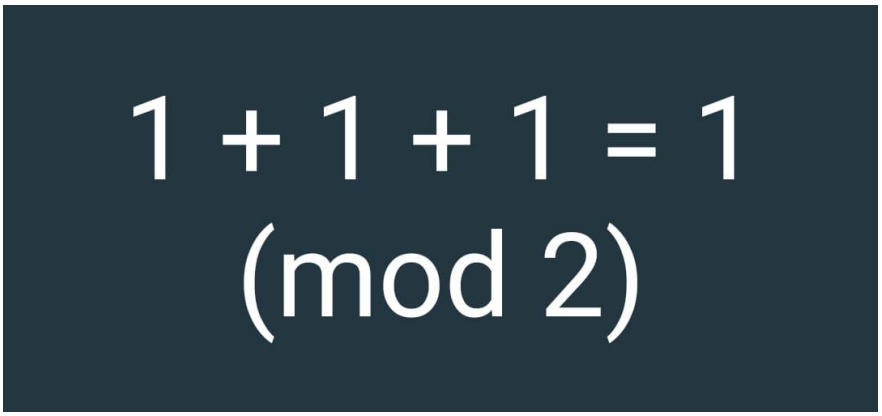
Universidade do Minho
Escola de Engenharia

Criptografia

TP5



João Miguel da Silva Alves (83624)

Paulo Jorge Alves (84480)

MESTRADO INTEGRADO EM ENGENHARIA BIOMÉDICA

INFORMÁTICA MÉDICA 2020/2021

Parte 1

Alínea a)

$$\begin{cases} x \equiv 48\ (mod\ 13) \\ x \equiv 57\ (mod\ 23) \\ x \equiv 39\ (mod\ 27) \end{cases} (=) \begin{cases} x = 48 + 13y \\ 48 + 13y \equiv 57\ (mod\ 23) \\ - \end{cases} (=) \begin{cases} - \\ 13y \equiv 9\ (mod\ 23) \\ - \end{cases}$$

$$(=) \begin{cases} - \\ y \equiv 6\ (mod\ 23) \\ - \end{cases} (=) \begin{cases} - \\ y = 6 + 23z \\ - \end{cases} (=) \begin{cases} x = 48 + 13 * (6 + 23z) \\ - \\ - \end{cases}$$

$$(=) \begin{cases} x = 126 + 299z \\ - \\ 126 + 299z \equiv 39\ (mod\ 27) \end{cases} (=) \begin{cases} - \\ - \\ 299z \equiv -87\ (mod\ 27) \end{cases} (=) \begin{cases} - \\ - \\ z \equiv 24\ (mod\ 27) \end{cases}$$

$$(=) \begin{cases} - \\ - \\ z = 24 + 27k \end{cases} (=) \begin{cases} x = 126 + 299 * (24 + 27k) \\ - \\ - \end{cases} (=) \begin{cases} x = 7302 + 8073k \\ - \\ - \end{cases}$$

Primeiramente, uma vez que x é congruente com 48 mod 13, logo pode ser escrito da forma apresentada a seguir: Depois ao substituir essa expressão de x na 2ª equação obtemos uma equação modular com a variável y. A passagem do 3º para o 4º sistema corresponde ao facto de necessitarmos de encontrar um valor que possa ser divisível por 13. Para tal, fomos somando 23 ao valor 9 até obter um número divisível por 13, que foi 78. Pode-se fazer isto, uma vez que o máximo divisor comum entre 13 e 23 é 1. De seguida, foi necessário descobrir a última variável z para se conseguir saber o valor de x. A estratégia foi igual à da usada para descobrir y. Mais uma vez, isto acontece porque o máximo divisor comum entre 299 e 27 é 1. Sabendo z, substituímos na equação e obtivemos x. Sendo k um número inteiro, logo o mínimo valor de x possível acontece quando k é igual a 0, dando um valor de x igual a 7302.

