УДК 004.056.55

АНАЛІЗ КРИПТОСТІЙКОСТІ ЕЛЕМЕНТІВ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Кожухівський А. Д., *д.т.н., професор кафедри інформатики та інформаційної безпеки,*
Сагун А. В., *к.т.н., доцент кафедри інформатики та інформаційної безпеки,*
Кожухівська О. А., *к.т.н., ст. викладач кафедри інформатики та інформаційної безпеки,*
Снісаренко О. Ю., *магістрант кафедри інформатики та інформаційної безпеки*
Степанець Ю. В., *магістрант кафедри інформатики та інформаційної безпеки*
Черкаський державний технологічний університет
бульвар Шевченка, 460, Черкаси, 18006,
andrejdk@mail.ru

Анотація. *Розглянуті основні задачі криптоаналізу ЕЦП. Наведено оцінки ймовірності зламу геш-функції методами зламостійкості до зіткнень та парадоксу "днів народження". Побудовано і проаналізовано графічні залежності оцінки ймовірності цих методів.*

Ключові слова: *електронний цифровий підпис, геш-функція, еліптична крива.*

THE ANALYSIS OF CRYPTOGRAPHIC SECURITY OF THE ELEMENTS OF ELECTRONIC DIGITAL SIGNATURE

Kozhukhivskyi A. D., *D.Sc., professor of information and information security department,*
Sagun A. V., *Ph.D., associate professor of information and information security department,*
Kozhukhivska O. A., *Ph.D., senior teacher of informatics and information security department,*
Snisarenko O. Ju., *undergraduate of information and information security department*
Stepanetz Ju. V., *undergraduate of information and information security department*
Cherkasy State Technological University,
Shevchenko blvd, 460, Cherkasy, Ukraine, 18006,
andrejdk@mail.ru

Abstract. *Basis tasks of cryptoanalysis of electronic digital signature are reviewed. Evaluations of probability of hash-function cracking by the methods of cracking stability to collisions and "birth-days date" paradox are shown. Schedules of the evaluations of cracking probability by these methods are built and analyzed.*

Keywords*: electronic digital signature, hash-function, elliptical curve.*

Вступ. Наявність кількох циркулюючих в Україні стандартів схем електронно-цифрового підпису (ЕЦП), що практично реалізовані в умовах підприємств різної форми власності, дає підґрунтя на проведення аналізу окремих елементів криптостійкості схеми ЕЦП з метою отримання чіткого уявлення про їх властивості та особливості.

В схемах симетричної (одноключової) криптографії, зокрема в алгоритмах шифрування та генерування імітовставки, обидві сторони інформаційного обміну мають один і той же секретний ключ. Цей ключ може бути згенерований як звичайний масив випадкових або псевдовипадкових бітів.

Аналіз стану наукових досліджень. Як було з'ясовано в [1–3], в асиметричних схемах ЕЦП існує поняття асиметрії ролей учасників ЕЦП, яке вимагає наявності в схемах ЕЦП двох тісно пов'язаних один з одним ключів: секретного (ключа підпису) та відкритого (ключа перевірки підпису). Але, в принципі, кожен з них окремо не є ключем у традиційному для криптології розумінні. Будь-яка схема ЕЦП повинна визначати три функціональні алгоритми, зокрема, алгоритм генерації ключової пари для підпису та його перевірки, алгоритм підпису, алгоритм перевірки підпису. На теперішній час текст специфікації ДСТУ 4145-2002 на алгоритм ЕЦП існує у вигляді короткої інформації [4, 5]. Цей алгоритм ґрунтується на еліптичних кривих над полем F(2) (несуперсингулярні криві). В стандарті використовуються криві в поліноміна-

льному і в оптимальному нормальному базисах. Причому, криві в поліномінальному базисі можуть бути другого та третього типів.

Основою для розробки цього стандарту став міжнародний стандарт IEEE 1363a. Для досягнення цим стандартом автентичності в ДСТУ 4145-2002, порівняно з IEEE 1363a, використовується своя функція гешування. Як алгоритм геш-функції використовується міждержавний стандарт ГОСТ Р 34.311-95 (раніше ГОСТ 28147-89 в режимі імітовставки).

