МАТЕРІАЛИ ДРУКУЮТЬСЯ УКРАЇНСЬКОЮ, АНГЛІЙСЬКОЮ, ПОЛЬСЬКОЮ ТА РОСІЙСЬКОЮ МОВАМИ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

XII Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів

До 70-річчя заснування університету

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Частина 2

Львів – 2017

РЕДАКЦІЙНА КОЛЕГІЯ:

УДК 512.8

КВАДРАТИЧНІ ЛИШКИ. СИМВОЛИ ЛЕЖАНДРА ТА ЯКОБІ.

Кордунова Ю.
Стасюк М.Ф., канд. фіз.-мат. наук, доцент
Львівський державний університет безпеки життєдіяльності

Формування ключа для ймовірнісної модифікації криптографічної системи з відкритим ключем (Шафі Гольдвассер, Сільвіо Мікелі) вимагає вибору пари великих простих чисел p і q та псевдоквадрата a, який генерується на основі поняття квадратичного лишку та символів Лежандра, Якобі.

Розглянемо конгруенцію

$$x^2 \equiv a \pmod{m}, \quad (a,m)=1. \tag{1}$$

Якщо конгруенція (1) має розв'язок для деякого x, то число a називається *квадратичним лишком* за модулем m, якщо ж конгруенція (1) не має розв'язків, то число a називається *квадратичним нелишком* за модулем m.

Для цілого a і непарного простого числа p символ Лежандра означується як

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{якщо } a \text{ є квадратичним лишком за } \bmod m,\\ -1, & \text{якщо } a \text{ є квадратичним нелишком за } \bmod m.\end{cases}$$

Нехай p – непарне просте число, а a_1, a_2 – цілі числа. Тоді символ Лежандра має такі властивості [1].

1. Якщо $a_1 \equiv a_2 \pmod{p}$, то $\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right)$.

2. Мультиплікативність: $\left(\frac{a_1 \cdot a_2}{p}\right)=\left(\frac{a_1}{p}\right)\cdot\left(\frac{a_2}{p}\right)$.

3. $\left(\frac{a_1 \cdot a_2^2}{p}\right)=\left(\frac{a_1}{p}\right)$, якщо a_2 не ділиться на p.

4. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, \text{ якщо } & p=4m+1,\\ -1, \text{ якщо } & p=4m+3.\end{cases}$

5. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{якщо } p=8m+1 \text{ або } p=8m+7,\\ -1, & \text{якщо } p=8m+3 \text{ або } p=8m+5.\end{cases}$

6. Квадратичний закон взаємності. Якщо p, q – прості непарні, то

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Нехай $n\geq 3$ – непарне число з розкладом на прості множники $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ і a – ціле. Тоді символ Якобі, який є узагальненням символу Лежандра означується як $\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{\alpha_1}\cdot\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_s}\right)^{\alpha_s}$, де множники в правій частині є символами Лежандра.

Зауважимо, що ціле число a, для якого $\left(\frac{a}{n}\right)=1$ для непростого n, проте конгруенція $x^2\equiv a\pmod n$ не має розв'язків, називається *псевдоквадратом.*

Приклад. Згенеруємо відкритий ключ n,a ймовірнісної криптографічної системи. Для ілюстрації виберемо прості числа $p=47,\ \ q=89$. Тоді $n=47\cdot 89=4183$. Для знаходження числа a виберемо випадкові нелишки a_1,a_2 за модулями 47 і 89 відповідно.

Нехай $a_1=5,\ \ a_2=3$. Перевіримо, що a_1 – нелишок за модулем 47, використовуючи властивості символу Лежандра. Маємо

$$\left(\frac{5}{47}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{47-1}{2}}\left(\frac{47}{5}\right)=\left(\frac{5\cdot 9+2}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{25-1}{8}}=-1.$$

Аналогічно для a_2 отримаємо

$$\left(\frac{3}{89}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{89-1}{2}}\left(\frac{89}{3}\right)=\left(\frac{29\cdot 3+2}{3}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{9-1}{8}}=-1.$$

Тоді для числа a яке справджує системі конгруенцій $a\equiv a_1\pmod{47},\ \ a\equiv a_2\pmod{89}$ маємо

$\left(\frac{a}{4183}\right)=\left(\frac{a_1}{47}\right)\cdot\left(\frac{a_2}{89}\right)=(-1)\cdot(-1)=1$, тобто число a – псевдоквадрат.

Розв'язуючи систему конгруенцій $a\equiv a_1\pmod{47},\ \ a\equiv a_2\pmod{89}$ з допомогою китайської теореми про лишки, отримуємо другий елемент відкритого ключа $a=804$.

Література

1. Вербіцький О.В. Вступ до криптології / О.В.Вербіцький. – Львів.: ВНТЛ, 1998. – 246с.