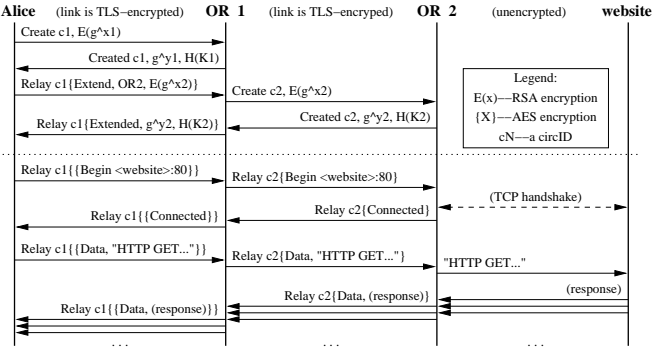


2	1	509 bytes				
CircID	CMD	DATA				

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA



$$C_{AB}$$

$$g^x$$

$$g^y$$

$$K = g^{xy}$$

$$g^{x_2}$$

$$C_{BC}$$

$$C_{BC} \qquad C_{AB}$$

$$K_2 = g^{x_2y_2}$$

$$H \qquad E_{PK_{Bob}}(\cdot) \qquad |$$

$$\begin{array}{l} \text{Alice} \rightarrow \text{Bob} : E_{PK_{Bob}}(g^x) \\ \text{Bob} \rightarrow \text{Alice} : g^y, H(K|\text{“handshake”}) \end{array}$$

$$g^x \qquad y$$

-
-
-

•

•

•

•

•

•

•

$$N$$

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

$$m > 1$$

~

<
>

<
>

<

>

<

>

<

>

$$p^5$$

⟨

- ⟩

$$8^{th}$$