Ejercicios:
Cifrado con clave pública

5.1) Antonio y Blanca necesitan compartir una clave de siete bits haciendo uso del protocolo Diffie-Hellman. Acuerdan como primo p = 101 y como generador de 9_{101} el valor α=11. Si Antonio elige como clave privada el valor a=17 y Blanca el valor b=20, ¿qué clave comparten?

5.2) Alice y Bob desean intercambiar una clave de sesión mediante el protocolo Diffie-Hellman. Para ello acuerdan un número primo p=503 y un generador α=399 de $\mathbb{Z}_{503}$. Alice genera aleatoriamente un número privado a=257 y Bob otro número privado b=320.
a) Comprueba que el generador se ha elegido correctamente.
b) ¿Qué valor envía Alice a Bob?
c) ¿Qué valor envía Bob a Alice?
d) ¿Qué clave comparten?

5.3) Sean p=13, q=17 y A={AB...NÑO...YZ} el alfabeto de textos en claro al que asignamos los números {2,3,....,27,28}.
a) Cifra la palabra CRIPTOGRAFIA utilizando clave pública e=11.
b) Descifra la secuencia numérica obtenida para recuperar la palabra original.

5.4) Consideremos un sistema de cifrado RSA en el que n=55 y e=7.
a) Cifra el número 10.
b) Factoriza n para obtener p y q y de esa manera descifrar el criptograma c=35.

5.5) En un criptosistema RSA en el que p=29 y q=31 descifra el número 126, sabiendo que la clave pública utilizada es e=17.

5.6) Cifra la palabra CRIPTOGRAFIA utilizando un criptosistema RSA cuya clave pública viene dada por los valores n = 943 (p = 41, q = 23) y e = 7, de manera que el agrupamiento de caracteres haga que el criptograma se pueda codificar con el mismo alfabeto que el texto en claro.
El alfabeto que se debe emplear es {A,B,...,N,Ñ,O,...,Z,_} con asignación numérica {0,1,...,27}.

5.7) Cifra la palabra CRIPTOGRAFIA utilizando un criptosistema RSA cuya clave pública viene dada por los valores n = 221 (p = 13, q = 17) y e = 11, de manera que el agrupamiento de caracteres haga que el criptograma se pueda codificar con el mismo alfabeto que el texto en claro.
El alfabeto que se debe emplear es {A,B,...,N,Ñ,O,...,Z,_} con asignación numérica {0,1,...,27}.
Descifra el criptograma obtenido para recuperar el mensaje original.

5.8) Supongamos que en una red de comunicación se utiliza RSA con agrupación óptima de letras y alfabeto

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	?
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Un usuario, con clave pública (n=1501, e=37), recibe el mensaje

c = AL?_KKAFR_V__KL_CTANI_S?

¿A qué texto en claro corresponde?

5.9) Alicia, Benito y Carlos son tres amigos que utilizan para comunicarse RSA con alfabeto de cifrado

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

y clave pública de cada uno de ellos:
Alicia ($n_A = 33$, $e_A = 7$), Benito ($n_B = 34$, $e_B = 5$), Carlos ($n_C = 35$, $e_C = 11$).
Alicia recibe el mensaje cifrado c = 22 30 29 20 08 con firma digital s=18. El remitente del mensaje ha firmado digitalmente la suma de los elementos del texto en claro módulo n_A.
a) ¿Qué mensaje en claro ha recibido Alicia?
b) ¿Puede saber cual de los dos amigos se lo ha enviado y estar segura de que no ha sido el otro?

5.10) En una red, Alicia desea enviar a Belén un mensaje m y firmarlo digitalmente. Para ello se uti-liza un algoritmo de clave pública en el que las funciones de cifrado y descifrado de Alicia son $\boldsymbol{E}_{k_A}$ y $\boldsymbol{D}_{k_A}$ y las de Belén son $\boldsymbol{E}_{k_B}$ y $\boldsymbol{D}_{k_B}$. El proceso seguido consiste en que Alicia cifra el mensaje $\mathbf{c} = \boldsymbol{E}_{k_B}(\mathbf{m})$, obtiene la firma digital $\mathbf{s} = \boldsymbol{E}_{k_B}\left[\boldsymbol{D}_{k_A}(\mathbf{m})\right]$ y envía los valores de c y s a Belén. ¿Qué proceso tiene que realizar Belén para descifrar c y comprobar que el mensaje es auténtico?

5.11) Explica, brevemente, por qué no se utiliza la criptografía de clave pública para el cifrado general de la información. ¿Qué alternativa se utiliza?

5.12) Explica, brevemente, por qué crees que en todos certificados con algoritmo RSA la clave pública e = 65537.

5.13) Si se desea utilizar un algoritmo para cifrar una videoconferencia (audio y video); explica, brevemente, qué tipo de algoritmo de entre los siguientes resultaría inadecuado: cifrado en flujo, cifrado en bloque simétrico, cifrado asimétrico.

5.14) Explica, brevemente, cuál es la principal ventaja de los criptosistemas de clave pública frente a los de clave secreta y el principal inconveniente.

5.15) Explica, brevemente, qué papel desempeñan las funciones hash en la firma digital.

5.16) Explica, brevemente, en qué consisten las características siguientes que debe cumplir una función hash para que se considere segura: unidireccionalidad, colisión fuerte.