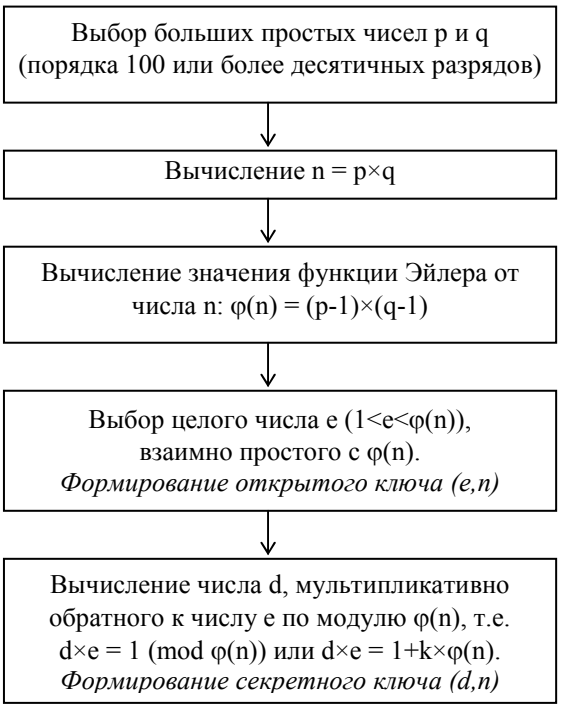
Основы криптографии с открытым ключом (асимметричной криптографии)

Общая схема шифрования с открытым ключом

Алгоритм RSA (Rivest, Shamir, Adleman)

Общая схема алгоритма RSA



Шифрование

Блок шифртекста C вычисляется посредством возведения блока открытого текста M в степень e по модулю n:

$C = M^e \pmod n$

Дешифрование

Блок открытого текста M вычисляется посредством возведения блока шифртекста C в степень d по модулю n:

$M = C^d \pmod n$

Пример использования алгоритма RSA (с малыми числами)

$p = 5; q = 11$

$n = p \times q = 55$

$\varphi(n) = (p-1) \times (q-1) = (5-1) \times (11-1) = 40$

$e = 7$

$d = 23$, поскольку $23 = (1+4 \times 40)/7$

Открытый ключ: (7,55) Секретный ключ: (23,55)

Шифрование посредством открытого ключа

Открытый текст: КОЛОКОЛ_ОКОЛО_КОЛОКОЛЬНИ:)

Таблица шифрования

Символ	Десятичный код (открытый текст) M	Десятичный код (шифртекст) $C = M^e \pmod n$	Символ	Десятичный код (открытый текст) M	Десятичный код (шифртекст) $C = M^e \pmod n$
И	01	1 (mod55) = 01	**Ь**	06	279936 (mod55) = 41
К	02	128 (mod55) = 18	**:**	07	823543 (mod55) = 28
Л	03	2187 (mod55) = 42	**)**	08	2097152 (mod55) = 02
Н	04	16384 (mod55) = 49	**_**	09	4782969 (mod55) = 04
О	05	78125 (mod55) = 25			

Открытый текст

К	О	Л	О	К	О	Л	_	…	К	О	Л	Ь	Н	И	:	)
02	05	03	05	02	05	03	09	…	02	05	03	06	04	01	07	08
18	25	42	25	18	25	42	04	…	18	25	42	41	49	01	28	02

Шифртекст

Дешифрование посредством секретного ключа

Шифртекст: 18 25 42 25 18 25 42 04 … 18 25 42 41 49 01 28 02

Таблица дешифрования

Десятичный код (шифртекст) C	Десятичный код (открытый текст) $M = C^d \pmod n$	Символ	Десятичный код (шифртекст) C	Десятичный код (открытый текст) $M = C^d \pmod n$	Символ
01	1 (mod55) = 01	**И**	41	1,241734376913948688227832002063 2e+37 (mod 55) = 06	**Ь**
18	74347713614021927913318776832 (mod 55) = 02	**К**	28	1,925904380037276068854119113162 8e+33 (mod 55) = 07	**:**
42	2,161392694157980082942258127284 5e+37 (mod 55) = 03	**Л**	02	8388608 (mod 55) = 08	**)**
49	7,490483309651862334944941026945 6e+38 (mod 55) = 04	**Н**	04	70368744177664 (mod 55) = 09	**_**
25	1,421085471520200371742248535156 3e+32 (mod 55) = 05	**О**			

Шифртекст

18	25	42	25	18	25	42	04	…	18	25	42	41	49	01	28	02
02	05	03	05	02	05	03	09	…	02	05	03	06	04	01	07	08
К	О	Л	О	К	О	Л	_	…	К	О	Л	Ь	Н	И	:	)

Открытый текст