PROBLEMA 1

		CUMPLE
A) a	ENTRADA CUALQUIER LONG	SI
b	SALIDA LONG FIJA	SI
c	DADO m ES FACIL CALCULAR $H(m)$	SI
d	" $H(m)$ NO PODEMOS ENCONTRAR UN m QUE LO GENERE	NO
e	NO ES POSIBLE $\exists$ DOS m QUE GENEREN MISMA $H(m)$	NO

B)
$$M = \begin{array}{r} 101010 \\ 101010 \\ 101010 \\ 100000 \end{array}$$

$H(M) = 001010$ (= 10 en decimal)

C) $N = pq = 143$ $\quad \boxed{P_A \equiv e_A = 23,\ N_A = 143}$ CLAVE PÚBLICA

$ed = 1 \bmod \phi(N) \Rightarrow d = 47$ $\quad \boxed{S_A \equiv d = 47}$ CLAVE PRIVADA

$\phi(N) = 120$ $\quad$ 1º ALG EULER EXTENDIDO

D) $M \,||\, E_{S_A}(H(M)) = M \,||\, 10^{47} \bmod 143 : \boxed{M \,||\, 43}$

MENSAJE FIRMADO: 101010101010101010 | 101011

+ AUTENTICIDAD ORIGEN / CONTENIDO (INTEGRIDAD)
+ NO REPUDIO (CON ARBITROS)

e] LA FORMA MAS EFICIENTE ES GENERAR UN MENSAJE QUE GENERE LA MISMA H(M)

p.e. M = 0 0 1 0 1 0

M' puede suplantar a M

PROBLEMA 2

a] $V_t(max) = W \log_2\left(1+\frac{S}{N}\right) = 9000$ bps

$I(min) = 10.000 \cdot H = 15.000$ bits

$H = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 = \frac{1}{2}+\frac{1}{2}+\frac{1}{2} = 1'5$

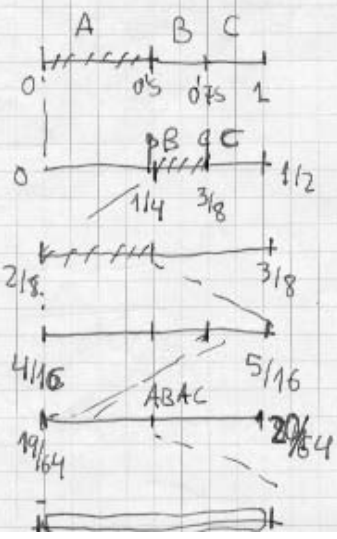
$t_{min} = \frac{I(min)}{V_t(max)} = \frac{15.000}{9.000} = \frac{5}{3}$ s

b]

A	0'5	0'5	0	A → 0
B	0'25	0'5	10	B → 10
C	0'25		11	C → 11

ABACAAA → 0 10011000

c]



ABAGA → $\left(\frac{38}{128} ; \frac{39}{128}\right)$

SEGMENTO $[0'296875 , 0'3046875]$

CUALQUIER PTO. DE ESTE SEGMENTO ES VÁLIDO

d]

RX:	0	0	1	1	4	2	6
SALIDA:	A	A	B	B	AB	C	BA
AÑADIR DICC:	—	AA	AB	BB	BA	BC	CB

DIC:

0	A	6	BA
1	B	7	BC
2	C	8	CB
3	AA		
4	AB		
5	BB		

SALIDA: A A BB AB C BA

e] FUENTE SIN MEMORIA

⇒ HUFFMAN O ARITMÉTICO LOS MÁS APROPIADOS

EN ESTE CASO, EN HUFFMAN $\bar{l} = H$, Y ES MÁS SENCILLO QUE EL ARITMÉTICO, POR LO QUE ES EL MÁS APROPIADO