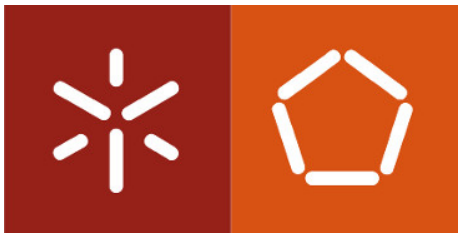
# Tecnologia Criptográfica

27 de Dezembro de 2020

**Trabalho Prático 5**


| | |
|---|---|
| a83899 | André Morais |
| a84485 | Tiago Magalhães |


## Teorema Chinês do resto & RSA




Mestrado Integrado em Engenharia Informática
Universidade do Minho

# Conteúdo

# 1 Introdução

No âmbito da Unidade Curricular de Tecnologia Criptográfica, o trabalho proposto era dividido em duas partes. Numa primeira, onde aplicamos o Teorema Chinês do resto e numa segunda parte onde tínhamos de decifrar uma mensagem através de um criptograma cifrado com cifra de chave pública (RSA)[1].

[1] *Rivest-Shamir-Adleman*, sistema de criptografia de chave pública

# 2 Primeira Parte - Teorema Chinês do resto

Para resolver um sistema de congruências lineares de acordo com o Teorema Chinês do resto são necessários os seguintes cálculos presentes na tabela 1, em que as congruências linear se encontram na seguinte forma $x \equiv b \mod n$.

Tabela 1: Tabela geral

| $b_i$ | $N_i$ | $x_i$ | $b_i \cdot N_i \cdot x_i$ |
|---|---|---|---|
| $b_1$ | $N_1 = n_2 \cdot n_3$ | $x_1$ | $b_1 \cdot N_1 \cdot x_1$ |
| $b_2$ | $N_2 = n_1 \cdot n_3$ | $x_2$ | $b_2 \cdot N_2 \cdot x_2$ |
| $b_3$ | $N_3 = n_1 \cdot n_2$ | $x_3$ | $b_3 \cdot N_3 \cdot x_3$ |

## 2.1 Sistema a)

Está apresentada na Tabela 2 as equações de onde obtemos $x_i$:

Tabela 2: Encontrar $x_i$

| | | |
|---|---|---|
| $621x_1 \equiv 1 \pmod{13} \Leftrightarrow$<br>$10x_1 \equiv 1 \pmod{13} \Leftrightarrow$<br>$x_1 \equiv 4 \pmod{13}$ | $351x_2 \equiv 1 \pmod{23} \Leftrightarrow$<br>$6x_2 \equiv 1 \pmod{23} \Leftrightarrow$<br>$x_2 \equiv 4 \pmod{23}$ | $299x_3 \equiv 1 \pmod{27} \Leftrightarrow$<br>$2x_3 \equiv 1 \pmod{27} \Leftrightarrow$<br>$x_3 \equiv 14 \pmod{27}$ |

Depois de calculado os $x_i$, preenchemos a tabela com os dados corretos:

Tabela 3: Tabela com resultados finais

| $b_i$ | $N_i$ | $x_i$ | $b_i \cdot N_i \cdot x_i$ |
|---|---|---|---|
| 48 | 621 | 4 | 119232 |
| 57 | 351 | 4 | 80028 |
| 39 | 299 | 14 | 163254 |

Por fim, sabendo que $N = \prod n_i$ , obtemos que $N = 8073$ e por isso conseguimos descobrir o valor de $x$:

Tabela 4: Calcular o valor de $x$

| |
|---|
| $x = 119232 + 80028 + 163254 = 362514$<br>$x \equiv 362514 \pmod{8073} \Leftrightarrow$<br>$x \equiv 7302 \pmod{8073}$ |

## 2.2 Sistema b)

Este sistema inicialmente não se encontra na forma do Teorema Chinês do resto($x \equiv b \mod n$) e por isso começamos por manipular o sistema de modo a aplicarmos os mesmos passos que no sistema anterior.

Queremos então as congruências lineares na seguinte forma: $x \equiv b \mod n$ .

Tendo $19x \equiv 21 \mod 16$ que se encontra na forma $ax \equiv b \mod n$, sabendo que 19 é relativamente primo com 16, o que significa que a equação anterior tem solução única, podemos obter a solução multiplicando ambos os membros pela inversa multiplicativa modular de $19 \mod 16$, sabendo que $19 \times 11 = 209$ e $209 \equiv 1 \mod 16$ (inversa multiplicativa modular $x \equiv a^{-1} \mod n$). O mesmo foi aplicado para a outra expressão, sendo assim temos :

Tabela 5: Manipulação congruências lineares

| | |
|---|---|
| $19x \equiv 21 \pmod{16} \Leftrightarrow$<br>$x \equiv 21 \times 11 \pmod{16} \Leftrightarrow$<br>$x \equiv 231 \pmod{16} \Leftrightarrow$<br>$x \equiv 7 \pmod{16}$ | $37x \equiv 100 \pmod{15} \Leftrightarrow$<br>$x \equiv 100 \times 13 \pmod{15} \Leftrightarrow$<br>$x_2 \equiv 1300 \pmod{15} \Leftrightarrow$<br>$x \equiv 10 \pmod{15}$ |

Depois de termos simplificado as congruências, seguimos os passos do sistema a) em que obtemos a Tabela 7, com os resultados finais.

