Технічні науки

УДК 004.056.55

Казаченко Ольга Дмитрівна

Студентка

Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Казаченко Ольга Дмитриевна

Студентка

Национальний технический университет Украины

«Киевский политехнический институт им. Игоря Сикорского»

Kazachenko Olha

Student

National technical university of Ukraine

«Igor Sikorsky Kyiv Polytechnic Institute»

РЕАЛІЗАЦІЯ АЛГОРИТМУ RSA З ЗАСТОСУВАННЯМ КИТАЙСЬКОЇ ТЕОРЕМИ ПРО ЗАЛИШКИ

РЕАЛИЗАЦИЯ АЛГОРИТМА RSA С ИСПОЛЬЗОВАНИЕМ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

RSA ALGORITHM IMPLEMENTATION USING CHINESE REMAINDER THEOREM

Анотація. У даній статті описано модифікацію алгоритму шифрування RSA використання китайської теореми про залишки, а також вплив використання китайської теореми про залишки на роботу криптосистеми.

Ключові слова: Алгоритм RSA, шифрування, цифровий підпис, CRT, Китайська теорема про залишки.

Анотация. В данной статье описано модификацию алгоритма шифрования RSA с использованием китайской теоремы про остатки, а

также влияние внедрения китайской теоремы об остатках на работу криптосистемы.

Ключевые слова: Алгоритм RSA, шифрование, цифровая подпись, CRT, Китайска теорема про остатки.

Summary. This article describes the modification of the RSA encryption algorithm using the Chinese remainder theorem, as well as the impact of the implementation of encryption using Chinese remainder theorem on the behavior of cryptosystem.

Keywords: RSA, encryption algorithm, digital signature, CRT, Chinese remainder theorem.

1. Вступ

RSA (Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем. Він став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису [1]. Криптосистема RSA використовується у різних продуктах, на різних платформах і у багатьох галузях. В даний час вона вбудовується в комерційні продукти, число яких постійно збільшується. Також її використовують операційні системи Microsoft, Apple, Sun і Novell. В апаратному виконанні RSA алгоритм застосовується в захищених телефонах, на мережних платах Ethernet, на смарт-картах. Математичний апарат, що лежить в основі роботи алгоритму дуже складний і базується на обчислювальній складності задачі факторизації великих цілих чисел. Існує багато дослідження з приводу модифікацій алгоритм та його удосконалення. Розглянемо китайську теорему про залишку та її вплив при використанні у даній криптосистемі.

2. Алгоритм RSA

Криптографічні системи з відкритим ключем використовують так званні односторонні функції, котрі характеризуються наступними властивостями:

- Якщо відомо *x*, то *f(x)* відносно легко розрахувати;
- Якщо відомо $y = f(x)$, то для того щоб розрахувати *x* немає легко та ефективного шляху.

Під односторонністю мається на увазі не теоретична одно направленість, а практична неможливість розрахувати оберне значення з використання сучасних обчислювальних засобів за прийнятний час.

В основі криптосистеми покладена задача факторизації добутку двох великих чисел. Для шифрування потрібно реалізувати операцію піднесення у степінь великого числа по модулю, а для дешифрування необхідно обчислити функцію Ейлера від великого числа, для чого потрібно знати розклад числа на прості множники [1].

2.1 Генерація ключів

Користувачі мають відкритий за приватний ключ, кожен з яких складається з пари цілих чисел. Приватний ключ тримається у секреті, відкритий же можна повідомляти, вони являються взаємно оберненими. Це означає:

- Для всіх допустимих відкритого та приватного ключа P та S існують відповідні функції шифрування $E_p(x)$ та дешифрування $D_s(x)$, такі, що

$$\boldsymbol{m = D_s\,(Ep\,(m))\; = \; Ep\,(D_s(m))}$$

- Це виконується для всіх повідомлень $m \in M$, де M – множина допустимих повідомлень

Для генерації ключів використовують наступний алгоритм:

1. Вибирають два різних, довільних, простих числа p та q заданого розміру (512/1024/2048 біт кожне)
2. Розраховується добуток $n = p * q$, який називається модулем
3. Розраховується значення функції Ейлера від числа $n: f = (p - 1) * (q - 1)$

4. Вибирається ціле, взаємно просто число e, таке що $1 < e < f$. Воно називається відкритою експонентою. Час затрачений на шифрування пропорційний числу одиничних біт в e. Таким чином, частіше вибирають e з більшою кількістю одиниць у двійковому представленні.

