Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito. Primera convocatoria (60% nota final)
Curso 2021–2022

Fecha: 12 de enero de 2022
Hora: 16:00–20:00
Lugar: Aula 02

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 la próximas 4 páginas.

Ejercicio 1. *(15%)* Sea $C \subset \mathbb{F}_2^7$ el código lineal dado por la matriz generadora

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(a) Codifica $(1,1,1,1)$ usando C.

(b) Calcula una matriz de control del código C.

(c) Razona si las siguientes palabras de $\mathbb{F}_2^7$ pertenecen al código o no

- $(1,1,0,0,1,1,1)$.
- $(1,1,1,1,1,1,1)$.

(d) ¿Cuáles son los parámetros de C?

(e) ¿Cuántos errores puede detectar C?, ¿Cuántos borrones puede corregir C?, ¿Cuántos errores puede corregir C?

Ejercicio 2. *(5%)*

(a) Razona si puede existir un código lineal sobre $\mathbb{F}_7$ con parámetros $[5,2,5]$. En caso afirmativo, da la matriz generadora de un código con esos parámetros.

(b) Razona si puede existir un código lineal sobre $\mathbb{F}_7$ con parámetros $[5,2,4]$. En caso afirmativo, da la matriz generadora de un código con esos parámetros.

Ejercicio 3. *(5%)*

(a) Indica razonadamente que criptosistemas de clave pública, de los explicados en este curso con detalle, serían seguros frente a un ataque implementado con un ordenador cuántico con un número elevado de qubits.

(b) Considera que se quiere implementar uno de los criptosistemas nombrados en el apartado anterior. ¿Cuáles serían las ventajas y desventajas de cada uno de ellos?

Nota: Este ejercicio sólo vale el 5% de la nota. Se espera una respuesta muy breve. ¡No os enrolleis contestando!

Ejercicio 4. *(25%)* Cuatro personas P_1, P_2, P_3 y P_4 quieren votar de forma electrónica. Las votaciones posibles son ″si″ o ″no″, donde ″si″ es representado por 1 y ″no″ por 0. El resultado de la votación será la suma de los votos. Para ello, deciden usar un esquema de votación (con seguridad pasiva) basado en computación multiparte lineal a partir del esquema de Shamir módulo $p = 5$ para 4 personas en el que se necesita la información de al menos 2 personas para recuperar el secreto (es decir, una persona no puede recuperar el secreto).

P_1 y P_2 votan ″no″ y P_3 y P_4 votan ″si″. En este ejercicio debes hacer de *dealer* y escoger números al azar cuando corresponda.

(a) Describe y calcula la votación de acuerdo al método descrito en el enunciado.

(b) ¿Puede una persona, en general, saber que han votado los demás? ¿Pueden dos personas, que compartan los datos recibidos, saber que han votado los demás?

(c) ¿Cuál podría ser el resultado de la votación si una persona decide no seguir el protocolo y envía información errónea al resto?, ¿Podrían el resto darse cuenta?

Ejercicio 5. *(25%)* Alice quiere enviar un mensaje a Bob. 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 McEliece. Alice para su clave privada escoge el código $C \subset \mathbb{F}_5^3$ con parámetros $[3, 1, 3]_5$ dado por la matriz generadora

$$G = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix},$$

la matriz de permutación

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

y la matriz *scramble*

$$S = \begin{pmatrix} 2 \end{pmatrix}.$$

Nota: la matriz de permutación está dada por la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

(b) Bob quiere enviar el mensaje $\overrightarrow{m} = (2)$ a Alice. Calcula el cifrado del mensaje $\overrightarrow{m}$ con la clave pública de Alice, $\overrightarrow{c}$.

(c) Alice recibe y descifra $\overrightarrow{c}$, el mensaje enviado por Bob. Calcula dicho descifrado.

Ejercicio 6. *(25%)* Considera el esquema de distribución de claves cuántico BB84. Para ello consideramos que representamos las cuatro polarizaciones de BB84 usando la notación $-$, $|$, $/$, $\backslash$ vista en clase (que corresponde a $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ en los libros). Alice y Bob acuerdan enviar 8 fotones. También acuerdan que en el paso 7 del algoritmo, de los fotones que no son descartados en el paso 6 del algoritmo, van a anunciar públicamente la segunda mitad de bits (redondeando hacia abajo). Es decir, si por ejemplo hay 5 bits no descartados, entonces los 3 primeros bits se usan para la clave y los 2 últimos bits se anuncian públicamente en el paso 7 del algoritmo (hay una tabla al final del ejercicio para evitar confusiones).

Alice envía 8 fotones a Bob con la siguiente polarización:

$$- \ | \ / \ \backslash \ - \ | \ / \ \backslash$$

Y Bob usa rejillas con siguiente orientación:

$$- \ - \ / \ - \ - \ / \ / \ -$$

Consideramos primero la situación en la que no hay ningún espía:

(a) ¿Qué fotones son descartados en el paso 6 del algoritmo BB84?

(b) ¿Qué bits son publicamente anunciados por Alice y Bob en el paso 7 del algoritmo BB84?

(c) ¿Cuál es la clave acordada por Alice y Bob?

Consideramos ahora que Alice envía los mismos fotones y que Bob usa las mismas rejillas, pero ahora la espía Eve usa una rejilla para todos los fotones, excepto el primero (es decir, Eve espía los fotones 2, 3, . . ., 8), con la siguiente orientación (hay una tabla al final del ejercicio para evitar confusiones):

$$/ \ / \ / \ - \ - \ - \ -$$

(d) De los fotones que no son descartados en el paso 6 del algoritmo BB84, escribe todas las posibles resultados que obtiene Bob en su medición en el paso 3 del algoritmo BB84.

(e) De los fotones que no son descartados en el paso 6 del algoritmo BB84, escribe las posibles adivinaciones que hace Bob de los bits, de acuerdo a los posibles resultados del apartado (d).

(f) ¿En que casos se detecta a la espía Eve?, de acuerdo a los posibles resultados del apartado (d). ¿Cuál es la probabilidad de que la espía Eve sea detectada?

(g) Suponiendo que el el ataque de Eve no es detectado y de acuerdo a los posibles resultados del apartado (d), ¿Cuál es la clave acordada? ¿Es posible que la clave acordada sea diferente para Alice y para Bob? (y que por tanto el intercambio de clave falle sin que Alice y Bob lo detecten). ¿Cuál es la probabilidad de que el intercambio de clave falle?

Nota: para evitar confusiones, la siguiente tabla recoge la información proporcionada en el enunciado.

Fotones enviados por Alice	−	|	/	\	−	|	/	\
Rejilla espía Eve		/	/	/	−	−	−	−
Rejilla receptora Bob	−	−	/	−	−	/	/	−
Bits anunciados públicamente					SI		SI	