Метою роботи є аналіз результатів порівнянь ймовірностей зламу геш-функцій за умови однакової довжини геш-значення методом зламу стійкості до зіткнень з методом зламу строгої стійкості до зіткнень.

Виклад основного матеріалу. Порівняємо алгоритми стандартів ЕЦП України, Росії та США. Як видно з аналізу таблиці алгоритмів ЕЦП США та РФ [6], стандарти РФ, України та США дуже схожі, але відрізняються виключно деякими числовими параметрами та деталями генерування ключової пари, обчислення та перевірки підпису. В свою чергу, стандарти України мають набагато більше спільних рис зі стандартами Росії. Дійсно, всі ці три алгоритми є варіантами схеми Ель-Гамаля [7].

При проведенні процедури гешування блоки даних, які можуть бути підписані безпосередньо, обмежені за розміром. Це робиться для того, щоб вони не виходили за межі розрядної сітки, що використовується під час роботи алгоритму. В той же час може виникнути потреба в розробці ЕЦП для документа довільного розміру. Для усунення цього обмеження в схемах ЕЦП підписують не безпосередньо електронний документ, а результат його перетворення в блок даних фіксованого розміру, що називається гешем. Алгоритми гешування або геш – функції, що, крім використання в схемах ЕЦП, можуть застосовуватися і самостійно в схемах захисту інформації. Наприклад, за їх допомогою можна виробляти ключ шифрування з пароля. В системах криптографічних стандартів України, Росії та США містяться визначення алгоритмів гешування. В Україні він встановлений відповідно до ГОСТ Р 34-311-95, в США – нормативними документами FIPS 180-1 і FIPS 180-2, в Росії – ГОСТ Р 34.11-94. В США раніше на геш існував стандарт SHS (secure hash standard), де розмір геш-блоку дорівнював 160 бітів. Однак у 2002 році цей стандарт був переглянутий. Надалі продовжив діяти старий стандарт з назвою SHA-1, але до нього було додано три нові алгоритми, що генерують геш-блоки розміром 256, 384 і 512 бітів, названі SHA-256/384/512 відповідно.

Російський та український стандарти відрізняються від стандарту США використанням принципово різних підходів до побудови геш-функції. В російському стандарті для генерування геша застосовується процедура шифрування ГОСТ 28147-89, в американському – цей стандарт є повністю самостійним. В українському стандарті підхід схожий на російський, гешування здійснюється відповідно до ГОСТ 28147-89.

Як наслідок, обидва стандарти, РФ та України, мають не один, а кілька варіантів гешей, оскільки параметром шифру є набір вузлів заміни. В такому випадку для кожного набору отримуємо свій геш. Цей нюанс має деякі переваги, але породжує й деякі проблеми сумісності, адже кожен із таких алгоритмів визначає крокову функцію гешування, яка на вході приймає два блоки даних: поточне значення геша з попереднього кроку і черговий фрагмент вхідного масиву даних. Внутрішня будова крокових функцій є різною. Так, у стандарті США SHA-1 ця функція реалізована в ітеративній процедурі і складається з 80 відносно нескладних раундів, інші геш-функції побудовані аналогічно. В російському стандарті гешування крокова функція гешування складається з лінійних операцій перемішування і чотирьох шифрувань за ГОСТ 28147-89 в режимі простої заміни. Вони виступають як основні джерела складності й нелінійності гешуючого перетворення. В табл. 1 наведено основні характеристики крокових функцій гешування.

