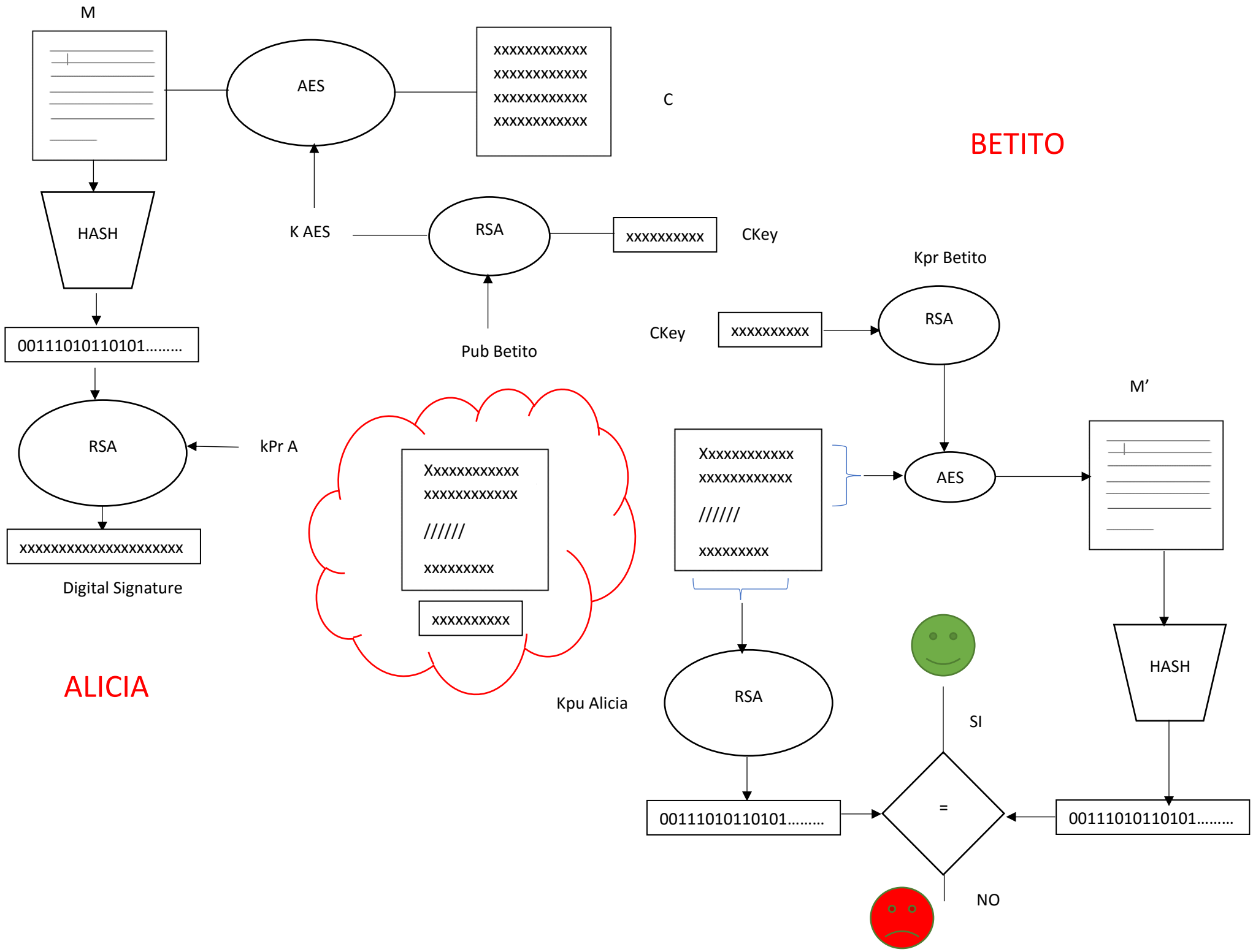
M
AES
xxxxxxxxxxxx
xxxxxxxxxxxx
xxxxxxxxxxxx
xxxxxxxxxxxx
C
BETITO
HASH
K AES
RSA
xxxxxxxxxx
CKey
Kpr Betito
00111010110101.....
Pub Betito
CKey
xxxxxxxxxx
RSA
M'
RSA
kPr A
Xxxxxxxxxxxx
xxxxxxxxxxxx
//////
xxxxxxxxx
xxxxxxxxxx
Xxxxxxxxxxxx
xxxxxxxxxxxx
//////
xxxxxxxxx
AES
xxxxxxxxxxxxxxxxxxxx
Digital Signature
ALICIA
Kpu Alicia
RSA
HASH
SI
=
00111010110101.....
00111010110101.....
NO