

КОММЕНТАРИИ, КРИТИКА И ЗАМЕЧАНИЯ ПО СТАТЬЕ “КРИПТОСИСТЕМА RSA ПРОТИВ ВТФ”

Автор весьма признателен всем, кто помог уточнить формулировки и дать полезные замечания.

*Актуальная версия статьи размещена по адресу:
http://www.2000.ru/fermats/2000ru_vsm_rsa1a_01_04_2010.htm*

Форум: dxdy.ru

Замечание по сути, - критический пересмотр доказательной части статьи с более строгим (детальным) выводом полученного результата. (Наибольший общий делитель обозначается только скобками) .

===== 14.05.2010 г. =====

Пусть для простого $e > 2$

$$x^e + y^e = z^e \quad (1),$$

$$z > y > x > 0 \quad (2),$$

$$(x, y) = (x, z) = (y, z) = 1 \quad (3)$$

Пусть $(e, \varphi(x)) = 1$ (4).

Рассмотрим сравнения по $(\text{mod } x)$.

Введём обозначения $\bar{y} = y \pmod{x}$, $\bar{z} = z \pmod{x}$.

$$\text{Из (1) и (2)} \Rightarrow x+y > z \quad (5) \Rightarrow \bar{y} \neq \bar{z}.$$

Если $\bar{y} = \bar{z}$, то $x|(z-y)$, т.е. $(z-y) = kx$ для некоторого целого k ;

т.к. $z > y$, то $k \geq 1 \Rightarrow z - y \geq x$, что противоречит (5).

Следовательно и $\bar{y}^e \not\equiv \bar{z}^e \pmod{x}$, принимая во внимание (4) и фундаментальные основы RSA на базе функции Эйлера, можно условно считать, что \bar{y} и \bar{z} – (математические вычеты) являются исходными сообщениями для последующего шифрования, а \bar{y}^e и \bar{z}^e (вычеты степени e

по модулю x) – криптограммы. Результатом шифрования двух разных сообщений (с использованием одного и того же ключа шифрования) будут разные криптограммы.

$$\bar{y}^e = y^e \pmod{x}, \bar{z}^e = z^e \pmod{x}, \text{ а исходя из уравнения (1) } \Rightarrow$$

$\bar{y}^e \equiv \bar{z}^e \pmod{x}$. Налицо противоречие. Следовательно, невозможно выполнение (4) (в предположении существования примитивного решения уравнения Ферма). Т.е. доказано: $(e, \varphi(x)) = e$.

Аналогично доказывается $(e, \varphi(y)) = e$ (все выкладки проводятся с \pmod{y}).

Пусть $(e, \varphi(z)) = 1$ (6). Переходим к вычислениям по \pmod{z} .

Из (2) $\Rightarrow 2z > x+y > z$. Т.е. $\bar{x} + \bar{y} \not\equiv 0 \pmod{z} \Rightarrow \bar{x} \not\equiv z - \bar{y} \pmod{z}$.

$(z - \bar{y} - \text{это вычет } (-y) \text{ по } \pmod{z})$; приходится следить за знаками, поскольку работаем с приведённой системой вычетов: $0 \leq \bar{t} < z$). Вновь мы вправе рассчитывать на сохранение неравенства при возведении в степень $e \pmod{z}$. Помним, что мы предположили (6), тогда по подобию RSA:

$\bar{x}^e \not\equiv (z - \bar{y})^e \pmod{z}$, а это означает $\bar{x}^e \not\equiv -\bar{y}^e \pmod{z}$, (помним, что $e - \text{нечётно}$). Опять приходим к противоречию с $x^e + y^e \pmod{z^e}$, вытекающему из (1). Следовательно доказано: $(e, \varphi(z)) = e$.

Contact: 2000@2000.ru

S.M. Vakhterov, student, Moscow State Technical University n.a. N.E. Bauman

M.I. Vakhterov, editor

http://www.2000.ru/fermats/fermats_rsa_comments_vakhterov.htm

Last Modified: May, 14, 2010