Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito 2 (10% nota final)
2021

Fecha: 02 diciembre 2021
Hora: 11:05–11:55
Lugar: Aula 8

Ayuda permitida: cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ...
No se permite ninguna ayuda de forma electrónica, salvo una sencilla calculadora y un ordenador portátil o tablet 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.
Preferentemente, se usará una calculadora de bolsillo. En el caso de no tener una calculadora de bolsillo, se podrá usar la calculadora de Windows/Linux.
Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras científicas avanzadas, teléfono móvil, tablets/pdas, smartwatchs, reproductores de música, . . .

Nota: la resolución de los ejercicios debe **justificarse** de forma **razonada**.

Nota: escribe tu nombre y apellidos y DNI/NIE en todas las hojas que entregues.

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

Ejercicios: pueden encontrarse en las próximas 2 páginas.

Ejercicio 1. *(25%)* Considera un canal sin ruido que transmite bits (1's y 0's) y considera el alfabeto fuente $\mathcal{A} = \{a, b, c, d, e, f\}$. 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	f
Frecuencia	0.10	0.20	0.15	0.34	0.12	0.09

(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. *(15%)* Considera un código de transposición cuya clave está dada por la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 6 & 7 & 1 \end{pmatrix}$$

y cifra el siguiente mensaje: "MATEMATICASDIVERTIDAS".

Ejercicio 3. *(30%)* Bob quiere enviar un mensaje a Alice. Dado que comunican a través de un canal inseguro, debe cifrar el mensaje para evitar que un espía lo obtenga. Alice y Bob deciden usar el criptosistema de ElGamal para cifrar el mensaje. Escogen trabajar módulo $p = 11$ con $g = 2$ como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generador del grupo multiplicativo).
El mensaje, que es un entero módulo p, que Bob quiere enviar a Alice es $M = 5$. La clave privada de Alice es 4.

(a) ¿Cuál es la clave pública de Alice?

(b) Bob cifra el mensaje M y se lo envía a Alice. Calcula el mensaje cifrado que Bob envía a Alice.

(c) Alice recibe el mensaje cifrado de Bob y procede a descifrarlo. Calcula como recupera Alice el mensaje M de Bob.

Nota: la respuesta de este ejercicio no es única porque Bob debe escoger un número al azar para el cifrado (que escoges tu).

Ejercicio 4. *(30%)* Alice quiere firmar un documento M y mostrárselo a Bob. Para ello deciden usar la firma digital basada en RSA con una función hash h. Alice escoge $p = 3$ y $q = 17$ como primos y como clave privada $d = 5$. El hash del documento a firmar tiene valor $h(M) = 3$.

(a) Muestra como Alice calcula la firma del mensaje M.

(b) ¿Cuál es la clave pública de Alice?

(c) Calcula como Bob comprueba la veracidad de la firma del mensaje M calculada en el apartado (a).