Схеми перетворень даних при гешуванні за ГОСТ Р 34.11-94 і SHA-1 зображено на рис. 1 і 2 відповідно. З наведених даних зрозуміло, що складність американського стандарту гешування даних нижча, ніж у російського та українського. Російський стандарт передбачає виконання чотирьох зашифрованих за один цикл операцій генерування геша, або 128 раундів. Кожний раунд шифрування вимагає виконання приблизно 15 елементарних машинних операцій, що істотно збільшує витрати машинного часу на виконання операцій лінійного перемішування. Здійснення одного раунду гешування за SHA-1 набагато простіше: він весь може бути реалізований приблиз-

но за 15-20 команд. При цьому загальна кількість раундів становить 80, а за один цикл генерування геша оброблюється вдвічі більше вхідних даних – 512, проти 256 в ГОСТ Р 34.11-94. Таким чином, можна говорити про те, що швидкодія програмних реалізацій SHA-1 буде приблизно в 3-6 разів швидшою, ніж у стандартів Росії та України.

Таблиця 1

Крокові функції гешування в стандартах Росії, США та України на геш-функцію

Алгоритм	ГОСТ Р 34.11-94	SHA-1	ГОСТ Р 34-311-95
Розмір геш-функції, біт	256	160	256
Розмір блоку вхідних даних на крок, біт	256	512	256
Кількість раундів шифрування	128	80	128
Складність	Висока	Середня	Висока
Швидкодія	Невисока	Середня	Невисока

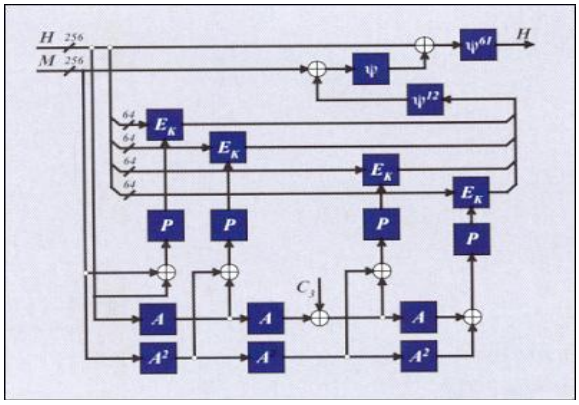

Рис. 1. Схема перетворення даних при гешуванні за ГОСТ Р 34.11-94

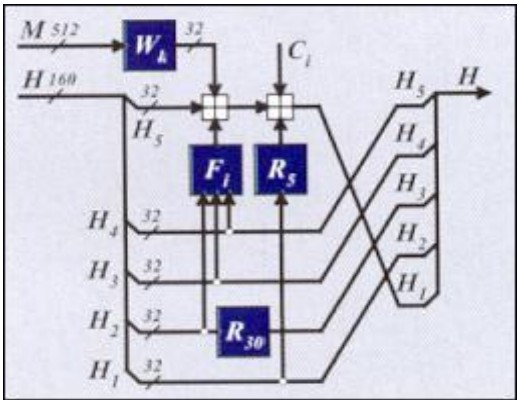

Рис. 2. Схема перетворення даних при гешуванні за SHA-1

На рис. 1 і 2 прийнято такі позначення: ***A, ψ*** – лінійні перемішування перетворення; ***P*** – перестановка байтів; E_K – операція шифрування за ГОСТ 28147-89; C_3 = const; F_i – нелінійні функції, де $1 \le i \le 4$; W_k – функції генерування 32-бітових елементів з 512-бітового блоку даних; C_i – константи, де $1 \le i \le 4$; R_i – операція циклічного зсуву аргументу на ***i*** біт ліворуч.

Окрім тривіальної функції гешування, система стандартів США визначає функції генерування геша, що залежать від ключа [6]. В стандартах гешування України та Росії аналог цього алгоритму відсутній. В принципі, аналог може бути розроблений доволі просто, адже достатньо легко можна внести зміни в звичайну процедуру гешування. Тим самим вона буде змінювати результат (довжину геш-повідомлення) залежно від довжини секретного ключа. Для цього достатнім буде додавати секретний ключ до масиву даних, що генеруються. Тому необхідність розробки окремого стандарту гешування, залежного від ключа, не є нагальною.

Теоретичні засади криптоаналізу ЕЦП за ДСТУ 4145-2002. Використання того чи іншого стандарту ЕЦП спирається на результати проведеного криптоаналізу. В результаті проведення такого криптоаналізу можна констатувати, наскільки стійким є той чи інший алгоритм. Надійність ЕЦП визначається стійкістю до криптоаналітичних атак таких її компонент, як: 1) геш-функції, 2) алгоритми ЕЦП.

