Кошелєв О.О.
студент,
Одеська національна Академія зв'язку
імені О.С. Попова

ПОРІВНЯННЯ АСИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

В сучаних реаліях постало питання захищенності повідомлень, конфіденційної та таємної інформації, котра потребує передачі незахищеними каналами. В дипломній роботі проводиться аналіз асиметричних алгоритмів шифрування RSA, ECC, NTRU та інших.

В основі RSA (Rivest, Shamir и Adleman) лежить завдання факторизації простих великих чисел. Для шифрування використовується проста операція піднесення до степеня за модулем N. Для розшифрування необхідно обчислити функцію Ейлера від числа N, для цього необхідно розкласти число n на прості множники (В цьому і полягає завдання факторизації). В RSA відкритий і закритий ключ складається з пари цілих чисел. Закритий ключ зберігається в секреті, а відкритий ключ повідомляється іншому учаснику.

Для того, щоб згенерувати пари ключів виконуються такі дії:

1. Вибираються два великі прості числа p і q приблизно 512 біт завдовжки кожне;
2. Обчислюється їх добуток

$$n = pq;$$

3. Обчислюється функція Ейлера

$$\varphi(n) = (p-1)(q-1);$$

4. Вибирається ціле число e таке, що $1 < e < \varphi(n)$ та e взаємно просте з $\varphi(n)$;
5. За допомогою розширеного алгоритму Евкліда знаходиться число d таке, що

$$ed \equiv 1\ (mod\varphi(n)).$$

Число n називається модулем, а числа e і d – відкритою й секретною експонентами відповідно. Пари чисел (n,e) є відкритою частиною ключа, а (n,d) – секретною. Числа p і q після генерації пари ключів можуть бути знищені, але в жодному разі не повинні бути розкриті.

Алгоритм шифрування RSA, хоча і має достатню крипостійкість, через велику довжину ключа потребує використання потужної обчислювальної техніки. За відсутності такої, генерація ключів займатиме велику кількіть часу.

ECC (Elliptic Curve Cryptography) – це метод криптографії з відкритим ключем, заснований на використанні еліптичних кривих над кінцевими полями. Криптосистеми з відкритим ключем на еліптичних кривих забезпечують таку ж функціональність, як і алгоритм RSA. Проте їх крипостійкість заснована на рішення іншої задачі, а саме на проблемі дискретного логарифма в групі точок еліптичної кривої.

Еліптична крива – це набір точок, описуються рівнянням Вейерштрассе:

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

У криптографії розглядається два види еліптичних кривих: над кінцевим полем Z_p – кільце вирахувань по модулю простого числа. І над полем $GF(2^m)$ – бінарне кінцеве поле.

Для зашифруваня тексту:

1. Обирається точка G на еліптичній кривій $E_p(a, b)$;
2. Обирається особистий ключ n_A та генерується відкритий ключ:

$$P_A = n_A G;$$

3. Обирається число k таобчислюється шифрований текст G_m:

$$G_m = (kG, P_m + kP_B), G_m \neq P_m, \textit{де } G_m \textit{ – пара точок.}$$

Для розшифрування тексту першу точку в парі потрібно помножити на секретний ключ n_B і результат відняти від другої точки:

$$(P_m + kP_B) - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m,$$

де P_B- відкритий ключ, P_m – повідомлення.

Криптосистема NTRU (Number Theorists aRe Us) була запатентована 24 липня 2000 року. NTRU заснована на алгебраїчної структурі деякого полиномиального кільця. Важкою задачею є пошук найкоротшого вектора в заданій ришітці. Процедура шифрування грунтується на змішаних операціях: полиномиальной алгебри і приведення по модулю двох чисел.

Формування ключа

Нехай дано поліноміальне кільце Г з поліномом $X^N - 1$: $\Gamma = Z[X]/(X^N - 1)$.

Дано: два випадкових числа p і q;

Випадковим чином обираються два полінома $f,g \in \Gamma$, якщо

$$\exists I_{fq} \equiv f^{-1} mod q,$$

$$\exists I_{fp} \equiv f^{-1} mod p;$$

Розрахунок $h \equiv I_{fq} \otimes g \mathrm{mod} q$;

Отримаємо h, f, I_{fp}, де h – відкритий ключ, f – особистий ключ, I_{fp} – інверсія особистого ключа.

Зашифрування

Дано: відкритий текст $m \in \Gamma$ (за коефіцієнтами, приведеними по модую q), відкритий ключ h;

Вибір випадкового полінома $\varphi \in \Gamma$;

Обчислення шифрованого тексту

$$e \equiv (p\varphi \otimes +m) \mathrm{mod} q;$$

Отримаємо шифртекст e.

Розшифрування

Дано: шифртекст e, особистий ключ f

Обчислення

$a \equiv (f \otimes e) \mathrm{mod} q$, де обираються коєфіцієнти полінома a з (-q/2,q/2);

Обчислення

$$m \equiv \left(I_{fp} \otimes a \right) \mathrm{mod} p.$$

Отримаємо відкритий текст m.

Як стало видно з процедури розшифрування, криптосистема NTRU є ймовірнісної, що дозволяє отримати неправильне вихідне повідомлення на етапі розшифрування при тих же значеннях параметрів φ, f, g імовірність помилки мізерно мала, і вона прямо залежить від коректного вибору φ, f, g.

В таблиці наведено результати порівняння довжини ключів ECC, RSA і NTRU, які забезпечують однаковий рівень безпеки.

Таблиця 1

Порівняння довжини ключів

	RSA	ECC	NTRU
Довжина особистого ключа, біт	1024	168	263
Довжина блока тексту, біт	1024	160	416
Довжина відкритого ключа, біт	1024	169	1841
Час формування ключа, мс	1432	65	19,8
Зашифрування, мс	4,28	140	1,9
Розшифрування, мс	48,5	67	3,5

Як видно алгоритми шифрування ECC, NTRU мають більш високу продуктивність у порівнянні з RSA при однаковій криптостійкості. Що дозволяє забезпечувати високу швидкість і захист при мінімальних вимогах до системних ресурсів. Стійкість алгоритмів шифрування ECC, як правило, заснована на труднощі рішення задачі дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) Стійкість алгоритмів шифрування NTRU забезпечується труднощами знаходження найкоротшого вектора в заданій числовий решітці, що в свою чергу робить шифрування NTRU стійким до атак на квантових комп’ютерах.

Список використаних джерел:

1. Jerey Hostein NTRU: A Ring-Based Public Key Cryptosystem / Jerey Hostein, Jill Pipher, Joseph H. Silverman, 2006. – 22 с.

2. NTRU Encrypt. [Электронный ресурс]. Режим доступа: https://ru.Wikipedia.org/wiki/ NTRUEncrypt.

3. Онацький А. В. Асиметричні методи шифрування / А. В. Онацький, Л. Г. Йона. – 2010. – 148 с.

4. Ковтун В. Ю. Методы и алгоритмы арифметических преобразований с уменьшенной вычислительной сложностью на алгебраических кривых для криптографических приложений: Диссертация кандидата технических наук: Системы защиты информации. – Харьковский университет Воздушных Сил.– Украина: Харьков, 2005. – 249 с.