підрозділом 6.3 ДСТУ 4145;
2. Якщо $d \neq 0$, то *d* є ключ розшифрування, інакше переходять до шагу 1.

Умови обчислення, використання та зберігання ключа розшифрування повинні виключати несанкціонований доступ до нього, його частин та проміжних даних, які використовувалися в процесі обчислення ключа розшифрування.

Ключ зашифрування *Q* обчислюється як точка еліптичної кривої $Q = -dP$, де *P*– базова точка еліптичної кривої, а *d* – ключ розшифрування.

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (28), 2014 р.

Умови зберігання ключа зашифрування повинні виключати модифікацію або підміну цього ключа. Припускається зберігання та передача ключа зашифрування в стисненому вигляді. Стиснення ключа виконується згідно з 6.9 [1], відновлення ключа виконується згідно з 6.10 [1].

V Перевіряння правильності ключів асиметричного шифрування

Правильність ключів асиметричного шифрування перевіряється згідно з розділом 10 [1], при цьому ключу зашифрування відповідає відкритий ключ цифрового підпису, а ключу розшифрування – особистий ключ цифрового підпису.

VI Обчислення разового ключа зашифрування

Разовий ключ зашифрування *e* обчислюється наступним чином.

1. Обчислюється випадкове ціле число *e* згідно з підрозділом 6.3 [1];
2. Якщо $e \neq 0$, то *e* є разовим ключем зашифрування, інакше переходять до шагу 1.

Умови обчислення та використання разового ключа зашифрування повинні виключати несанкціонований доступ до нього, його частин та проміжних даних, які використовувалися в процесі обчислення разового ключа зашифрування.

VII Зашифрування повідомлення

Цей розділ встановлює алгоритм зашифрування повідомлення *T*.

Вхідні дані:

- загальні параметри алгоритму асиметричного шифрування;
- ключ зашифрування *Q*;
- повідомлення *T*;
- функція гешування *H* згідно з 6.2 ДСТУ 4145;

Результат виконання алгоритму: криптограма (f_r, f_s).

Алгоритм асиметричного зашифрування:

1. Перевіряють виконання нерівностей $0 < L_T < m - 72$. Якщо не виконується перша нерівність, то видають повідомлення «Немає даних для зашифрування» і виконання алгоритму припиняється. Якщо не виконується друга нерівність, то видають повідомлення «повідомлення завелике» і виконання алгоритму припиняється.
2. Перевіряють правильність загальних параметрів алгоритму асиметричного шифрування згідно з розділом III. Якщо загальні параметри обчислено неправильно, то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених 8.1 – 8.3 [1].
3. Перевіряють правильність ключа зашифрування згідно з розділом V цього документу. Якщо ключ зашифрування неправильний, то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених 10.1 [1].
4. За повідомленням *T* обчислюють форматоване повідомлення $\widetilde{T}$ згідно з розділом II.
5. Обчислюють автентифікатор $\widetilde{h}(\widetilde{T})$ форматованого повідомлення $\widetilde{T}$ згідно з II.
6. Обчислюють елемент f_T основного поля наступним чином:

1. Приймають $f_{T,i} = \widetilde{T}_i$ для $i = 0, \ldots, L_{\widetilde{T}} - 1$;
2. Приймають $f_{T,i+L_{\widetilde{T}}} = \widetilde{h}_i$ для $i = 0, \ldots, 63$.
3. Приймають $f_{T,j} = 0 \quad для \quad j = L_{\widetilde{T}} + 64, \ldots, m$

7. Обчислюють разовий ключ зашифрування *e* згідно з розділом 10 цього документу.
8. Обчислюють точку еліптичної кривої *R*=-*eP*. Стискають цю точку в елемент основного поля f_r згідно з 6.9 [1].
9. Обчислюють точку еліптичної кривої $R' = eQ$. Нехай f_e – *x*-координата цієї точки R'.
10. Обчислюють елемент основного поля $f_s = f_T f_e$.
11. Пара елементів основного поля (f_r, f_s) утворює криптограму.

VIII Розшифрування криптограми

Цей розділ встановлює алгоритм розшифрування криптограми, обчисленої згідно з розділом VII.

Вхідні дані алгоритму:

- загальні параметри алгоритму асиметричного шифрування;
- ключ розшифрування *d*;
- криптограма (f_r, f_s);
- функція гешування *H* згідно з 6.2 [1];

Результат виконання алгоритму: прийняте повідомлення T' та ознака правильності розшифрування.

Алгоритм розшифрування криптограми.

1. Перевіряють правильність загальних параметрів алгоритму асиметричного шифрування згідно з розділом III. Якщо загальні параметри обчислено неправильно, то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених 8.1 – 8.3 [1].

2. Перевіряють правильність ключа розшифрування згідно з розділом V. Якщо ключ розшифрування неправильний, то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених 10.2 [1].

3. Якщо хоча б одна складова частина криптограми не належить до основного поля, то виконання алгоритму припиняється.

4. Якщо $f_r = 0$ або $f_s = 0$, то виконання алгоритму припиняється.

5. Відновлюють точку еліптичної кривої *R* з елементу основного поля f_r згідно з 6.10 [1].

6. Обчислюють точку еліптичної кривої $R' = dR$. Нехай f_d – *x*-координата цієї точки R'.

7. Обчислюють елемент основного поля $f_T = f_s f_d^{-1}$.

8. Обчислюють прийняте повідомлення $\widetilde{T}'$ наступним чином.

– Приймають $l_i = f_{T,i}$ для $i = 0, \ldots, 7$. Цьому двійковому рядку відповідає ціле число l'. Приймають $l' \leftarrow 8l'$.