Відомо, що стійка схема ЕЦП повинна використовувати геш-функцію з такими властивостями: а) односторонність, б) стійкість до зіткнень (колізії), в) строга стійкість до зіткнення (колізії).

Отже, основною задачею криптоаналізу ЕЦП є оцінка ймовірності зламу геш-функції за умов проведення таких атак: а) Broot-force (грубий підбір), б) підбір геш-значення.

На даний час стійкість всіх нових стандартів ЕЦП ґрунтується на складності

розв'язку задачі дискретного логарифмування в групі точок еліптичних кривих [8, 9].

Цю задачу можна сформулювати таким чином. Задано еліптичну криву E над полем $GF(p)$, де p – просте число; обрано точку P, що має простий порядок q в групі точок кривої E; знаючи точку dP, необхідно відновити натуральне число d. Відомо, що найбільш швидкими алгоритмами розв'язку задач дискретного логарифмування в групі точок еліптичної кривої за умови правильного вибору параметрів вважаються: r-метод та i-метод Полларда [8, 9].

Оцінка ймовірності зламу геш-функції. Базуючись на апараті криптоаналізу, сформульованому вище, оцінимо ймовірність зламу геш-функції. Для атаки методом broot-force розглянемо два методи.

1) Метод зламостійкості до зіткнень. За відомим значенням геш-функції $H(M)$ зловмисник створює інший документ M' такий, що $H(M')=H(M)$. Зловмисник намагається знайти два випадкових повідомлення M і M' таких, що $H(M')=H(M)$.

Припустимо, що геш-функція є абсолютно надійною і однонаправленою, і не існує іншого методу її зламу, ніж broot-force. На виході цієї функції отримуємо число, розрядність якого – m. Тоді кількість вихідних значень функції $H=2^m$.

Позначимо $P(n,k)$ ймовірність того, що для конкретного значення X і хоча б одного Y_i з діапазону значень $Y_1 \mathbf{L} Y_k$ виконується рівність $H(X)=H(Y)$. Для одного Y ймовірність того, що $H(X)=H(Y)$, становитиме $1/n$. Звідси легко знайти, що ймовірність тотожності виразу $H(X)\neq H(Y)$ становить $(1-(1/n))$. Якщо генерувати k значень, то ймовірність того, що жодне з них не буде повторюватися, визначається як добуток ймовірностей, що відповідають одному значенню $(1-(1/n))^k$. Отже, логічно зробити висновок, що ймовірність хоча б одного збігу буде дорівнювати $P(n,k)=1–(1–(1/n))$. Для випадку абсолютного зламу ймовірність настання такого випадку буде дорівнювати $P(n,k)=1$.

Розглянемо парадокс «днів народження». В математичній статистиці існує декілька парадоксів, які дозволяють значно полегшити задачу зламу, зокрема, парадокс «днів народження». Він полягає в тому, що з імовірністю P=0,5 з 23 осіб, зібраних в одному місці, як мінімум, у двох буде день народження в один день. Звідси можна записати: $P(n,k)=0.5$, отже, $k=n/2=2^{m-1}$. Таким чином, можна стверджувати відносну ймовірність здійснення атаки методом зламу стійкості до зіткнень, тобто для знаходження повідомлення, що генерується до заданого значення, необхідно гешування 2^{m-1} випадкових повідомлень. А ймовірність зламу геш-функції знаходиться як $1/2^{m-1}$.

Використовуючи наведене вище, можна отримати значення ймовірностей зламу геш-функції для геш-значень різної розрядності (табл. 2).

Побудуємо графічну залежність ймовірності зламу геш-функції від довжини геш-значення (рис. 3) на основі даних табл. 2.

Як видно з графічної залежності на рис. 3, ймовірність зламу геш-функції методом, що ґрунтується на припущенні парадоксу «днів народження», показує адекватний результат відносно довжини секретного ключа.

