

The RSA logo consists of the letters 'RSA' in a white, bold, sans-serif font, centered within a solid red rectangular background.

RSA

A gray rectangular box with a subtle gradient, containing the word 'ALGORITHM' in a bold, black, sans-serif font.

ALGORITHM

Криптографический алгоритм асимметричного шифрования

RSA

Private key

Public key



Криптографический алгоритм асимметричного шифрования

RSA

Функция Эйлера

$$\Phi = \{P - 1\} * \{Q - 1\} = \{3 - 1\} * \{7 - 1\} = 12$$

e:

1. Простое число ;

2. $< \Phi [12]$ 2 3 5 7 11

3. Взаимно простое с $[\Phi]$

Public key



21, e

x^3
7
—
21

- P

- Q

- mod

Криптографический алгоритм асимметричного шифрования

$$\{e, \text{mod}\} = \{5, 21\}$$

RSA

$$\Phi = 12$$

Функция Эйлера

$$\Phi = \{P - 1\} * \{Q - 1\} = \{3 - 1\} * \{7 - 1\} = 12$$

Public key



21, e

$$\begin{array}{r} \times 3 \\ 7 \\ \hline 21 \end{array}$$

- P

- Q

- mod

e = 5:

1. Простое число ;

{e, mod} – Открытый ключ

Криптографический алгоритм асимметричного шифрования

Открытый ключ

$\{e, \text{mod}\} = \{5, 21\}$

$X < \text{mod}\{21\}$

11

11 в 5

161 051

$161\ 051 \% 21 = 2$

$161\ 051 - 7669 * 21 = 2$

RSA

$3 * 7$
mod
21

Закрытый ключ

$\{d, \text{mod}\} = \{17, 21\}$

2

2 в 17

131 072

$131\ 072 \% 21 = 11$

$131\ 072 - 6241 * 21 = 11$

Криптографический алгоритм ассимитричного шифрования

220

220 / 2

110 / 2

55 / 5

11 – простое число

221

На 2 не делится

На 3 не делится

На 5 не делится

На 7 не делится

На 11 не делится

Лишь 13 дает ответ: $221 / 13 = 17$

Просты множители $13 * 17(\text{mod})$

Криптографический алгоритм асимметричного шифрования

Шифрование

Открытый ключ

$$\{e, \text{mod}\} = \{5, 377\}$$

ЕВРО

6, 3, 18, 16

$$6^5 \% 377 = 236$$

$$3^5 \% 377 = 243$$

$$18^5 \% 377 = 44$$

$$16^5 \% 377 = 139$$

236, 243, 44, 139

$$13 * 29 = 377 \text{ (mod)}$$

$$\varphi = (p-1)*(q-1) = 336$$

$$[d * e] \% \varphi = 1$$

$$[269 * 5] \% 336 = 1$$

Дешифрование

Личный ключ

$$\{d, \text{mod}\} = \{269, 377\}$$

236, 243, 44, 139

$$236^{269} \% 377 = 6$$

$$243^{269} \% 377 = 3$$

$$44^{269} \% 377 = 18$$

$$139^{269} \% 377 = 16$$

6, 3, 18, 16 - ЕВРО

Интернет

Криптографический алгоритм ассимитричного шифрования

Проблемы RSA шифрование по буквам:

1. Частые коды пробелов позволяют разбить шифровку на слова
2. Легко вычислить коды однобуквенных слов [а,в,р,л]
3. Недолгие пробелы вычисляются дополнительные буквы по коротким словам , типа “но”, “не”, “да”
4. По более длинным словам можно без труда восстаноить оставшиеся буквы.
5. Поэтому злоумышленнику не придется отгадывать ваши секретные ключи. Он вломает сообщение не зная их.

Криптографический алгоритм ассиметричного шифрования

Дополнительные алгоритмы шифрование

Каждая предыдущая часть сообщения начинает влиять на следующую

$$b := [b + a] \% \text{mod}$$

a – предыдущая часть сообщения; **b**-следующая

6.3.18.16

6-без изменений, т.к. $(6+0)\%377 = 6$

$$(3+6)\%377=9$$

6,9,27,46

$$(18+9)\%377 = 27$$

$$b := (b - a) \% \text{mod}$$

$$(16+27)\%377 = 43$$

Криптографический алгоритм асимметричного шифрования

Шифровщик

