Tutorial #6

João Freitas up202100373
Rui Gonçalves up202103077

O presente relatório tem como objetivo descrever o processo seguido para a resolução da ficha `Tutorial #6`, disponibilizada no âmbito da disciplina de Criptografia Aplicada. As seções numeradas em baixo representam cada um dos exercícios resolvidos.

RSA

1) Num sistema público RSA, é descoberta a mensagem cifrada `C=20`, enviada a um utilizador com a chave pública `(e = 13, n=77)`. Qual é o valor da mensagem original *M*?

Em RSA uma mensagem *M* é cifrada usando a chave pública `(e, n)` da seguinte forma: `C = M^e mod n`. A sua decifração é dado por `M = C^d mod n`. Visto isto, para obter a mensagem original *M* é necessário obter o valor de d, que pode ser deduzido da seguinte maneira:

```
d=(e^-1) mod φ(n)
φ(n) = (p-1)(q-1), sendo p e q os números primos usados na produção da chave privada.
```

2) Num sistema público RSA, a chave pública de um utilizador é `(e = 65, n = 2881)`. Qual a chave privada do utilizador `(d, n)`?

Como sabemos que `d=(e^-1) mod φ(n)`, então a chave privada é dado por:

```
(d, n)
= ((65^-1) mod φ(2881), 2881)
```

4) Suponha que o Bob utiliza o RSA com um grande valor *n*, cuja factorização não pode ser encontrada em tempo útil. A Alice envia a mensagem cifrada para o Bob contendo apenas o seu número de telemóvel. Esta operação é segura?

Como a mensagem original é bastante pequena (9 digitos), então a operação não é segura pois o número de hipóteses de descoberta por força bruta é também pequeno.