Таблиця 2

Оцінка ймовірностей зламу геш-функції для атаки методом стійкості до зіткнень

Довжина значення геш-функції	Ймовірність зламу
64	1,08420217248550443400745280086 99e-19
128	5,87747175411143753984368268611 12e-39
192	3,18618382226490455405776079553 54e-58
256	1,72723371101888892507727037256 01e-77
384	5,07588367463129844654804911166 11e-116
512	1,49166814624004134865819306309 26e-154

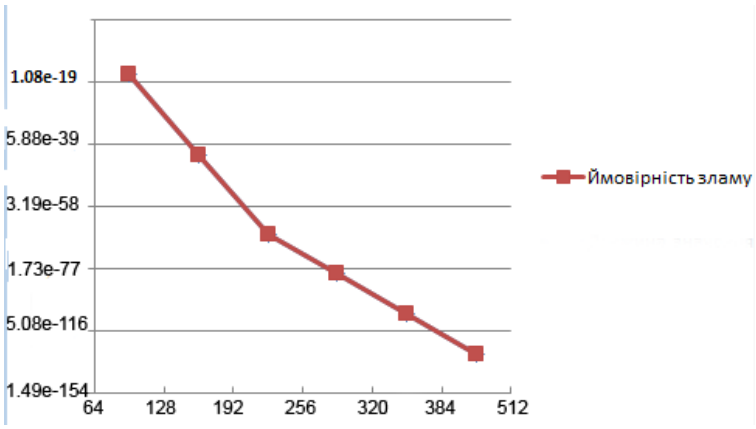

Рис. 3. Графічна залежність ймовірності зламу геш-функції від довжини геш-значення першим методом

2) Метод зламу строгої стійкості до зіткнень. Нехай $P(n,g)$ – ймовірність того, що у множині з g елементів, кожен з яких може набувати n значень, є, як мінімум, два елементи, значення яких рівні. Значення, якого повинне набувати g для того, щоб виконувалася умова:

$$P(n,g)>0.5. \qquad (1)$$

З (1) можна зробити висновок, що кількість способів вибору елементів таким чином, щоб при цьому не було повторень, становить $n!/(n-g)!$ при тому, що загальна кількість способів вибору таких елементів дорівнює n^g. Ймовірність того, що елементи не повторюються, становить $n!/[(n-g)!n^g]$. Вираз (1) можна переписати для випадку ймовірності появи повторень:

$$P(n,g)=1-[n!/((n-r)!)n^g)]. \qquad (2)$$

Якщо $P(n,g)=0.5$, тоді $g=\sqrt{n\ln 2}=\ln 2\sqrt{n}\approx n^{1/2}$. Припустимо, що довжина геш-коду становить m біт, тоді кількість значень, яких він набуває, дорівнює 2^m, і $g=\sqrt{2^m}=2^{m/2}$. Звідси можна зробити висновок про те, що для отримання двох повідомлень з однаковим вмістом необхідно загешувати $2^{m/2}$ випадкових повідомлень. Ймовірність зламу при цьому можна оцінити як $(1/2)^{m/2}$. Скориставшись виразом (2), можна отримати значення ймовірностей зламу геш-функції для геш-значень різної розрядності (табл. 3).

Побудуємо графічну залежність ймовірності зламу геш-функції від довжини геш-значення на основі даних табл. 3 (рис. 4).

Таблиця 3

Оцінка ймовірностей зламу геш-функції для атаки методом строгої стійкості до зіткнень

Довжина значення геш-функції	Ймовірність зламу
64	0,0000000002328306436538696289062 5
128	5,421010862427522170037264004349 7e-20
192	1,262177448353618888658765704452 5e-29
256	2,938735877055718769921841343055 6e-39
384	1,593091911132452277028880397767 7e-58
512	8,636168555094444625386351862800 4e-78

