

# An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics – Help page

Made by Asaf Yusuf & Roni Belkin

**If this is your first time here, WELCOME !**

[Important note –](#)

In our window we present a lot of parameters. To understand each of them and how they calculated thoroughly, please check our book - An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics.

[Explanation about The window-](#)

[RSA-information analysis –](#)

This window shows all the information about the values and results that had been used and measured in the running.

[Top of the window –](#)

The screenshot shows a window titled "RSA - Information analysis" with a yellow border. The window is divided into two main sections: "Encryption" and "Decryption".

**Encryption Section:**

- $p =$  283
- $q =$  347
- $e =$  13,823
- $d =$  16,643
- $N =$  98,201
- $Mx, My =$  ( 83,135 )
- $D =$  47,347
- $M =$  48,010
- $C =$  36,647
- Encryption time is : 4.914415 ( sec )
- Original RSA encryption time is : 0.000007 ( sec )

**Decryption Section:**

- $M =$  4,951
- $\varphi^{-1} =$  ( 83,135 )
- Decryption time is : 7.357103 ( sec )
- Original RSA decryption time is : 0.000012 ( sec )

- $p$  is a prime number that had been chosen randomly.
- $q$  is a prime number that had been chosen randomly.
- $N$  is a result of multiplication of  $p \cdot q$ .
- $e$  had been chosen randomly and must confirm the following  $\gcd(e, \text{lcm}(p+1, q+1)) = 1$ .
  - The  $e$  defines the number of iterations in the encryption.
- $d$  is a modular multiplicative inverse of an integer  $e$  -  $e^{-1} \text{ modulo } (\text{lcm}(p+1, q+1))$ .
  - The  $d$  defines the number of iterations in the decryption.

Left side of the Window (encryption)–

The screenshot shows a window titled "RSA - Information analysis". It contains two main sections: "Encryption" and "Decryption".

**Encryption Section (highlighted with a yellow box):**

- Inputs:  $p = 283$ ,  $q = 347$ ,  $e = 13,823$ ,  $d = 16,643$ ,  $N = 98,201$ .
- Output:  $Mx, My = (83, 135)$
- Intermediate value:  $D = 47,347$
- Result:  $M = 48,010$
- Encrypted message:  $C = 36,647$
- Encryption time: 4.914415 (sec)
- Original RSA encryption time: 0.000007 (sec)

**Decryption Section:**

- Input:  $M = 4,951$
- Intermediate value:  $\varphi^{-1} = (83, 135)$
- Decryption time: 7.357103 (sec)
- Original RSA decryption time: 0.000012 (sec)

- $M_x, M_y$  is an ordered pair that represent the message before the encryption. Those values will be encrypted, and they are point values over conic.
- $D$  is a non quadratic residue square.  $D$  is calculated by  $\frac{M_x^2 - 1}{M_y^2} \pmod{N}$ .
- $M$  is the result of parametrization on the point -  $M = \Phi(M_x, M_y) = \frac{M_x + 1}{M_y} \pmod{N}$ .
- $C$  is the result of using Rédei rational function -  $C = M^{\odot Pe} \pmod{N} = Q_e(D, M) \pmod{N}$ .
  - After this step the message  $M$  becomes an encrypted message  $C$ .

Note –

In the next two labels you will see the encryption running time result for RSA-like cryptosystem first, and then the encryption running time result for original RSA. This time measured in seconds.

Right side of the Window (decryption) –

The screenshot shows a window titled "RSA - Information analysis". At the top, there are input fields for parameters:  $p = 283$ ,  $e = 13,823$ ,  $N = 98,201$ ,  $q = 347$ , and  $d = 16,643$ . Below these, there are two main sections: "Encryption" and "Decryption". The "Encryption" section shows  $M_x, M_y = (83, 135)$ ,  $D = 47,347$ ,  $M = 48,010$ ,  $C = 36,647$ , and encryption times of 4.914415 sec and 0.000007 sec. The "Decryption" section, highlighted with a yellow border, shows  $M = 4,951$ ,  $\varphi^{-1} = (83, 135)$ , and decryption times of 7.357103 sec and 0.000012 sec.

- $M$  is the decryption result after getting the value of  $C$ .  $M$  is calculated as  $C^{\odot Pd} \pmod{N} = M$ , and then you get the decrypted message  $M$ .
- $\varphi^{-1}$  is the inverse parametrization of the message  $M$  to get the point values  $M_x, M_y$ . It is calculated as  $\Phi^{-1}(M) = \left( \frac{M^2 + D}{M^2 - D}, \frac{2M}{M^2 - D} \right) \pmod{N} = (M_x, M_y)$ .

Note –

In the next two labels you will see the encryption running time result for RSA-like cryptosystem first, and then the encryption running time result for original RSA. This time measured in seconds.