Шифр:
Таємниця

Студентська наукова робота по профілю:
«Інформаційна безпека»
Тема: «Узагальнення криптоалгоритма RSA і спосіб його реалізації»

Зміст

Вступ

У сучасному світі інформаційний ресурс став одним з найбільш потужних важелів економічного розвитку. Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху в будь-якому вигляді господарської діяльності. Монопольне володіння певною інформацією виявляється найчастіше вирішальною перевагою в конкурентній боротьбі і обумовлює, тим самим, високу ціну "інформаційного фактора". Широке впровадження персональних ЕОМ вивело рівень "інформатизації" ділового життя на якісно новий рівень. Нині важко уявити собі фірму або підприємство (включаючи найдрібніші), які не були б озброєні сучасними засобами обробки та передачі інформації. У ЕОМ на носіях даних накопичуються значні обсяги інформації, що найчастіше носять конфіденційний характер або становлять велику цінність для її власника.

Криптографія займається методами перетворення інформації, які б не дозволили противнику витягти її з перехоплених повідомлень. При цьому по каналу зв'язку передається вже не сама інформація, що захищається, а результат її перетворення за допомогою шифру, і для противника виникає складне завдання розкриття шифру. Розкриття (злом) шифру – процес отримання інформації, яка є закрита у шифрованому повідомленні без знання застосованого шифру. Противник може намагатися не отримати, а знищити або модифікувати інформацію, що захищається в процесі її передачі. Це – зовсім інший тип загроз для інформації, відмінний від перехоплення і розкриття шифру. Для захисту від таких загроз розробляються свої специфічні методи. Отже, на шляху від одного законного користувача до іншого інформація повинна захищатися різними способами, що протистоять різним загрозам. Виникає ситуація поетапного захисту інформації. Природно, коли противник буде намагатись знайти найбільш слабку частину у комплексі захисту, щоб з найменшими витратами дістатися до інформації. А значить, і законні користувачі повинні враховувати цю ситуацію у своїй стратегії захисту: безглуздо удосконалювати якусь частину захисного комплексу, якщо є свідомо більш слабкі місця ("принцип рівноміцності захисту"). Розробка хорошого шифру справа трудомістка. Тому бажано збільшити час життя хорошого шифру і використовувати його для шифрування як можна більшої кількості повідомлень.

Опис RSA було опубліковано в 1977 році Рональдом Райвест (Ronald Linn Rivest), Аді Шамір (Adi Shamir) і Леонардом Адлеманом (Leonard Adleman) з Массачусетського Технологічного Інституту (MIT).

Британський математик Кліффорд Кокс (Clifford Cocks), який працював в центрі урядового зв'язку (GCHQ) Великобританії, описав аналогічну систему в 1973 році у внутрішніх документах центру, але ця робота не була розкрита до 1977 року і Райвест, Шамір і Адлеман розробили RSA незалежно від роботи Кокса.

У 1983 році MIT був виданий патент 4405829 США, термін дії якого закінчився 21 вересня 2000 року.

На 2011 рік система шифрування на основі RSA вважається надійною, починаючи з розміру N у 1024 біта.

Система RSA використовується для захисту програмного забезпечення й у схемах цифрового підпису. Також вона використовується у відкритій системі шифрування PGP.

Із-за низької швидкості шифрування (близько 30 Кбіт / с при 512 бітному ключі на процесорі 2 ГГц), повідомлення зазвичай шифрують за допомогою більш продуктивних симетричних алгоритмів з випадковим ключем (сеансовий ключ), а за допомогою RSA шифрують лише цей ключ.

§1 Постановка задачі

У початковій формі криптосистема потребує виконання двоетапного порядку дій.

Перший етап – генерація ключів, що включає у себе наступні дії:

1) вибираються два великих простих числа (порядку 1024-2048 біт) p,q;
2) обчислюємо їх добуток $n = pq$;
3) обчислюємо функцію Ейлера $\varphi(n) = (p-1)(q-1)$;
4) вибираємо ціле число, що задовольняє наступним вимогам: $1 < e < \varphi(n)$, $НОД(e, \varphi(n)) = 1$;
5) находимо таке число, що $ed = 1 (\mathrm{mod}\, \varphi(n))$.

Пара чисел (e,n) називається відкритим ключем (або відкритою частиною ключа), а число d – закритим ключем (або закритою частиною ключа).