5. Розраховується число d мультиплікативно зворотне числу e по модулю f, тобто таке, що : $d * e \equiv 1 mod\, f$. Воно називається секретною експонентою і зазвичай рахується з застосуванням розширеного алгоритму Евкліда.

6. Таким чином отримується пара відкритого ключа {e, n} та приватного{d, n} [2].

2.2 Шифрування та дешифрування

Розглянемо на відомому прикладі спілкування Боба та Аліси. Припустимо, Боб хоче відправити повідомлення m Алісі.

Алгоритм шифрування зображено на рисунку 1 і виконується у такій послідовності:

- Взяти відкритий ключ $\{e, n\}$ Аліси
- Взяти відкритий, вхідний текст m
- Зашифрувати повідомлення з використанням відкритого ключа Аліси

$$c = E(m) = m^e \, mod \, n$$

Після отримання Бобом повідомлення виконується дешифровка:

- Взяти зашифроване повідомлення
- Взяти приватний ключ $\{d, n\}$
- Розшифрувати по формулі : $m = D(c) = c^{\,d} mod \, n$

Рисунок 1. Схема обміну даними, зашифрованими алгоритмом RSA [розробка автора]

3. Швидкість алгоритму та використання CRT

Оскільки генерація ключів використовується набагато рідше за шифрування, дешифрування, створення та перевірку підписів, задача обчислення $a = b^{c} mod\, n$ являється основним обчислювально-складним моментом. Вирішується вона алгоритмом швидко піднесення в степінь і таким чином витрачає $O(ln\, e)$ операцій множення по модулю.

Для аналізу часу виконання операцій з приватним та відкритим ключами, візьмемо $\{d, n\}$ та $\{e, n\}$, які задовольняють умовам : $log_2 e = O(1), log_2 d \leq O(\beta)$. Тоді при їх використанні виконується відповідно *O(1)* та *O(β)* операцій множення по модулю.

Таким чином час виконання тим більший, чим більше одиниць у двійковому представленні відкритої експоненти. По евристичний оцінкам довжина секретної експоненти d нетривіальним чином пов'язана з відкритою *e* та модулем *n*. Тому дешифровка повільніша за шифрування, а перевірка цифрового підпису швидша за створення [3].

При дешифрування та підписуванні повідомлення алгоритмом RSA показник обчислювальної степені буде достатньо великим числом (близько 1000 біт). Таким чином, потрібен алгоритм, що скоротить кількість операцій. Так як числа p та q в розкладі $N = p * q$ відомі шифрувальнику повідомлення, то можна обчислити:

$$m_p = C^d\, mod\, p = C^{d\ mod\, p-1}\ mod\, p$$

$$m_q = C^d \bmod q = C^{d \bmod q-1} \bmod q$$

Оскільки p та q – числа порядку 2^{512} на ці дії потрібно буде зробити два піднесення у степінь з показником у 512 біт по модулю 512-бітового числа. Це набагато швидше ніж одне піднесення у степінь з 1024-бітним показником по модулю 1024-бітного числа. В кінці потрібно буде лише відновити повідомлення m використовуючи m_q та m_p. Це легко зробити за допомогою китайської теореми про залишки. [4]

Теоретично вважається, що дешифрування з використанням CRT допомагає пришвидшити процес у чотири рази. Середній час дешифрування нормального методу близько 0.157 секунд, а з використанням китайської теореми становить близько 0.046 секунд, що дає приріст по швидкості приблизно у 3.4 рази.

4. Висновок

Було розглянуто принцип роботи алгоритму RSA та вплив на роботу алгоритму використання китайської теореми про залишки. Стандартна реалізація алгоритму маю досить низьку швидкість дешифрування повідомлень порівняно з симетричним та широко розповсюдженим алгоритмом AES. Китайська теорема про залишку розвантажує RSA від піднесення у степінь з дуже великим показником, зменшуючи його розрядність вдвічі. Таким чином можна збільшити швидкість алгоритму на практиці у 3.4 рази.

Література:

1. Wikipedia (https://en.wikipedia.org/wiki/RSA_(cryptosystem)).
2. Evgeny Milanov, The RSA Algorithm, https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf
3. G.N. Shinde, H.S. Fadewar Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem, http://www.techscience.com/doi/10.3970/icces.2008.005.255.pdf

4. Johann Großschadl The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip, Graz University of Technology, Institute for Applied Information Processing and Communications, Inffeldgasse 16a, A–8010 Graz, Austria.