RSA Algorithm Overview

RSA algorithm is used to encrypt and decrypt numbers. Original (unencrypted) number is called plaintext number (or just plaintext). Encrypted number is called ciphertext number (or just ciphertext).

Note that plaintext and ciphertext terms do not mean that the data is a text in common sense - the data is binary. We use plaintext number and ciphertext number to emphasize that the algorithm deals with numbers.

See https://cryptographyacademy.com/rsa/ for details.

Public and private Keys

Public key pk is a pair of numbers (n,e). Private key (also called secret key) sk is a pair of numbers (n,d). n, e, and d are calculated or selected as described below.

Assuming that p and q are two prime numbers, calculate $n = p \cdot q$ and $\phi(n) = (p-1) \cdot (q-1)$. Then select some number e so $3 \le e \le n-1$ and $\gcd(e, \phi(n)) = 1$.

Finally, compute d that is the modular multiplicative inverse of e, so $e \cdot d \bmod \phi(n) = 1$. The inverse is calculated as $d = \lambda \bmod \phi(n)$, where λ is a result of extended Euclidean algorithm equation $e \cdot \lambda + \phi(n) \cdot \mu = \gcd(e, \phi(n))$.

See https://brilliant.org/wiki/bezouts-identity/ for more information about the Euclidean algorithm. See https://www.geeksforgeeks.org/multiplicative-inverse-under-modulo-m/ for possible inverse code.

Encryption via public key, decryption via private key

Data encrypted via a public key can be decrypted only by somebody who has the matching private key.

- To encrypt via a public key $pk(n,e)$ calculate $C = M^e \bmod n$.
- To decrypt via a private key $sk(n,d)$ calculate $M = C^d \bmod n$.

© Copyright 2019 Kamilla Murashkina

Signing via private key, verification via public key

Notice - Signing/verification is not in scope of this assignment, this section is for information only.

Data encrypted via a private key can be decrypted by anybody (assuming that the public key is published). But the fact that the data can be decrypted via the public key proves that the data is encrypted by somebody who has the private key.

In practice, the message itself is not encrypted. Instead, a "fingerprint" of the message is calculated by applying some hash function to the message. The resulting fingerprint then encrypted via the private key and attached to the message.

Summary of algorithm parameters and variables

Parameter	**Calculated or selected as**	**Secret?**	**Description**
p	some large prime number	secret	large prime number
q	some large prime number not equal p	secret	large prime number
n	$p \cdot q$	public	crypto modulus
$\phi(n)$	$(p-1)\cdot(q-1)$	secret	Euler's phi function
e	some number that $3 \le e \le n-1$ and $\gcd(e, \phi(n))=1$	public	public exponent
d	$e \cdot d \bmod \phi(n) = 1$	secret	secret exponent, the inverse of e
pk	(n,e)	public	public key
sk	(n,d)	secret	private (secret) key
M	$M = C^d \bmod n$	secret	plaintext number
C	$C = M^e \bmod n$	public	ciphertext number

© Copyright 2019 Kamilla Murashkina