РЕАЛІЗАЦІЯ АЛГОРИТМУ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ ECDSA НА PYTHON 3.7

Щербина Д.В.
Науковий керівник – к.т.н, доц. Ляшенко О.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Радіотехніки, тел. (057) 702-13-06)
e-mail: denys.shcherbyna@nure.ua, факс (057) 702-11-13

The given work is devoted to one of the standard digital signature algorithm named Elliptic Curve Digital Signature Algorithm (ECDSA), which is widely used is TLS, SSL, PGP, Bitcoin and elsewhere. ECDSA is the elliptic curve analogue of the DSA and has been standardized by many standards organizations around the world including NIST, IEEE, ANSI and ISO [1]. Unlike the ordinary discrete logarithm and the integer factorization problem, no subexponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an elliptic curve.

Рукописні підписи здавна використовуються як доказ авторства документу або повідомлення та згоду з його змістом. Їхніми основними властивостями є достовірність, непідробність, неможливість зміни після підписання і т. д [2].

На жаль, ті проблеми, які присутні у реальному житті так само переносяться у світ електронної передачі інформації. Для подолання цих проблем був розроблений електронно-цифровий підпис (ЕЦП), що представляє собою невеликий обсяг даних, переданих разом з документом або повідомленням при його пересиланні.

ECDSA (Elliptic Curve Digital Signature Algorithm) – це алгоритм з відкритим ключем для створення цифрового підпису, аналогічний за своєю будовою DSA, але визначений, на відміну від нього, не над полем цілих чисел, а в групі точок еліптичної кривої.

Стійкість цього алгоритму ґрунтується на проблемі дискретного логарифмування в групі точок еліптичної кривої [1]. На відміну від проблеми простого дискретного логарифма і проблеми факторизації цілого числа, не існує суб-експоненціального алгоритму для проблеми дискретного логарифма в групі точок еліптичної кривої. З цієї причини «сила на один біт ключа» набагато вище в алгоритмі з еліптичними кривими.

У 1998 році алгоритм ECDSA був прийнятий стандартом ISO. Пізніше був прийнятий як стандарт ANSI у 1999 році, а у 2000 році – як стандарт IEEE і NIST.

ECDSA працює з хешем повідомлення, а не з самим повідомленням. У програмній реалізації, написаній на мові Python 3.7, була використана хеш-функція SHA-512 з модуля hashlib. Хеш повідомлення необхідно урізати,

щоб бітова довжина хеша була такою ж, як і бітова довжина порядка підгрупи n. Урізаний хеш – це ціле число, позначене, як z.

Алгоритм який виконується Алісою для підписування повідомлення, виглядає так:

1. Беремо випадкове ціле k, вибране у діапазоні від 1 до $n-1$, де n – порядок підгруппи. За це відповідає функція make_keypair.

2. Обчислюємо точку $P = kG$, де G – базова точка підгруппи. Функція scalar_mult відповідає за цей крок.

3. Обчислюємо число $r = x_P \, mod \, n$, де x_P – координата x точки P.

4. Якщо $r = 0$, то обираємо інше k і повторюємо кроки, починаючи з другого.

5. Обчислюємо $s = k^{-1}(z + rd_A) \, mod \, n$, де d_A – закритий ключ Аліси, k^{-1} – мультиплікативна інверсія k за модулем n (обчислюється функцією inverse_mod).

6. Якщо $s = 0$, то обираємо інше k і повторюємо кроки, починаючи з другого.

Пара (r, s) і є підписом. За генерацію підпису відповідає функція sign_message.

Для перевірки підпису необхідний відкритий ключ Аліси H_A, урізаний хеш z і підпис (r, s):

1. Обчислюємо ціле $u_1 = s^{-1}z \ \ mod \, n$.
2. Обчислюємо ціле $u_2 = s^{-1}r \ \ mod \, n$.
3. Обчислюємо точку $P = u_1G + u_2H_A$.

Підпис дійсна, якщо $r = x_P \, mod \, n$. За перевірку підпису відповідає функція verify_signature.

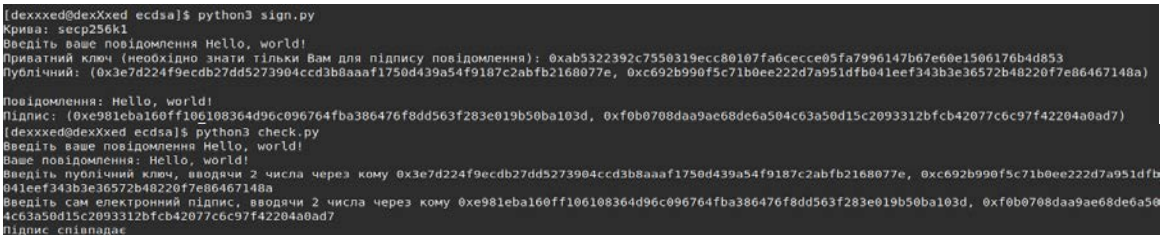

Рисунок 1 – Результат роботи скриптів

Для генерування та перевірки підписів були написані скрипти на мові Python 3.7. нижче.

Список джерел:

1. D. Brown, Generic groups, collision resistance, and ECDSA, Designs, Codes and Cryptography, 35 (2005), 119-152 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. – 40 с.