Другий етап – це шифрування або дешифрування повідомлення, що містить у собі виконання наступних дій:

1) для того, щоб зашифрувати повідомлення $m < n$, обчислюється шифротекст за формулою $c = m^e (\mathrm{mod}\, n)$;
2) для того, щоб розшифрувати текст $c < n$, обчислюємо початкове повідомлення за формулою $m = c^d (\mathrm{mod}\, n)$.

Всі докази можливості реалізації даних дій можна прочитати практично в будь-якій літературі по криптографії, де описаний алгоритм RSA зокрема криптосистеми з використанням відкритого ключа, у загальному.

Як бачимо, тут використовується лише степеневі функції. Ми ж пропонуємо брати не степеневі функції, а многочлени $T_n(k,x)$ з цілими коефіцієнтами, які по своїй суті є узагальненням степеневої функції.

Для шифрування і розшифрування ми будемо використовувати многочлени виду:

$$T_n(k,x) = C_1(k,x)\lambda_1^n(k,x) + C_2(k,x)\lambda_2^n(k,x), (n = 2,3,...), \quad (1.1)$$

Нехай вихідне повідомлення – це x, тоді зашифроване повідомлення буде:

$$y = T_m(b,x) (\mathrm{mod}\, pq), \quad (1.2)$$

А отримати вихідне повідомлення із отриманої раніше шифрограми можна за формулою:

$$x = T_n(a, y)(\mathrm{mod}\ pq) = T_n\left(a, T_m(b, x)\right)(\mathrm{mod}\ pq). \quad (1.3)$$

По-суті, необхідно виконання наступного відношення:

$$T_n\left(a, T_m(b, x)\right) = T_{nm}(c, x), (n = 2, 3, \ldots). \quad (1.4)$$

Головним завданням є отримання значень і можливі взаємозв'язки між параметрами $a, b, c, C_i(a, x), C_i(b, x), C_i(c, x), (i = 1, 2)$.

§2 Схема узагальненого криптоалгоритма RSA

Розглянемо многочлени $T_n(k,x)$, що будуть задовольняти умові кінцево-різницевого рівняння:

$$T_{n+2}(a,x) = axT_{n+1}(a,x) - T_n(a,x), (n = 2,3,...) \quad (2.1)$$

З деякими початковими умовами:

$$T_0(a,x), T_1(a,x). \quad (2.2)$$

Загальний розв'язок такого рівняння можна представити у вигляді:

$$T_n(a,x) = C_1(a,x)\lambda_1^n(a,x) + C_2(a,x)\lambda_2^n(a,x), (n = 2,3,...), \quad (2.3)$$

де

$$\lambda_{1,2}(a,x) = \frac{ax \pm \sqrt{a^2x^2 - 4}}{2} \quad (2.4)$$

Таким чином, ми отримуємо нашу початкову умову у наступному вигляді:

$$T_0(a,x) = C_1(a,x) + C_2(a,x) \quad (2.5)$$

$$T_1(a,x) = C_1(a,x)\lambda_1(a,x) + C_2(a,x)\lambda_2(a,x) \quad (2.6)$$

Нехай задані три послідовності $\{T_n(a,x)\}$, $\{T_n(b,x)\}$, $\{T_n(c,x)\}$, але так, що буде вірним наступне співвідношення:

$$T_n(a,T_m(b,x)) = T_{nm}(c,x), \ (n = 2,3,...) \quad (2.7).$$

Співвідношення (2.7) являється основою для здійснення процесів шифрування і розшифрування.

Але, для можливості виконання вказаних дій, для початку необхідно визначити всі параметри, при виконанні яких буде вірно (2.7).

Тобто, необхідно знайти вид і, як наслідок зв'язки між параметрами: $a,b,c,C_i(a,x),C_i(b,x),C_i(c,x),(i = 1,2)$.

З (2.1) – (2.4) слідує, що (2.7) можна представити у вигляді:

$$T_n(a,T_m(b,x)) = C_1(a,T_m(b,x))\left[\lambda_1^*(a,T_m(b,x))\right]^n + C_2(a,T_m(b,x))\left[\lambda_2^*(a,T_m(b,x))\right]^n, \quad (2.7^*)$$

де

$$\lambda_{1,2}^*(a,T_m(b,x)) = \frac{aT_m(b,x) \pm \sqrt{a^2T_m^2(b,x) - 4}}{2}. \quad (2.7^{**})$$

Сам процес шифрування і розшифрування найчастіше відбувається за участю ЕОМ. А для ЕОМ більш зручними арифметичними діями є операції додавання,

множення, піднесення до степеня. По-суті, вся робота зводиться до оперування цілими числами (мається на увазі біти, байти і т.д.). Тобто, необхідно якомога краще спростити вираз (2.7 **).

$$[T_m(b,x)]^2 = [C_1(b,x)\lambda_1^m(b,x) + C_2(b,x)\lambda_2^m(b,x)]^2;$$

$[T_m(b,x)]^2 = C_1^2(b,x)\lambda_1^{2m}(b,x) + C_2^2(b,x)\lambda_2^{2m}(b,x) + 2C_1(b,x)C_2(b,x)$, тут ми врахували, що $\lambda_1(b,x)\lambda_2(b,x)=1$.