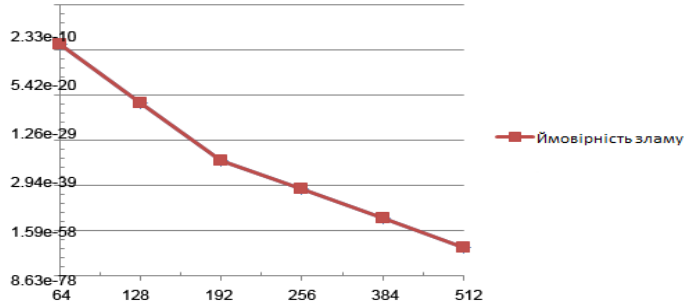

Рис. 4. Графічна залежність ймовірності зламу геш-функції від довжини геш-значення другим методом

Висновки. З отриманих у статті результатів порівнянь ймовірностей зламу геш-функцій зрозуміло, що за умови однакової довжини геш-значення ймовірність зламу геш-значення методом зламу стійкості до зіткнень набагато нижча, ніж з використанням методу зламу строгої стійкості до зіткнень. Так, для розрядності геш-функції 128 біт ймовірність зламу відрізняється для обох методів у 9223372036854775808 рази. На основі цього можна зробити висновок, що для підвищення стійкості геш-функції ЕЦП до зламу хоча б до рівня $1*10^{-25}$ слід застосовувати 192-бітне шифрування.

Список літератури

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002.
2. Menezes, A., Oorschot, O. and Vanstone, S. (1996) Handbook of applied cryptography. CRC Press.
3. Wang, X., Feng, D., Lai, X. and Yu, H. (2004) Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. CRYPTO.
4. Мир защиты информации [Электронный ресурс]. – Режим доступа : http://infoch.info/view_lesson.php?id=334.
5. ДСТУ 4145-2002 Головна [Електронний ресурс]. – Режим доступу : http://www.cryptography.org.ua/index.html
6. Винокуров А. Ю. Стандарты криптографической защиты информации России и США / А. Ю. Винокуров // Отраслевой каталог «Технологии и средства связи-2003». – М. : Гротек, 2003.
7. Щербаков А. Прикладная криптография. Использование и синтез криптографических интерфейсов / А. Щербаков, А. Домашев. – М. : Русская редакция, 2002.
8. Горбенко І. Д. Прикладна криптологія: Теорія. Практика. Застосування : [монографія] / І. Д. Горбенко, Ю. І. Горбенко. – [Вид. 2-ге, перероб. і доп.]. – Харків : Форт, 2012. – 880 с.
9. Горбенко Ю. І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : [монографія] / Ю. І. Горбенко, І. Д. Горбенко. – Харків : Форт, 2010. – 608 с.

References

1. Shnayer, B. (2002) Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na yazyke Si. Moskva: Triumf [in Russian]
2. Menezes, A., Oorschot, O. and Vanstone, S. (1996) Handbook of applied cryptography. CRC Press.
3. Wang, X., Feng, D., Lai, X. and Yu, H. (2004) Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. CRYPTO.
4. Mir zashhyty informaczyy. Available at: http://infoch.info/view_lesson.php?id=334. [in Russian]
5. DSTU 4145-2002: Golovna. Available at: http://www.cryptography.org.ua/index.html [in Ukrainian]
6. Vinokurov, A. Yu. (2003) Standarty kriptografycheskoj zashhyty informaczyy Rossiy i SSHA. Otraslevoj catalog *“Tehnologij i sredstva cvyazi - 2003”*. Moskva: Grotek. [in Russian]
7. Shherbakov, A. and Domashev, A. (2002) Prikladnaja kriptografija. Ispolzovanie i sintez kriptograficheskih interfejsov. Moskva: Russkaja redakzija. [in Russian]
8. Horbenko, I. D. and Horbenko, Yu. I. (2012) Prykladnaja kryptologiia: Teorija. Praktyka. Zastosuvannia. Vyd. 2-e, pererob. i dop. Kharkiv: Vyd-vo “Fort”, 880 s. [in Ukrainian]
9. Horbenko, Yu. I. and Horbenko, I. D. (2010) Infrastruktury vidkrytykh kliuchiv. Elektronnyi tsyfrovyi pidpys. Teorija ta praktyka. Kharkiv: Vyd-vo “Fort”, 608 s. [in Ukrainian]