Нахождение закрытого ключа RSA по скомпрометированной паре ключей с тем же модулем

студент гр. 5057/2, Владимир Руцкий

29.03.2011

1 Постановка задачи

После компрометирования своего секретного ключа RSA криптограф создал новую пару ключей $(\mathrm{SK}, \mathrm{ePK})$, не перегенерировав модуль n. Необходимо найти "отмычку" для новых ключей.

Дано:

- Скомпрометированные старые ключи RSA криптографа SK', (ePK', n): $[M]_n^{\mathrm{ePK}' \cdot \mathrm{SK}'} = [M]_n$.
- Новый открытый ключ криптографа (ePK, n).

Найти: Секретный ключ для нового открытого ключа ePK криптографа SK: $[M]_n^{\mathrm{ePK} \cdot \mathrm{SK}} = [M]_n$ (он необязательно будет совпадать с секретным ключом криптографа).

2 Решение

Из алгоритма построения ключей RSA следует, что $\mathrm{ePK}' \cdot \mathrm{SK}' = 1 + t \cdot \varphi(n)$. Тогда можно вычислить $t \cdot \varphi(n) = \mathrm{ePK}' \cdot \mathrm{SK}' - 1 \neq 0$.

Вычислим $\gcd(t \cdot \varphi(n), \mathrm{ePK}) = c$. Т. к. $\varphi(n)$ и ePK взаимно просты по построению, то $c \nmid \varphi(n) \Longrightarrow c \mid t$.

Тогда $\frac{t \cdot \varphi(n)}{c} = t' \cdot \varphi(n), \quad t' \in \mathbb{Z}$, и

$$\gcd(t' \cdot \varphi(n), \mathrm{ePK}) = 1 = C_1 \cdot t' \cdot \varphi(n) + C_2 \cdot \mathrm{ePK} \Longrightarrow C_2 \cdot \mathrm{ePK} = 1 - C_1 \cdot t' \cdot \varphi(n),$$

а значит $\mathrm{SK} = C_2$ — секретный ключ для открытого ключа криптографа ePK.