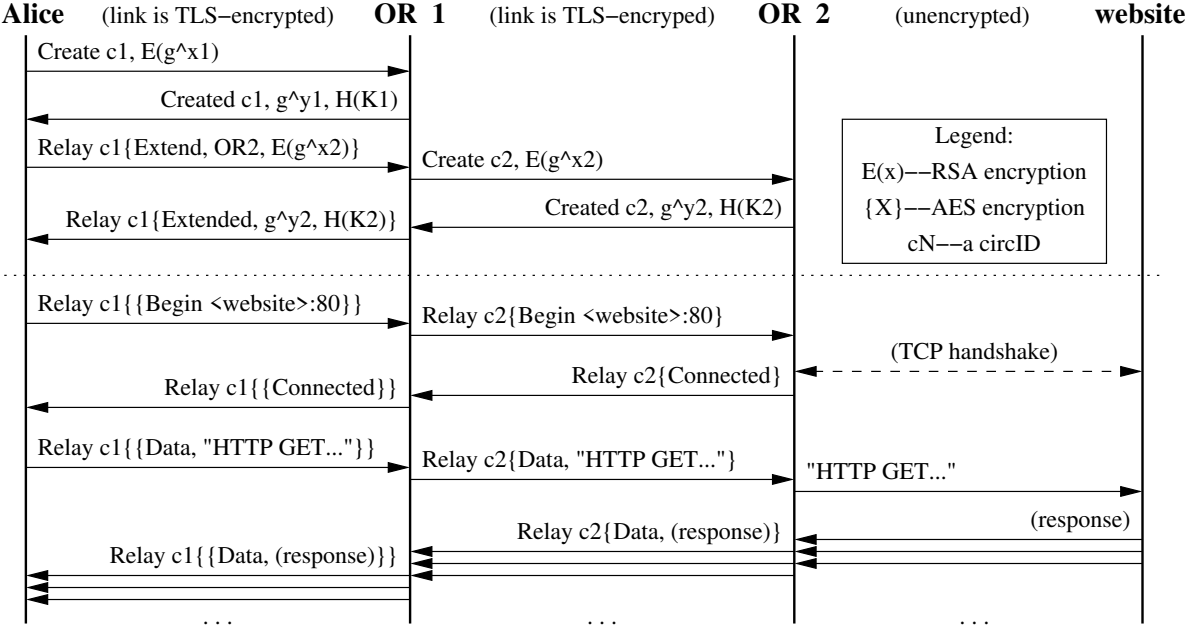
Alice
(link is TLS−encrypted)
OR 1
(link is TLS−encryped)
OR 2
(unencrypted)
website
Create c1, E(g^x1)
Created c1, g^y1, H(K1)
Relay c1{Extend, OR2, E(g^x2)}
Create c2, E(g^x2)
Created c2, g^y2, H(K2)
Relay c1{Extended, g^y2, H(K2)}
Legend:
E(x)−−RSA encryption
{X}−−AES encryption
cN−−a circID
Relay c1{{Begin <website>:80}}
Relay c2{Begin <website>:80}
(TCP handshake)
Relay c2{Connected}
Relay c1{{Connected}}
Relay c1{{Data, "HTTP GET..."}}
Relay c2{Data, "HTTP GET..."}
"HTTP GET..."
(response)
Relay c2{Data, (response)}
Relay c1{{Data, (response)}}
. . .
. . .
. . .