Tabela 6: Encontrar $x_i$

| | |
|---|---|
| $15x_1 \equiv 1 \pmod{16} \Leftrightarrow$<br>$x_1 \equiv 15 \pmod{16}$ | $16x_2 \equiv 1 \pmod{15} \Leftrightarrow$<br>$x_2 \equiv 1 \pmod{15}$ |

Tabela 7: Tabela com resultados finais

| $b_i$ | $N_i$ | $x_i$ | $b_i \cdot N_i \cdot x_i$ |
|---|---|---|---|
| 7 | 15 | 15 | 1575 |
| 10 | 16 | 1 | 160 |

Sabendo que $N = \prod n_i$ , obtemos que N = 15 x 16 = 240, então:

Tabela 8: Calcular o valor de $x$

| |
|---|
| $x = 1575 + 160 = 1735$<br>$x \equiv 1735 \pmod{240} \Leftrightarrow$<br>$x \equiv 55 \pmod{240}$ |

# 3 Segunda Parte - Quebrar RSA

Na segunda parte deste trabalho foi-nos proposto que quebrássemos a instância de utilização do RSA proposta no enunciado, dado que a segurança do RSA reside no facto de o problema de factorizarão ser um problema difícil para inteiros com pelo menos 2048 bits, neste caso como o módulo é um número pequeno este será relativamente fácil de quebrar.

Utilizado o esquema de RSA apresentado na aula [1] e sabendo os valores do expoente $e$ e módulo $N$, uma vez que estes são públicos para cifragem e verificação. Segue-se os nossos passos para a resolução deste problema com objetivo a obter o valor do expoente $d$ de maneira a decifrar o criptograma.

## 3.1 Encontrar valores para os números primos $q$ e $p$

Através da expressão ($e \times d = t \times k - 1$), conseguimos descobrir o expoente $d$ que é o nosso objetivo, mas para isso temos várias variáveis desconhecidas. Para isso, necessitamos de saber $p$ e $q$. Como $N = p \times q$, construímos uma função em que obtivéssemos todos os números primos até $N$ e com estes descobrimos qual o produto de dois primos que resulta em $N$, obtendo $p = 419$ e $q = 509$.

$$n = p \times q = 419 \times 509 = 213271$$

## 3.2 Encontrar valor de $t$

Conhecendo os valores de $p$ e de $q$ conseguimos calcular o valor de t, a partir da função em baixo representada:

$$t = lcm(p-1, q-1) = \frac{(p-1)(q-1)}{gcd(p-1),(q-1)} = 106172$$

## 3.3 Encontrar valores para o expoente $d$

Conhecendo o valor de $t$, já é possível calcular $d$ :

$$e \times d = t \times k - 1 \Leftrightarrow d = 74945$$

## 3.4 Decifragem do criptograma

Para decifrar, sabendo que cada sequência de três letras/espaços foi mapeada para um número que depois foi cifrado com RSA , ou seja:

$$valor\_cifrado = (valor\_sequencia\_mapeada)^e \mod N$$

tivemos que aplicar:

$$valor\_decifrado = (valor\_cifrado)^d \mod N$$

Após isto, para conseguirmos obter as letras resolvemos a seguinte equação que mapeava as letras : $27^2 \times L1 + 27 \times L2 + 27 \times L3 = valor\_decifrado$ .

### 3.5 Texto final

LET US THEREFORE PERMIT THESE NEW HYPOTHESES TO BECOME KNOWN TOGETHER WITH THE ANCIENT HYPOTHESES WHICH ARE NO MORE PROBABLE LET US DO SO ESPECIALLY BECAUSE THE NEW HYPOTHESES ARE ADMIRABLE AND ALSO SIMPLE AND BRING WITH THEM A HUGE TREASURY OF VERY SKILLFUL OBSERVATIONS SO FAR AS HYPOTHESES ARE CONCERNED LET NO ONE EXPECT ANYTHING CERTAIN FROM ASTRONOMY WHICH CANNOT FURNISH IT LEST HE ACCEPT AS THE TRUTH IDEAS CONCEIVED FOR ANOTHER PURPOSE AND DEPART FROM THIS STUDY A GREATER FOOL THAN WHEN HE ENTERED IT FAREWELL

# 4 Conclusão

Dado como terminado este trabalho, este permitiu-nos aprofundar os conhecimentos obtidos nas aulas teóricas, percebendo melhor na prática o uso da cifra de chave pública.

Neste trabalho conseguimos observar uma das inseguranças do RSA que se torna inseguro quando o módulo não tem pelo menos 2048 bits. O facto do valor de expoente $d$ ser muito superior ao expoente $e$ deve-se a questões de eficiência de modo à cifragem e verificação ser o mais rápida possível e para permitir que o valor de $d$ seja maior e por isso mais difícil de se obter. Devido aos grandes valores para os expoentes $d$ e módulo $N$ o Teorema Chinês do resto permite uma otimização devido às congruências modulares.

# Referências

[1] Pereira, Óscar.(2020).Lecture Notes in Cryptography Engineering,pp. 37-38.Acedido em Dezembro 2020, em: https://randomwalk.eu/media/Teaching/TC/LecturesCE.pdf