# Códigos y Criptografía
# Grado en Ingeniería Informática

## Examen escrito 2 (10% nota final)
## 2020

**Fecha:** 01 diciembre 2020
**Hora:** 12:05–12:55
**Lugar:** Aula 101

**Ayuda permitida:** Cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ... No se permite ninguna ayuda de forma electrónica, salvo un ordenador portátil con un lector de ficheros pdf abierto, donde se puede consultar un libro electrónico o las pizarras de clase. En particular no debe tenerse abierto un explorador, SageMath o cualquier programa de email/mensajería. El wifi y datos deben estar desactivados.
Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras, teléfono móvil, tablets/pda, smartwatches, reproductores de música, ...

**Nota:** Todas las respuestas deben justificarse de forma razonada.

**Nota:** Escribe tu nombre y apellidos en todas las hojas que entregues.

**Nota:** El porcentaje al principio de cada ejercicio indica su valor en el examen.

**Ejercicios:** pueden encontrarse en la próxima página.

**Ejercicio 1.** *(25%)* Considera un canal sin ruido que transmite bits (1's y 0's) y considera el alfabeto fuente $\mathcal{A} = \{a, b, c, d, e\}$. Después de transmitir muchos símbolos, se ha hecho un estudio y se ha visto que la frecuencia (en tanto por uno) de cada símbolo a transmitir está dada por la siguiente tabla

| Símbolo | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| Frecuencia | 0.20 | 0.15 | 0.05 | 0.15 | 0.45 |

(a) Diseña una codificación trivial de los elementos de $\mathcal{A}$ para este canal. ¿Cuál sería el número medio de bits usados para transmitir un símbolo de $\mathcal{A}$?

(b) Diseña un código compresor óptimo de acuerdo a las frecuencias mencionadas en la tabla (pista: Código de Huffman).

(c) Usando el código compresor de la pregunta anterior: ¿Cuál es el número medio de bits usados para transmitir un símbolo de $\mathcal{A}$?

**Ejercicio 2.** *(40%)* Sean $p = 3$ y $q = 17$. Considera el criptosistema RSA dado por los primos $p$ y $q$, donde un mensaje es un número entre 0 y $pq - 1$.

(a) Muestra que $e = 3$ es un exponente de cifrado válido.

(b) Calcula el exponente de descifrado para $e = 3$.

(c) ¿Qué datos deben ser públicos y privados en este criptosistema?

(d) Cifra el mensaje $M = 8$ con la ayuda del exponente $e = 3$.

(e) Descifra el mensaje que has obtenido en la pregunta anterior.

Nota: $p, q, e$ y $M$ han sido escogidos de forma que no es necesario utilizar una calculadora u ordenador para resolver este ejercicio.

**Ejercicio 3.** *(10%)* Considera el cifrado de César (método de substitución desplazando 3 unidades) y cifra el siguiente mensaje: "EXAMEN FACIL".

**Ejercicio 4.** *(25%)* Alice y Bob quieren escoger una clave privada, pero sólo pueden comunicar a través de un canal inseguro. Por tanto, deciden usar el método de intercambio de claves de Diffie-Hellman con el primo $p = 11$ y $g = 2$, como elemento generador del grupo multiplicativo (no hace falta demostrar que $p$ es primo o que $g$ es un generador del grupo multiplicativo). Además, Alice escoge (al azar) el número $a = 4$ y Bob escoge (al azar) el número $b = 3$.

(a) Dibuja un esquema donde se vea que números se transmiten Alice y Bob para acordar la clave.

(b) ¿Cuál es la clave que acuerdan Alice y Bob?

Nota: $p, g, a$ y $b$ han sido escogidos de forma que no es necesario utilizar una calculadora u ordenador para resolver este ejercicio.