37. Які вимоги до прямого асиметричного криптографічного перетворення типу НШ та з використанням якого ключа воно виконується?

На прикладі RSA

Згідно вимог нормативних документів та міжнародних стандартів в інформаційних технологіях повинні надаватися послуги причетності джерела та одержувача інформації (спостережливість). Причетність джерела, тобто авторство може бути забезпечено за рахунок застосування ЦП. Складніше забезпечити причетність одержувача. Ця задача може бути розв'язана за рахунок використання направлених шифрів.

Особливість крипто перетворень типу НШ:

пряме з використанням відкритого ключа $K_в$.

зворотне з використанням особистого ключа $K_о$.

Ключова пара ($К^о$, $К^в$) повинна бути випадковою та вибиратись із повної множини дозволених для використання ключових пар, причому

$$K_в \neq K_о$$

Відомий ряд методів побудування Криптографічних систем направленого шифрування. Основними з них є такі:

1) Метод складання рюкзака [ ]. Необхідно вкласти в рюкзак предмети з різною вагою, але щоб вага рюкзака залишалася постійною. Це не стійка система.

2) У 1978р. була опублікована стаття, у якій був запропонований алгоритм RSA направленого шифрування . Він закріплений в міжнародному стандарті ISO 11166-1,2. Крім того в США він закріплений в стандарті ANSI X10.31.

3) У 1985р. Єль - Гамаль запропонував нову схему НШ Є-Г. Всі ці алгоритми були запатентовані. На сьогодні рекомендовано до застосування стандарти X10.30 та у міжнародних стандартах ISO/IEC 1170-3 ISO/IEC 15946-10.

*Алгоритм направленного шифрування.*RSA криптоалгоритм є блоковим, у ньому повідомлення *M* розбивається на блоки M_i, з довжиною блоку $l_i \geq l_o$ (на сьогодні 2048 біт мінімум), реально 2048, 3072 і більше бітів. Блок криптограма C_i обчислюється за правилом

$$C_i = M_i^{E_K} (\mathrm{mod} N),$$

де E_k – є відкритий ключ прямого перетворення, *N* – модуль перетворення є добутком виду

$$N = P * Q,$$

де в свою чергу *P*, *Q* – великі прості, скоріше сильні, числа.

Якщо l_p є довжина простого числа *P*, наприклад в бітах, а l_q – довжина простого числа Q, то довжина модуля N

$$l_N = l_p + l_q.$$

Розшифрування блока криптограми здійснюється за правилом:

$$M_i = C_i^{D_K} (\mathrm{mod}\, N),$$

де $D_к$ – є ключ зворотного перетворення, тобто розшифрування $D^K = K^P$.

Однозначність розшифрування можна підтвердити, підставивши $M_i = C_i^{D_K} (\mathrm{mod}\, N)$,

в $C_i = M_i^{E_K} (\mathrm{mod}\, N)$. В результаті отримаємо:

$$M_i = M_i^{E_K D_K} (\mathrm{mod}\, N).$$

Оскільки ключова пара (E_K, D_K) пов'язана між собою порівнянням:

$$E_K D_K = 1(\mathrm{mod}\, \varphi(N)),$$

де $\varphi(N)$ є функцією Ойлера від модуля N

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

Якщо має єдине рішення, тобто існує єдина пара E_K, D_K, то такий шифр є однозначним і при таких умовах RSA криптосистема забезпечує однозначне направлене шифрування.

Зазначимо, що з точки зору забезпечення максимально можливої крипто-стійкості прості числа *P* і *Q* мають бути сильними в широкому або вузькому значенні. Так просте число *P* вважатимемо сильним в широкому значенні, якщо

$$P = 2R + 1,$$

де *R* – також велике просте число.

Аналогічно визначається і сильне в широкому значенні просте число *Q*.

Просте число *P* вважається сильним у вузькому значенні, якщо $P-1$ містить в своєму канонічному розкладі велике просте число *R*, *P*+1 містить в своєму розкладі велике просте число *S*, а крім того *R*-1 містить в своєму розкладі велике число *T*.