Encrypting a message with RSA

Authors

Luis Hernández Encinas, CSIC (Spain).
Agustín Martín Muñoz, CSIC (Spain).
Araceli Queiruga Dios, Universidad de Salamanca (Spain).

Type of activity

The example presents the application of algebra (specifically modular arithmetic and number theory modular arithmetic) to solve a simple message encryption problem using the RSA cryptosystem. This is a toy example, as the keys used are for illustrative purposes only, the real keys are much larger.

Target educational level

It can be addressed to last courses of High School students and to any university student from STEM degrees.

Initial information

Bob wants to allow anyone to send him secret messages. To do this, he uses the RSA algorithm, which relies on the difficulty of factoring large numbers. Alice, on her part, wants to send Bob a message securely.

Bob has generated his RSA key pair with the following parameters:

- Chosen prime numbers: $p = 7$ and $q = 17$.
- Public encryption exponent: $e = 5$.

Alice wants to send Bob the numerical message $M = 10$.

Source

Fuster Sabater, A., De La Guía Martínez, D., Hernández Encinas, L., Montoya Vitini, F., & Muñoz Masque, J. (2004). *Técnicas Criptográficas de Protección de Datos*. 3a Edición actualizada. Editorial Ra-Ma.

Hernández Encinas, L. (2005). *El criptosistema RSA*. RA-MA Editorial.

Problem statement

1. What is Bob's public key?
2. What is Bob's private key?
3. What is the ciphertext (C) that Alice will send to Bob?
4. How would Bob decrypt the message to obtain the original plaintext (M')?

Solution:

1. Bob's public key consists of two values: $(e, n) = (5{,}119)$, where $n = p \cdot q = 7 \cdot 17 = 119$. This is the key Bob shares publicly so anyone can encrypt messages for him.
2. Bob's private key consists of (d, n), where d is the decryption exponent. To find d, we need the Euler's totient function, $\emptyset(n)$, and d, the modular multiplicative inverse of e modulo $\emptyset(n)$, i.e., $e \cdot d \equiv 1 \pmod{\emptyset(n)}$.

   Calculation of $\emptyset(n) = (p-1)(q-1) = 6 \cdot 16 = 96$.

   Find d such that $5 \cdot d \equiv 1 \pmod{96}$. We can use the Extended Euclidean Algorithm, but for small numbers, we can test values or look for a multiple of 96 plus 1 that's divisible by 5. We find $d = 77$, which verifies that $5 \cdot 77 = 385 \equiv 1 \pmod{96}$.

   Thus, Bob's private key is $(77{,}119)$. Bob must keep this key secret.
3. Alice uses Bob's public key $(e, n) = (5, 119)$ to encrypt her message $M = 10$. The encryption formula is $C = M^e \pmod{n} = 10^5 \pmod{119} = 40$.
4. Bob receives the ciphertext $C = 40$ and uses his private key $(d, n) = (77{,}119)$ to decrypt it. $M' = C^d \pmod{n} = 40^{77} \pmod{119} = 10$.