Alínea b)

$$\begin{cases} 19x \equiv 21\ (mod\ 16) \\ 37x \equiv 100\ (mod\ 15) \end{cases} (=) \begin{cases} x \equiv 7\ (mod\ 16) \\ - \end{cases} (=) \begin{cases} x = 7 + 16y \\ 37 * (7 + 16y) \equiv 100\ (mod\ 15) \end{cases}$$

$$(=) \begin{cases} - \\ 592y \equiv -159\ (mod\ 15) \end{cases} (=) \begin{cases} - \\ y \equiv 3\ (mod\ 15) \end{cases} (=) \begin{cases} - \\ y = 3 + 15z \end{cases}$$

$$(=) \begin{cases} x = 7 + 16 * (3 + 15z) \\ - \end{cases} (=) \begin{cases} x = 55 + 240z \\ - \end{cases}$$

Na alínea b fomos resolver em primeiro lugar a primeira equação. Usamos a estratégia da alínea a), ou seja, fomos somando 16 ao 21 até obter um valor que pudesse ser divisível por 19. Tal acontece, porque o máximo divisor comum entre 19 e 16 é 1. De seguida, substituímos a expressão de x na segunda equação e a mesma estratégia foi usada. Mais uma vez, pelo facto de o máximo divisor comum entre 592 e 15 é 1. Para obter o valor mínimo de x, bastou apenas substituir o valor de z por 0, visto que este é o menor número do conjunto dos números inteiros, dando o valor 55 para x.

Parte 2

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

Figura 1 – Texto limpo da parte 2 do trabalho prático 5.

Para resolver o problema descrito na segunda parte era preciso, inicialmente, descobrir o valor de d usado na primitiva RSA, uma vez que o texto apresentado corresponde ao criptograma e, por esse motivo, seria preciso saber o valor de d usado para decifrar o criptograma. Para podermos descobrir esse valor, tivemos de fatorizar o valor n, 213271. Sendo este valor pequeno é, portanto, fácil de fatorizar. Implementamos uma função que retorna uma lista com todos os fatores de um número dado como parâmetro (todo o código está devidamente comentado no ficheiro). De seguida aplicamos a expressão: **t = (p − 1) * (q − 1) / gcd(p − 1, q − 1)**, sendo p e q, os valores correspondentes aos dois fatores do número 213271, excluindo, obviamente, o valor 1 e o próprio valor. Os valores de p e q foram 419 e 509. De seguida, implementamos uma função que retorna o máximo divisor comum entre dois números passados como argumento. O máximo divisor comum entre 419 e 509 é 2. O valor de t obtido foi 106172. Sabendo o valor de t, estávamos aptos para usar a expressão **ed ≡ 1 (mod t)** para descobrir d. Para o fazer, recorremos à mesma estratégia usada na primeira parte do trabalho, obtendo para d, o valor de 74945.

Com o valor de d já estávamos aptos para decifrar todos os números do criptograma, usando a expressão **T = (int(num)**int(d))%int(n)**, sendo num, um valor qualquer do criptograma, d igual a 74945 e n igual a 213271, obtendo um valor que designamos como T.

Por fim, tivemos de a partir de cada valor de T que obtemos para cada valor do criptograma obter as letras consecutivas do texto limpo. Portanto, recorremos à expressão **$T=27^2L1 + 27L2 + L3$**. Através de uma análise mais atenta a esta expressão percebemos que L3 corresponde a (T mod 23), uma vez que T=27*(27L1 + L2) +L3. De seguida, depois de saber o valor de L3, passamos a ter $\frac{T-23}{27}$= 27L1 + L2. Logo, L2 = $\frac{T-23}{27}$ mod 27. Sabendo L2 e L3, bastou substituir na primeira expressão e saberíamos o valor de L1. No fim de saber os valores de L1, L2 e L3, passamos para as correspondentes letras já que as letras A-Z estão mapeadas para 0-25 com o caractere espaço a corresponder ao valor 26. Aplicamos esta estratégia a todos os valores do criptograma e conseguimos obter o texto limpo mencionado na figura 1.