– Приймають $\widetilde{T}_i' = l_i$ для $i = 0, \ldots, 7$;

– Приймають $\widetilde{T}_i' = f_{T,i}$ для $i = 8, \ldots, 8 + l' - 1$.

9. Обчислюють автентифікатор $\widetilde{h}(\widetilde{T}') = (\widetilde{h}_{63}', \ldots, \widetilde{h}_0')$ повідомлення $\widetilde{T}'$.

10. Обчислюють повідомлення T' наступним чином: приймають $T_i' = \widetilde{T}'_{i+8}$ для $i = 0, \ldots, l' - 1$.

11. Обчислюють прийнятий автентифікатор $\widetilde{h}'' = (\widetilde{h}_{63}'', \ldots, h_0'')$ наступним чином: приймають $\widetilde{h}_i'' = f_{T,i+8+l'}$ для $i = 0, \ldots, 63$.

12. Якщо $\widetilde{h}_i'' = \widetilde{h}_i'$ для $i = 0, \ldots, 63$, то криптограму розшифровано правильно, інакше криптограму розшифровано неправильно.

IX Доказ коректності алгоритму

Якщо криптограма (f_r, f_s) прийнята без спотворень, то точка еліптичної кривої *R* буде правильно відновлена із стиснутого представлення цієї точки. Тому $R' = dR = -deP = eQ$. Таким чином, *x*-координата точки R' дорівнює f_e. Друга частина криптограми f_s по побудові дорівнює $f_T f_e$. Тому елемент поля f_T, містить передане повідомлення і його автентифікатор та обчислюється за формулою $f_T = f_s f_e^{-1}$. Прийняте повідомлення і автентифікатор однозначно відновлюються з елементу поля f_T і при зробленому припущенні будуть дорівнювати відповідно переданому повідомленню і переданому автентифікатору. Очевидно, переданий і обчислений автентифікатори при зробленому припущенні будуть збігатися.

X Стійкість алгоритму

Стійкість алгоритму асиметричного шифрування визначається стійкістю криптографічного перетворення, визначеного в ДСТУ 4145-2002 . Нині стійкість цього перетворення дорівнює $2^{m/2}$, де m - степінь розширення основного поля. Нехай складність перебору криптографічного параметра, який шифрується за допомогою даного алгоритму, дорівнює 2^t, $t>0$. Тоді алгоритм асиметричного шифрування забезпечить адекватний захист шифрованому параметру тільки у тому випадку, якщо виконується нерівність $m \geq 2t$.

Розглянемо два практично важливих застосування цього алгоритму.

а) Шифрування сесійних ключів алгоритму ДСТУ ГОСТ 28147:2009. В цьому випадку t=256 і $m \geq 512$.

б) Шифрування довгострокових ключових елементів алгоритму ДСТУ ГОСТ 28147:2009. В цьому випадку число можливих довгострокових ключових елементів дорівнює

$$16!\cdot(16!-1)\cdots(16!-7) \approx (16!)^8 = 3{,}67\cdot 10^{106} \approx 2^{353},$$

тобто t=353 і $m \geq 706$.

Якщо нерівність $m \geq 2t$ не виконана, то стійкість криптографічних алгоритмів, що використовують криптографічні параметри, передані за допомогою алгоритму асиметричного шифрування визначатиметься не стійкістю цих криптографічних алгоритмів, а стійкістю алгоритму асиметричного шифрування. Практично у більшості випадків для шифрування сесійних ключів і довгострокових ключових елементів алгоритму ДСТУ ГОСТ 28147 : 2009 можна використовувати основне поле m=571, в особливо важливих випадках слід використовувати основне поле m=701.

XI Автентифікація повідомлення

Оскільки повідомлення, що передаються, у більшості випадків будуть блоками випадкових даних, то потрібен спосіб визначення правильності розшифрування даних. З цією метою разом із повідомленням передається 8 байтів геш-коду, обчисленого, наприклад, за допомогою алгоритму ГОСТ 34.311-95. Ймовірність випадкового збігу геш-коду спотвореного повідомлення з істинним геш-кодом дорівнює $2^{-64} \approx 10^{-18}$. Оскільки в цьому застосуванні геш-код не несе криптографічного навантаження, більше того, він шифрується разом з повідомленням, то 8 байтів геш-коду цілком достатньо для автентифікації повідомлення, що передається.

Список використаної літератури: ***1.*** *ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння»// К.: Держстандарт України, 2003. 94 с.*

Людмила Ковальчук, Наталія Кучинська, Віктор Бездітний*
*ІСЗЗІ НТУУ "КПІ", *ФТІ НТУУ "КПІ"*

УДК 621.391:519.2:519.7

ПОБУДОВА ВЕРХНІХ ОЦІНОК СЕРЕДНІХ ІМОВІРНОСТЕЙ ЦІЛОЧИСЕЛЬНИХ ДИФЕРЕНЦІАЛІВ КОМПОЗИЦІЇ МОДУЛЬНОГО КЛЮЧОВОГО СУМАТОРА, БЛОКА ПІДСТАНОВКИ ТА ЛІНІЙНОГО ОПЕРАТОРА, ЩО МАЄ БЛОКОВУ СТРУКТУРУ

Анотація: **Отримані верхні оцінки середніх імовірностей цілочисельних диференціалів для раундових функцій у випадку нетривіального блока підстановки та лінійного оператора, що має блокову структуру.**

Summary: **The upper bounds are obtained of the integer differentials average probabilities for round functions in the case of a nontrivial block permutations and a block structure linear operator.**

Ключові слова: **Різницевий криптоаналіз, диференціальний криптоаналіз, блокові шифри, раундові функції, s-блоки.**

Вступ

В представленій роботі вперше отримано верхні оцінки середніх імовірностей цілочисельних