35. Дайте характеристику та обґрунтуйте вимоги до ключової пари для RSA перетворення?

Генерування асиметричної ключової пари. Система RSA відноситься до криптосистем з відкритими ключами. В цій системі ключі $E_k \neq D_k$, причому один з них має бути особистим, а другий – відкритим. Наприклад, E_k – особистий, а D_k – відкритий, якщо вони використовуються для ЕЦП і навпаки, якщо використовуються для направленого шифрування.

Усі параметри (N,P,Q) також поділяються на 2 класи: N – відкритий, P,Q – конфіденційні (секретні).

Сутність забезпечення моделі взаємної недовіри – кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Користувач також забезпечує цілісність і дійсність відкритих ключів.

E_k, D_k – мають вибиратися з повної множини випадково, порівняно ймовір-
но і незалежно, мають забезпечувати однозначну оборотність прямого та зворотного перетворення. Відповідним чином засвідчений відкритий ключ є сертифікатом.

Значення E_k, D_k для практичних використань мають задовольняти умову

$$1 \le E_K, D_K < \varphi(N),$$

де

$$\varphi(N) = \varphi(P*Q) = \varphi(P)*\varphi(Q) = (P-1)(Q-1).$$

Порівняння (1.54) можна звести до Діафантового рівняння:

$$ax+by=1. \qquad (10.9\ \ 1.56)$$

Це діафантове рівняння – нормоване, тому що справа коефіцієнт дорівнює 1; a, b – цілочисельні коефіцієнти, x, y – невідомі. Порівняння (10.7 1.54) можна подати у вигляді:

$$E_K D_K = k*\varphi(N)+1, \qquad (10.10\ \ 1.57)$$

k – деяке невідоме число.

Діафантове рівняння (10.9 1.56) має цілочисельне розв'язання, якщо a і b цілочисленні, і $a \ge b$, a і b взаємно прості. Подавши (10.10 1.57) у вигляді

$$\varphi(N)*(-k) + E_K D_K = 1, \qquad (10.11\ \ 1.58)$$

отримаємо $a=\varphi(N)$, $x=(-k)$, $b=E_k$, $y=D_k$.

Якщо E_k сформувати випадково, то a та b – відомі числа, а x та y – невідомі, що підлягають визначенню.

Найбільш швидке розв'язання (10.11 1.58) дає застосування ланцюгових дробів, які дозволяють визначити x та y як

$$\begin{cases} y = (-1)^{\mu} a_{\mu-1} \\ x = (-1)^{\mu+1} b_{\mu-1} \end{cases}, \qquad (10.12\ \ 1.59)$$

де μ – порядок ланцюгового дробу, *a* і *b* – параметри ланцюгового дробу.

Знаходимо параметри:

a/*b* подається у вигляді ланцюгового дробу

$$\frac{a}{b} = r_0 + \cfrac{1}{r_1 + \cfrac{1}{r_2 + \cfrac{1}{r_3 + \cfrac{\dots}{\cfrac{1}{r_\mu + 0}}}}}, \qquad (10.13\ \ 1.60)$$

μ - порядок ланцюгового дробу, перший коефіцієнт, у якого залишок дорівнює 0.

Значення (a_0,b_0) та (a_1,b_1) визначаються як

$$\frac{a_0}{b_0} = r_0 = \frac{r_0}{1} \qquad \left.\begin{matrix} a_0 = r_0 \\ b_0 = 1 \end{matrix}\right\},$$

$$\frac{a_1}{b_1} = r_0 + \frac{1}{r_1} = \frac{r_0 r_1 + 1}{r_1} \qquad \left.\begin{matrix} a_1 = r_0 r_1 + 1 \\ b_1 = r_1 \end{matrix}\right\}.$$

Значення (a_2,b_2), (a_3,b_3) і т.д. визначаються рекурентно відповідно до правил

$$\begin{cases} a_\mu = r_\mu * a_{\mu-1} + a_{\mu-2} \\ b_\mu = r_\mu * b_{\mu-1} + b_{\mu-2} \end{cases}. \qquad (10.14\ \ 1.61)$$

Середнє число ітерацій в (1.60), тобто $\bar{\mu}$, можна визначити як [16]

$$\bar{\mu} = \frac{12 \ln 2}{\pi^2} \ln E_k .$$