(8) M = IDA | e_A | N_A | FD(M)

$certificado_A$ = 0001 | 0101 | 0010 0011 | 0011 1111 1011

$H(M) = 0 \oplus 0 \oplus 0 \oplus 0, 0 \oplus 1 \oplus 0 \oplus 0, 0 \oplus 0 \oplus 1 \oplus 1, 1 \oplus 1 \oplus 0 \oplus 1 = 0101 \equiv 5$ //

$FD(M) \equiv 1019 = (H(M))^{d_{CA}} \bmod N_{CA}$ $\quad N_{CA} = p_{CA} \cdot q_{CA} = 29 \cdot 37 = 1073$

$H(M) = (FD(M))^{e_{CA}} \bmod N_{CA} = 1019^{11} \bmod 1073 = 5$ //

$K_{PA} = (e_A, N_A)$ es auténtica, pues ese certificado lo firmó CA.

(9) $C_{B \to A} = (M_{B \to A})^{e_A} \bmod N_A$

Como $M_{BA} = 100 > N_A = 35$, hay que romper M_{BA} en submensajes binarios de longitudes igual al nº de bits necesarios para codificar N_A menos 1.

$N_A = 35 \equiv 100011 \rightarrow$ 6 bits $\rightarrow$ rompo M_{BA} en bloques de 5 bits

$M_{BA} = 100 \equiv 00011 | 00100$

$M_{BA1} = 3 \quad 4 = M_{BA2}$

$C_{BA1} = (M_{BA1})^{e_A} \bmod N_A = 3^5 \bmod 35 = 33$

$C_{BA2} = (M_{BA})^{e_A} \bmod N_A = 4^5 \bmod 35 = 9$

(10)

U N S
N O C
A C A
G A S
U Z W
I A W
L H W
A O W

UN AGUILA NO CAZA MOSCAS

(AQUILA NON CAPIT MUSCAS)