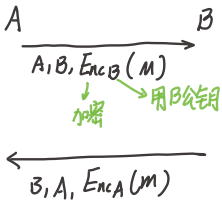
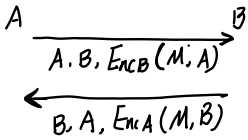
协议0：

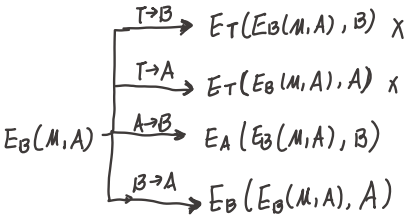


以下协议是否安全，若不安全如何攻击

1：



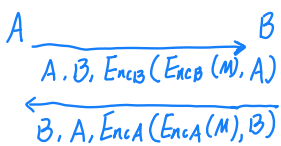
T截获 A, B, $E_B(M, A)$



将截获的消息以任何人名义重发给任何人都只会变得更复杂

无法找到有作用的攻击方法，认为协议1安全

2：



协议2不安全，攻击方法如下

攻击者T截获到 A, B, $E_B(E_B(M), A)$

T向B发送 $E_B(E_B(E_B(M), A), T)$ 则应得到 $E_T(E_T(E_B(M), A), B)$

即得到 $E_B(M)$

T再向B发送 $E_B(E_B(M), T)$ 则应得到 $E_T(E_T(M), B)$ 得到 M