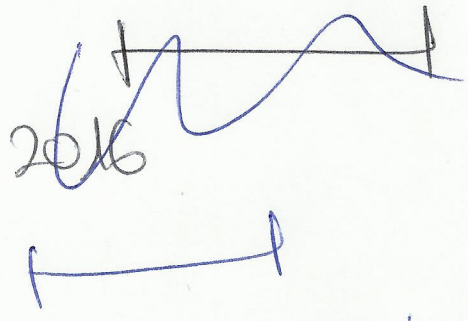
Mandamos

FIRMA

$m, K_A^-(HH(m))$

el mensaje lo manda normal y cifra privadamente el resumen del mensaje, para asegurarse que es de quien dice.

El receptor aplica K_A^+ sobre $K_A^-(HH(m))$ y aplica la func. hash (HH) sobre m, si son iguales, si sirve.



Caché - Control — PREFERENCIA SOBRE TODO.

Diffserv.

si el tráfico llega marcado, lleva lo de set_tc_index

si lo quiero marcar pq no viene marcado, pones dsmark.

la siguiente línea, el shift dice que te quedes con 6 bits, no 8.

Marcas con 8 bits

consultas con 6 bits.

$K_A^+ \Rightarrow$

K_A^-

$K_A^+(m)$ — mensaje cifrado con la clave pública

K_A^+, mensaje

$K_A^-(H(m))$ — resumen mensaje 256 bytes — cifrado con clave privada el resumen del mensaje

Firma

A emisor = m, $K_A^-(H(m))$

Receptor

m'

