Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito. Primera convocatoria (60% nota final)
Curso 2020–2021

Fecha: 13 de enero de 2021
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 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. *(20%)* Considera el código lineal binario C dado por la matriz generadora

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

(a) Escribe todas las palabras del código C.

(b) ¿Cuales son los parámetros de C?

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

(d) Calcula el polinomio de pesos de C.

(e) Se tiene un canal donde la probabilidad de error de cada bit es $1/11$, y se usa el código C para codificar la información. ¿Cuál es la probabilidad de que se reciba una palabra código diferente a la palabra código enviada? (un error no detectable)

(f) ¿Es C un código auto-ortogonal?

Ejercicio 2. *(15%)* Sea C el código Reed-Solomon sobre $\mathbb{F}_5$ con longitud 3, dimensión 1 y cuyos puntos de evaluación son $x_1 = 0, x_2 = 1, x_3 = 2$.

(a) ¿Cuál es la capacidad correctora de C?

(b) Sea $\mathbf{r} = (0, 0, 1)$ una palabra recibida. Decodifica $\mathbf{r}$ usando el algoritmo de decodificación para códigos Reed-Solomon. Es decir, con la notación vista en clase y en el libro, calcula los polinomios Q_0 y Q_1 que dan el polinomio evaluador g.

(c) Justifica que se puede usar para C el algoritmo de decodificación en lista para códigos Reed-Solomon de forma que la capacidad correctora aumente. ¿Para que valor mínimo de ℓ (el tamaño máximo de la lista output) la capacidad correctora aumenta?

Nota: Se recalca que la pregunta (b) debe resolverse usando el algoritmo específico para códigos Reed-Solomon. Se considera este sencillo código y esta palabra recibida para que resolver el sistema lineal no tenga dificultad.

Ejercicio 3. *(5%)*

(a) Explica brevemente en que consiste un criptosistema de clave privada (o simétrica) y un criptosistema de clave pública (o asimétrica). Explica brevemente su uso en la práctica.

(b) Explica brevemente las implicaciones en criptografía de la existencia de un ordenador cuántico con un número suficientemente grande de q-bits.

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

Ejercicio 4. *(25%)* Alice quiere enviar un mensaje junto con su firma digital 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 ElGamal para cifrar el mensaje y el sistema de firma digital basado en ElGamal. Para ambos sistemas, 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 generadordel grupo multiplicativo). El mensaje, que es un entero módulo p, que Alice quiere enviar a Bob, junto con su firma digital, es $M = 7$.
Para mayor seguridad, deciden usar una función hash h para la firma digital, dicha función es pública. Para resolver este ejercicio no es necesario especificar la función hash h, es suficiente con saber que $h(M) = 4$.
Alice escoge azar 4 como clave privada para firmar el mensaje. Bob escoge al azar 5 como clave privada para que Alice le envíe el mensaje el cifrado.

(a) Explica con un esquema cual es el proceso de firma digital y de cifrado del mensaje. En particular, menciona que datos son públicos y que datos son privados (para Alice y para Bob). También menciona que datos son enviados por Alice a Bob y como descifra Bob el mensaje y comprueba la veracidad de la firma.

(b) Calcula la firma del mensaje $M = 7$ usando la clave privada de Alice.

(c) Calcula el cifrado del mensaje $M = 7$ usando la clave pública de Bob.

(d) ¿Qué envía Alice a Bob a través del canal inseguro de comunicación?

(e) Calcula como Bob descifra el mensaje y comprueba la veracidad de la firma.

(f) ¿Qué beneficio tiene usar una función hash en la firma digital?, o dicho de otra forma, ¿Qué tipo de ataque de un criptoanalista evitan al usar una función hash?

Nota: El esquema de la pregunta (a), si se desea, se puede hacer en varias partes según se va contestando a las siguientes preguntas.

Nota: la respuesta de este ejercicio no es única porque Alice debe escoger un número al azar (que lo escogéis vosotros) para el cifrado y otro para la firma digital.

Ejercicio 5. *(15%)* Considera el esquema de compartición de secretos de Shamir módulo $p = 5$ para 4 personas. Consideramos el caso 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).

(a) Genera unas participaciones para el secreto $S = 3$. En este ejercicio debes hacer de *dealer* (gestor ajeno) para repartir el secreto entre los 4 participantes. Recuerda: la respuesta no es única, dado que los coeficientes de grado positivo del polinomio evaluador se escogen al azar (por el *dealer*).

(b) Recupera el secreto S a partir de 2 participaciones calculadas en el apartado (a).

Ejercicio 6. *(20%)* 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 para los fotones pares las rejillas 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).

(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).

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

Fotones enviados por Alice	−	|	|	\	−	|	/	\
Rejilla espía Eve		−		−		/		−
Rejilla receptor Bob	−	/	−	/	−	/	−	/
Bits anunciados publicamente					SI			SI