

# Códigos y Criptografía. Grado en Ingeniería Informática (2022)-Universidad de Valladolid

## Segunda entrega de ejercicios (10 % nota final)

Fecha de entrega: 22. diciembre 2022, hora: 23:59.

Se espera la resolución de los ejercicios en SageMath. Se deben entregar por email a la dirección [diego.ruano@uva.es](mailto:diego.ruano@uva.es) tanto la sesión de SageMath (ejecutable) como una impresión en pdf de dicha sesión. La resolución se debe acompañar de una breve explicación.

**Ejercicio 1** Considera un canal sin ruido que transmite bits (1's y 0's) y considera un alfabeto fuente en el que después de transmitir muchos símbolos, se ha hecho un estudio y se conoce la frecuencia (en tanto por uno) de cada símbolo.

- Implementa una función que tenga como input el alfabeto fuente y la frecuencia de cada símbolo y tenga como output una codificación trivial para este canal. ¿Cuáles el número medio de bits usados para transmitir un símbolo?
- Implementa una función que tenga como input el alfabeto fuente y la frecuencia de cada símbolo y tenga como output un código compresor óptimo (código Huffman) para este canal. ¿Cuáles el número medio de bits usados para transmitir un símbolo?

### Ejercicio 2

- Implementa una función que, dados dos primos  $p$  y  $q$ , calcule la clave pública y la clave privada del criptosistema RSA.
- Implementa una función que, dada la clave pública  $(n, e)$  de un criptosistema RSA y un mensaje en  $\mathbb{Z}_n$ , cifre dicho mensaje.
- Implementa una función que, dada la clave privada  $d$  de un criptosistema RSA y un mensaje cifrado con la función anterior, descifre dicho mensaje.

**Ejercicio 3** Ahora consideramos el mismo ejercicio que el número 2, pero con un cifrado en bloque de un texto. Es decir:

- Implementa una función que dada la clave pública de un criptosistema RSA y un texto  $M$  escrito con el alfabeto  $\mathbb{Z}_N$ , cifre dicho mensaje. Por ejemplo  $N$  puede ser igual a 256 y considerar el código ASCII. Nota: el tamaño del bloque será  $k$ , con  $N^k \leq n < N^{k+1}$ .
- Implementa una función que dada la clave privada de un criptosistema RSA y un texto cifrado con la función anterior, descifre dicho texto.

**Ejercicio 4** Vamos a considerar un ataque por fuerza bruta al criptosistema RSA y al criptosistema ElGamal:

- Implementa una función por fuerza bruta que dado  $n = p \cdot q$  producto de dos primos, factorice  $n$ . Es decir, encuentre  $p$  y  $q$ .
- Implementa una función por fuerza bruta que dada la clave pública  $(n, e)$  del criptosistema RSA, calcule  $\varphi(n)$ .
- Implementa una función por fuerza que dada la clave pública  $(n, e)$  del criptosistema RSA, calcule la clave privada  $d = e^{-1} \pmod n$ .
- Implementa una función por fuerza bruta que dados  $g, p$  y  $A$ , con  $g$  un generador de  $\mathbb{Z}_p^*$ , calcule el logaritmo discreto de  $A$  en base  $g$  modulo  $p$ :  $\log_g(A) \pmod p$
- ¿Hasta que tamaño del input las funciones anteriores son capaces de terminar?, ¿Hemos atacado con éxito los criptosistema RSA y ElGamal?

### Ejercicio 5

- Implementa una función que firme digitalmente un mensaje usando la firma digital con ElGamal y una función hash. Se puede usar cualquier función hash que el alumno quiera, en SageMath y Python está por ejemplo implementada la función `hash()`. Se puede truncar o reducir por un módulo el output de función hash. El input debe ser la clave privada de ElGamal (también son necesarios  $p$  y  $g$ ) y el mensaje a firmar. El output debe ser la firma.
- Implementa una función que dado un mensaje, una firma y una clave pública de ElGamal, compruebe si la firma del mensaje es válida o no, de acuerdo a la firma digital implementada con la función anterior.

**Ejercicio 6** Alice quiere enviar un mensaje a Bob por un canal inseguro y además quiere firmar dicho mensaje. Para ello supondremos que Alice sabe firmar un mensaje como en el Ejercicio 5 y que Bob tiene implementado un criptosistema de clave pública para recibir mensajes como en el Ejercicio 2.

- Implementa una función que firme digitalmente un mensaje usando la firma digital con ElGamal y una función hash. Y que además también cifre el mensaje usando RSA. El input debe ser la clave privada de Alice (de ElGamal), la clave pública de Bob (de RSA) y el mensaje a firmar. El output debe ser el mensaje cifrado y su firma.
- Implementa una función que dado un mensaje cifrado y una firma, descifre el mensaje y compruebe que la firma es válida, de acuerdo al método de la función anterior. El input debe ser la clave pública de Alice (de ElGamal), la clave privada de Bob (de RSA), el mensaje cifrado y la firma. El output debe ser el mensaje descifrado y un mensaje que nos diga si la firma era válida o no.

Este ejercicio es una aplicación directa del Ejercicio 2 y del Ejercicio 5. Por supuesto, deben usarse las funciones de estos ejercicios como funciones auxiliares para la resolución de este ejercicio.