Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito 2 (10% nota final)
2022

Fecha: 01 diciembre 2022
Hora: 11:05–11:55
Lugar: Aula 101

Ayuda permitida: cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ...
No se permite ninguna ayuda de forma electrónica, salvo 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	0.05	0.10	0.08	0.33	0.32	0.12

(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%)* Alice y Bob acuerdan comunicarse mediante el cifrado de Vernam y, para ello, han acordado usar la clave $K = 11110000$. Alice quiere enviar el mensaje $M = 10101010$ a Bob.

(a) Calcula el cifrado de M usando la clave K.

(b) Supongamos que Eve escucha la comunicación del mensaje cifrado. ¿Podría deducir alguna información del mensaje M? ¿Podrían Alice y Bob volver a usar la clave K?

Ejercicio 3. *(40%)* Sean $p = 5$ y $q = 11$. 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 $M = 4$ con la ayuda del exponente $e = 3$.

(e) Descifra el mensaje que has obtenido en el apartado anterior usando el algoritmo de los cuadrados repetidos para realizar la exponenciación modular.

Ejercicio 4. *(20%)* Alice firma documentos usando la firma digital basada en ElGamal con una función hash h con $p = 11$ 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). Su clave privada es $a = 5$.

Alice comete el error de firmar dos documentos públicos diferentes, M_1 y M_2, usando el mismo número aleatorio para la firma (k según la notación vista en clase). Más concretamente:

- Alice firma M_1, con $h(M_1) = 9$, obteniendo la firma $(r_1, s_1) = (7, 2)$.
- Alice firma M_2, con $h(M_2) = 2$, obteniendo la firma $(r_2, s_2) = (7, 1)$.

(a) Supongamos que Eve conoce los mensajes M_1, M_2 y sus respectivas firmas (r_1, s_1) y (r_2, s_2). Calcula como Eve obtiene la clave privada a de Alice a partir de esta información.

(b) ¿Qué consecuencia tiene esto para Alice?