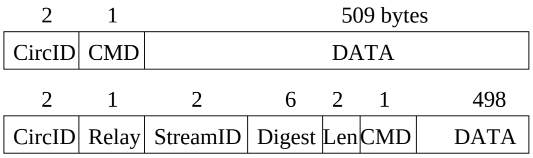

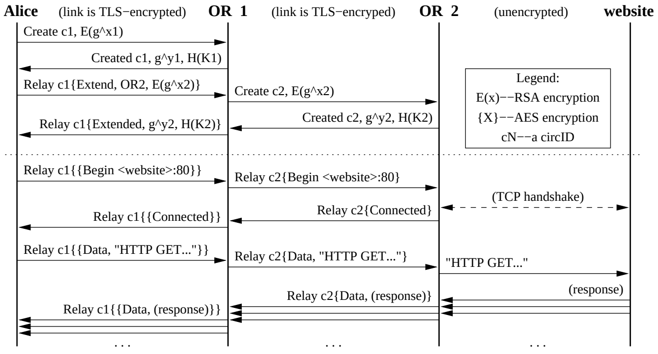

C_{AB}

g^x

g^y

$K = g^{xy}$

g^{x_2}

C_{BC}

C_{AB}

C_{BC}

$K_2 = g^{x_2 y_2}$

$E_{PK_{Bob}}(\cdot)$

H $|$

$$\begin{aligned} &\text{Alice} \rightarrow \text{Bob} : E_{PK_{Bob}}(g^x) \\ &\text{Bob} \rightarrow \text{Alice} : g^y, H(K|\text{``handshake''}) \end{aligned}$$

g^x y

-

-

-

-

-
-
-

$m > 1$

N $\left(\frac{m}{N}\right)^2$

$\langle \qquad \rangle$

$\langle$

$\sim$ $\rangle$

$\langle$

$\rangle$

$\langle$ $\rangle$

$\langle$ $\rangle$

$\langle$ $\rangle$

p^5

$\langle$

- $\rangle$

8^{th}