Розглянемо наступний складений вираз з (2.7**):

$$[aT_m(b,x)]^2 - 4 = a^2C_1^2(b,x)\lambda_1^{2m}(b,x) + a^2C_2^2(b,x)\lambda_2^{2m}(b,x) + 2a^2C_1(b,x)C_2(b,x) - 4.$$

Будемо дотримуватись виконання умови:

$$a^2C_1(b,x)C_2(b,x)=1, \qquad (2.8)$$

тоді попередній вираз набуде вигляд:

$$[aT_m(b,x)]^2 - 4 = a^2C_1^2(b,x)\lambda_1^{2m}(b,x) + a^2C_2^2(b,x)\lambda_2^{2m}(b,x) - 2a^2C_1(b,x)C_2(b,x)\lambda_1^m(b,x)\lambda_2^m(b,x),$$

спростивши вираз, отримуємо:

$$[aT_m(b,x)]^2 - 4 = a^2[C_1(b,x)\lambda_1^m(b,x) - C_2(b,x)\lambda_2^m(b,x)]^2.$$

Тепер (2.7 **) з урахуванням отриманого результату буде виглядати так:

$$\lambda_{1,2}^*(a,T_m(b,x)) = \frac{aT_m(b,x) \pm a\left(C_1(b,x)\lambda_1^m(b,x) - C_2(b,x)\lambda_2^m(b,x)\right)}{2},$$

що в свою чергу дає можливість представити корені характеристичного рівняння у формі:

$$\lambda_1^*(a,T_m(b,x)) = aC_1(b,x)\lambda_1^m(b,x) \text{ і } \lambda_2^*(a,T_m(b,x)) = aC_2(b,x)\lambda_2^m(b,x). \qquad (2.9)$$

Рівняння (2.7) з урахуванням форм коренів (2.9) набуде вигляду:

$$\begin{aligned} &a^nC_1\left(a,T_m(b,x)\right)C_1^n(b,x)\lambda_1^{nm}(b,x) + a^nC_2\left(a,T_m(b,x)\right)C_2^n(b,x)\lambda_2^{nm}(b,x) = \\ &= C_1(c,x)\lambda_1^{nm}(c,x) + C_2(c,x)\lambda_2^{nm}(c,x) \end{aligned} \qquad (2.10)$$

Допустивши, що $C_1(b,x)=C_2(b,x)=\frac{1}{a}$, ми автоматично задовольняємо (2.8), знаходимо значення і взаємозв'язок поточних коефіцієнтів, а також спрощуємо (2.10):

$$\begin{aligned} &C_1\left(a,T_m(b,x)\right)\lambda_1^{nm}(b,x) + C_2\left(a,T_m(b,x)\right)\lambda_2^{nm}(b,x) = \\ &= C_1(c,x)\lambda_1^{nm}(c,x) + C_2(c,x)\lambda_2^{nm}(c,x) \end{aligned} \qquad (2.11)$$

Із (2.11) витікають наступні факти:

$$C_1(b,x)=C_2(b,x)=\frac{1}{a} \tag{2.12.1}$$

$$C_1(a,T_m(b,x))=C_1(c,x); \tag{2.12.2}$$

$$C_2(a,T_m(b,x))=C_2(c,x); \tag{2.12.3}$$

$$b=c \tag{2.12.4}$$

Таким чином. ми отримуємо три наступні многочлена, які дають апарат для здійснення дій шифрування і дешифрування даних з урахуванням умов (2.12.1) - (2.12.4):

$$T_n(a,x)=C_1(a,x)\lambda_1^n(a,x)+C_2(a,x)\lambda_2^n(a,x); \tag{2.13.1}$$

$$T_m(b,x)=\frac{1}{a}\lambda_1^m(b,x)+\frac{1}{a}\lambda_2^m(b,x); \tag{2.13.2}$$

$$T_n\left(a,T_m\left(b,x\right)\right)=C_1\left(a,T_m\left(b,x\right)\right)\lambda_1^n\left(b,T_m\left(b,x\right)\right)+C_2\left(a,T_m\left(b,x\right)\right)\lambda_2^n\left(b,T_m\left(b,x\right)\right). \tag{2.13.3}$$

Власне для шифрування ми будемо використовувати многочлен $T_n(a,x)$, а для дешифрування – многочлен $T_m(b,x)$.