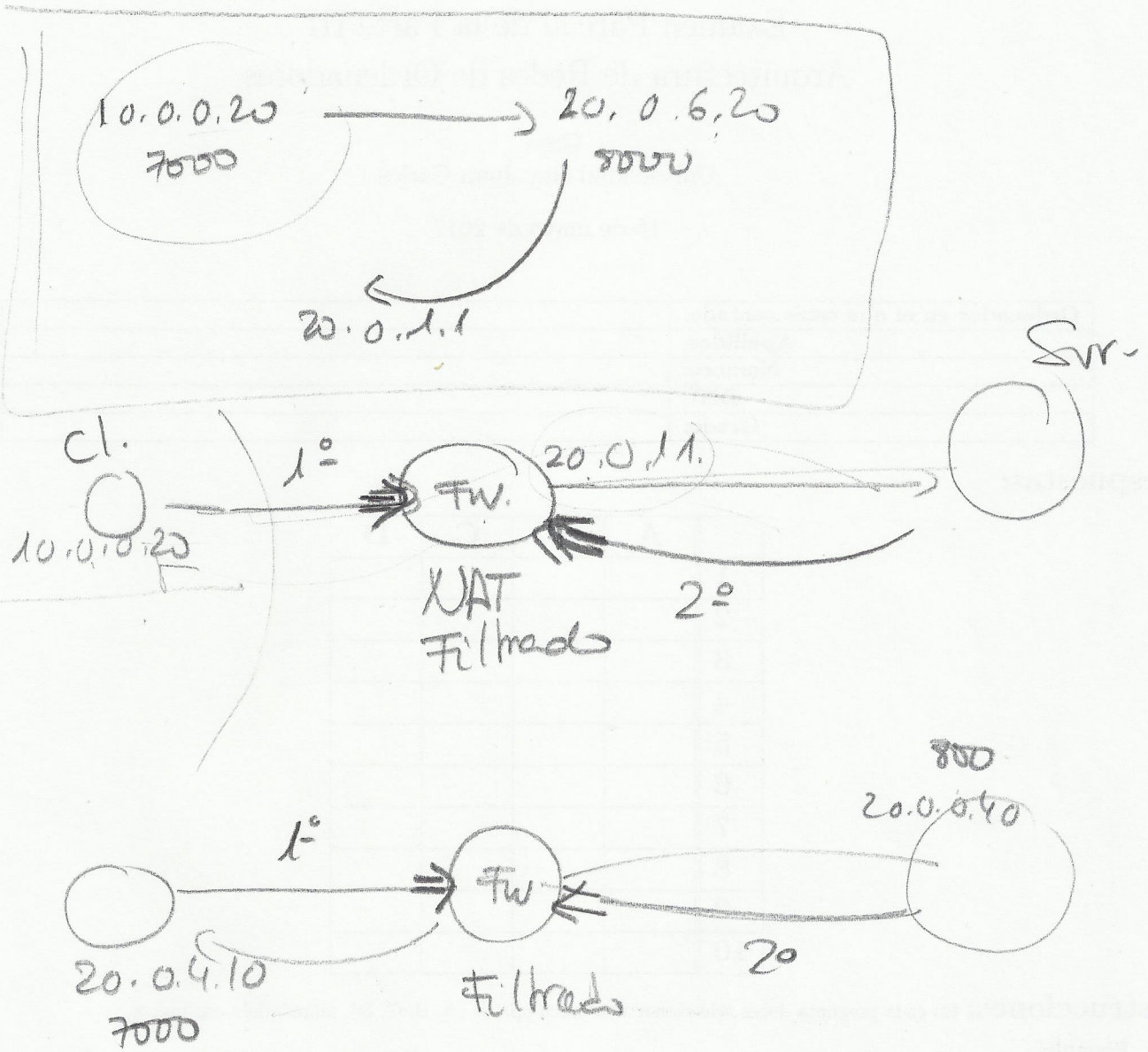
$K_A^-(H(m))$

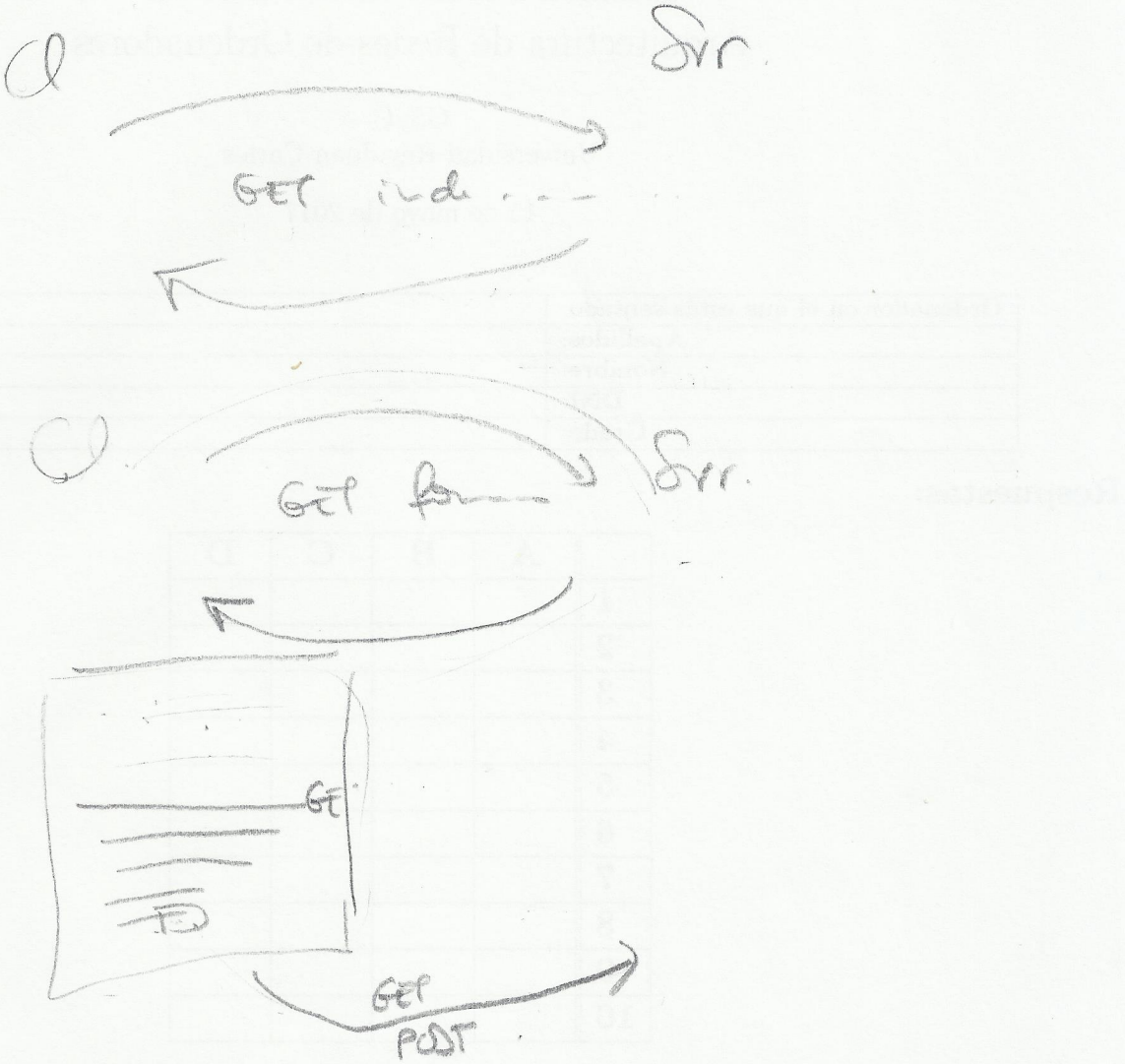
K_A^+

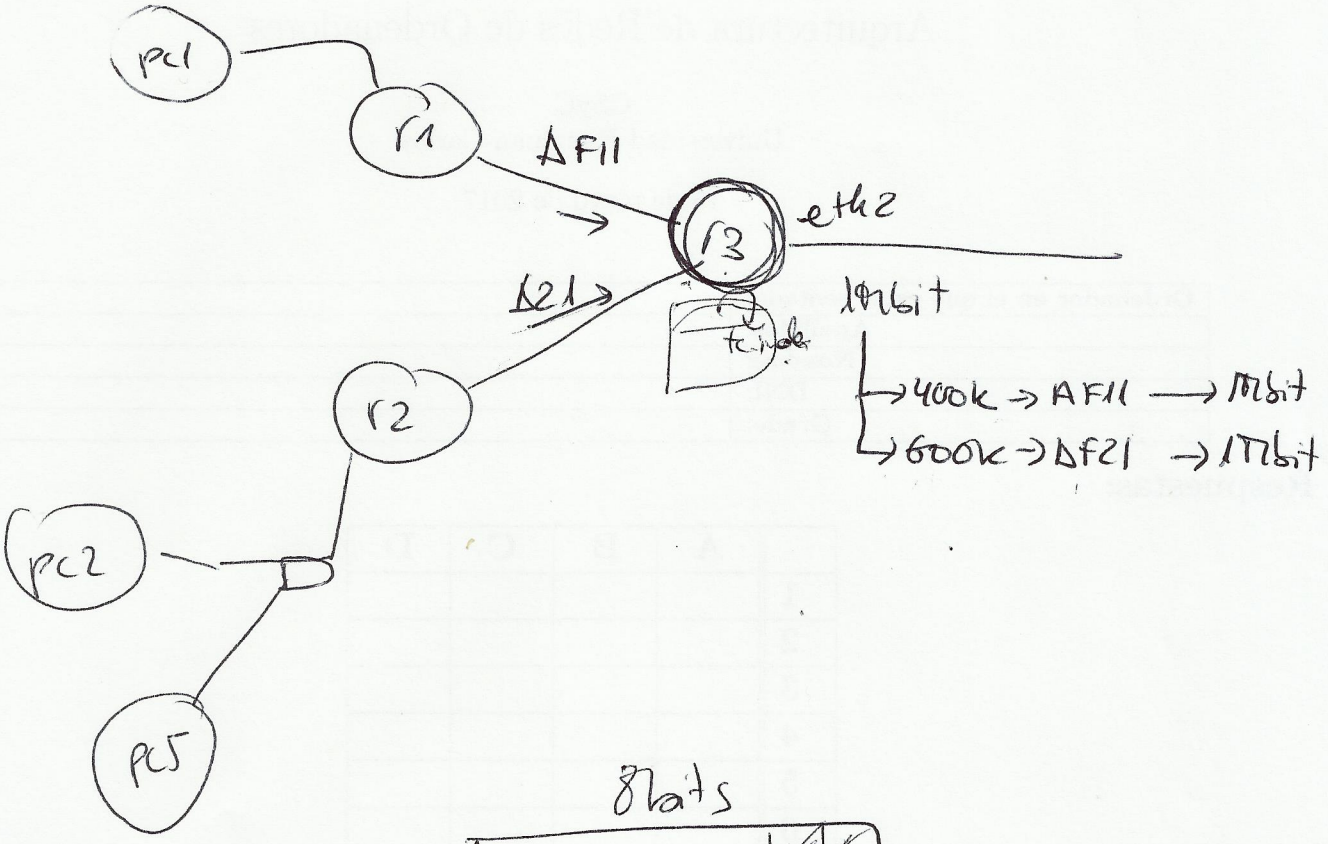
$H(m)$

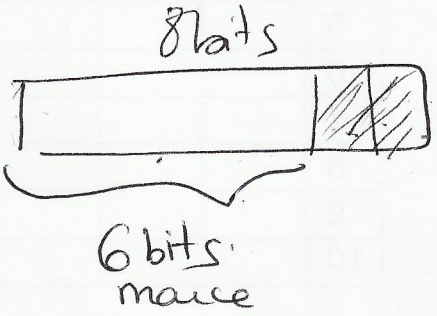
$K_A^+(K_A^-(H(m))) = H(m)$

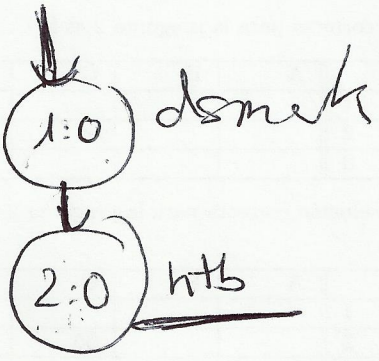
$= ??$


10.0.0.20
7000
20.0.6.20
8000
20.0.1.1
Svr.
Cl.
1º
FW.
20.0.1.1.
10.0.0.20
NAT
Filtrado
2º
800
20.0.0.40
1º
FW
20
20.0.4.10
7000
Filtrado


Cl
Svr
GET ind...
Cl
Svr.
GET for
Svr.
GET
POST
Cl
page1.html
SV1
2 img.
SV2
SV3
2 img
2 img
Cl.
SVM
GET
Cl
SV2
Cl
SV3
SVM


pc1
r1
AF11
r3
eth2
AF21
10Mbit
r2
400k → AF11 → 7Mbit
600k → AF21 → 17Mbit
pc2
pc5


8bits
6bits
mace


1:0
2:0
htb