УДК 004.056
Сава Л. – ст. гр. СБс-42
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ТА РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ДЛЯ АЛГОРИТМУ ECDH

Науковий керівник: д.т.н. проф. Карпінський М.П.

Sava L.
Ternopil Ivan Puluj National Technical University

ANALYSIS AND IMPLEMENTATION OF CRYPTOGRAPHIC TRANSFORMATIONS FOR ECDH ALGORITHM

Supervisor: M. Karpinski, Prof. Dr.

Ключові слова: ECC, ECCDH, RSA, асиметрична криптографія
Keywords: ECC, ECCDH, RSA, asymmetric cryptography

Сьогодні криптосистеми на еліптичних кривих використовуються в TLS, PGP та SSH, найважливіших технологіях, на яких базуються сучасний web та світ IT. Всім, хто знайомий із криптографією з відкритим ключем, відомі абревіатури ECC, ECDH та ECDSA. ECC (Elliptic Curve Cryptography) – це криптографія на еліптичних кривих, решта – назви заснованих на ній алгоритмів. До появи ECC переважна більшість алгоритмів з відкритим ключем ґрунтувалися на RSA, DSA та DH, альтернативних криптосистемах на основі модулярної арифметики. Вони і досі популярні, і часто використовуються з ECC. В даній роботі проведений аналіз алгоритму ECDH.

Еліптична крива - це безліч точок, що описується рівнянням:

$$y^2 = x^3 + ax + b$$

де $4a^3 + 27b^2 \neq 0$ (це необхідно, щоб виключити особливі криві). Наведене вище рівняння називається звичайним формулюванням Вейєрштраса для еліптичних кривих. Приклади еліптичних кривих наведені на рис. 1, де а) крива з точкою повернення ($y^2 = x^3$). б) крива із самоперетином ($y^2 = x^3 - 3x + 2$).

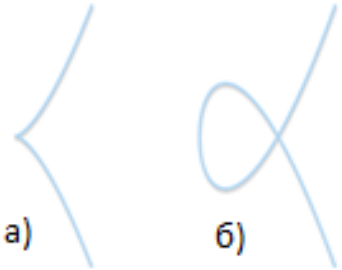

Рис. 1. Різні форми еліптичних кривих.

В залежності від значень a і b, еліптичні криві можуть набувати на площині різних форм та еліптичні криві симетричні щодо осі X.

Криптографія на еліптичних кривих буває із закритим ключем - це випадкове ціле d, вибране з {1, …, n - 1}, де n - порядок підгрупи та відкритим ключем – це точка H = dG, де G – базова точка підгрупи. Якщо відомі d і G (разом з іншими параметрами області визначення), то знайти H просто. Але якщо відомі H і G, то пошук закритого

ключа d є складним завданням, тому що вимагає вирішення задачі дискретного логарифмування.

ECDH (Elliptic curve Diffie-Hellman, протокол Діффі-Хеллмана на еліптичних кривих), що використовується для шифрування, заснований на принципі алгоритму з відкритим ключем. ECDH – це швидше протокол узгодження ключів. По суті, це означає, що ECDH задає (певною мірою) порядок генерування ключів та обміну ними. Спосіб шифрування даних за допомогою таких ключів можена вибирати.

Він вирішує наступну проблему: дві сторони (зазвичай Аліса та Боб) хочуть безпечно обмінюватися інформацією, щоб третя сторона (посередник, Man In the Middle) міг перехоплювати її, але не міг розшифрувати. Наприклад, це один із принципів TLS. Алгоритм працює наступним чином:

1. Спочатку Аліса та Боб генерують власні закриті та відкриті ключі. Аліса має закритий ключ d_A і відкритий ключ $H_A = d_AG$, у Боба є ключі d_B і $H_B = d_BG$. Аліса, і Боб використовують однакові параметри області визначення: одну базову точку G на одній еліптичній кривій в однаковому кінцевому полі.

2. Аліса і Боб обмінюються відкритими ключами H_A і H_B незахищеним каналом. Посередник (Man In the Middle) перехоплює H_A і H_B, але неможе визначити ні d_A, ні d_B, не вирішивши завдання дискретного логарифмування.

3. Аліса обчислює $S = d_A H_B$ (за допомогою власного закритого ключа та відкритого ключа Боба), а Боб обчислює $S = d_B H_A$ (за допомогою власного закритого ключа та відкритого ключа Аліси). Потрібно врахувати, що S для Аліси, і Боба однаковий:

$$S = d_A H_B = d_A(d_B G) = d_B(d_A G) = d_B H_A.$$

Однак посереднику відомі тільки H_A і H_B (разом з іншими параметрами області визначення) і він не зможе знайти спільний секретний ключ S. Це відомо як завдання Діффі-Хеллмана, яке можна сформулювати наступним чином: яким буде результат abP для трьох точок P, aP та bP, або яким буде результат k^{xy} для трьох цілих k, k^x та k^y? Останнє формулювання використовується у вихідному алгоритмі Діффі-Хеллмана, що базується на модулярній арифметиці.

Протокол Діффі-Хеллмана полягає у тому, що Аліса та Боб можуть просто вирахувати загальний секретний ключ, посереднику ж доведеться вирішувати складне завдання.

Задача Діффі-Хеллмана для еліптичних кривих вважається складною, як і завдання дискретного логарифмування, але математичних доказів цьому немає. Можна сказати, що вона не може бути складнішою, тому що розв'язання задачі логарифмування — це спосіб розв'язання задачі Діффі-Хеллмана. Отримавши спільний секретний ключ, Аліса та Боб можуть обмінюватися даними із симетричним шифруванням. Наприклад, вони можуть використовувати координату x ключа S як ключ для шифрування повідомлень такими безпечними шифрами, як AES або 3DES. Це робить TLS, різниця в тому, що TLS з'єднує координату x з іншими числами, що відносяться до підключення, а потім обчислюється хеш рядка байтів, що вийшло.

Для обчислення закритих/відкритих ключів та загальних секретних ключів над еліптичною кривою використовується стандартизована крива, а не проста крива на невеликому полі. Обрано криву secp256k1 групи SECG (Standards for Efficient Cryptography Group), що також використовується в Bitcoin для цифрових підписів.