Параметрами даної криптосистеми є величини: $a,b,C_1(a,x),C_2(a,x)$.

§3 Практична реалізація узагальненого алгоритму RSA

Якщо ми будемо оперувати даними типу цілих чисел, то відповідно необхідно описати отримані многочлени для того, щоб не виходити з множини цілих чисел.

Для шифрування будемо використовувати $T_m(b,x)=\frac{1}{a}\lambda_1^m(b,x)+\frac{1}{a}\lambda_2^m(b,x)$.

Для шифрування будемо використовувати $T_n(a,x)=C_1(a,x)\lambda_1^n(a,x)+C_2(a,x)\lambda_2^n(a,x)$.

Без сумніву, якщо ці операції призводять до вірного результату, то додаткова операція знаходження лишків по заданому модулю також даватиме вірний результат. Тобто, якщо вихідне повідомлення – це x, то зашифроване повідомлення буде отримано наступним чином:

$$y=T_m(b,x)(\mathrm{mod}\ pq)=\left(a^{-1}\lambda_1^m(b,x)+a^{-1}\lambda_2^m(b,x)\right)(\mathrm{mod}\ pq). \qquad (3.1)$$

Обернене значення зашифрованого повідомлення можна отримати за формулою:

$$x=T_n(a,y)(\mathrm{mod}\ pq)=\left(C_1(a,y)\lambda_1^n(b,y)+C_2(a,y)\lambda_2^n(b,y)\right)(\mathrm{mod}\ pq). \qquad (3.2)$$

Необхідно зауважити, що $nm=1\left(\mathrm{mod}\ HOK\left(\frac{p^2-1}{2},\frac{q^2-1}{2}\right)\right)$. (3.4)

Ознайомитись з доказом (3.4) можна у [5].

Виходячи з (3.4) ми суттєво ускладнюємо пошук секретного ключа, знаючи відкритий ключ.

Під час роботи ми багато разів робили акцент не тільки на збереженні криптостійкості запропонованого алгоритму, а й на збереженні швидкості необхідних обчислень. Для того щоб зберегти швидкість обчислень, ми пропонуємо наступні висновки:

для парної індексації $T_{2m}(k,x)=kT_m^2(k,x)-T_0(k,x)$; (3.5)

для непарної індексації $T_{2m+1}(k,x)=kT_m(k,x)T_{m+1}(k,x)-T_1(k,x)$. (3.6)

Параметри $a,b,C_1(a,x),C_2(a,x)$ можуть складати частину секретного ключа.

Висновки

Під час дослідження запропонованого алгоритму шифрування, були виявлені сильні сторони даного алгоритму перед вихідним алгоритмом RSA. Зокрема, наш алгоритм є узагальненням RSA і дає більш гнучку схему для оперування. Якщо раніше були використані степеневі функції, то тепер є можливість використовувати многочлени. Причому вид многочлена (2.3) показує, що досить багато параметрів може вплинути як на створення прямої функції шифрування, так і на створення оберненої функції знаходження вихідного повідомлення. Збільшення параметра, яким раніше була функція Ейлера, тепер дає більше стійку ситуацію до розкриття секретного ключа по відомому відкритому.

Також зазначені схеми (3.5) і (3.6) дають можливість не програвати у швидкості обчислення.

У цілому, описана вище криптосистема заслуговує уваги в плані практичного застосування, а також є хорошою базою для подальших досліджень у галузі захисту інформації.

Список літератури

1) Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. Handbook of Applied Cryptography. — CRC Press, October 1996. ISBN 0-8493-8523-7;
2) Венбо Мао. Современная криптография: теория и практика = Modern Cryptography: Theory and Practice. — М.: «Вильямс», 2005. — С. 768. — ISBN 0-13-066943-1;
3) Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: «Диалектика», 2004. — С. 432. — ISBN 0-471-22357-3;
4) Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Издательство ТРИУМФ, 2002 — 816с.:ил. ISBN 5-89392-055-4
5) В.А. Фильштинський, Л.А. Фильштинський, С.В. Фильштинський. Вступ до алгебри: Навчальний посібник. – Суми: ВВП «Мрія-1» ЛТД, 1999. - 208с.