南開大學 作业纸

系别 班级 姓名 张昊星 2113419 第 页

11.2 假设存在一个敌手截获第一次通信中 Cert(U) 与 b_U，则此时敌手可以计算新的 b_U' 替换 b_U，然后 V 在计算 K_{UV} 时并未发现 b_U 被篡改，因此在之后的通信中敌手便可替换身份。

密钥认证特性：敌手成功篡改密钥，从而协商双方被敌手的密钥控制，使不安全。

显式认证特性：敌手可以通过更改参数绕过密钥认证，使得双方无法进行认证。

11.4 假设存在一个算法 A 能够解决 MTI 问题；

设 Diffie-Hellman 问题有参数为 p（素数），g（Z_p^* 的本原元），$h = g^x \bmod p$，求 x

将 Diffie-Hellman 问题映射为 MTI 问题，其中 g 为 α，h 为 β，$r = \varepsilon = \delta = 1$

此时可以利用算法 A 得到 $\beta^{\log_\alpha r} \delta^{\log_\alpha \varepsilon} \bmod p$ 即为 DH 问题的结果

反之使得 $g = 1$，$x = \beta^{\log_\alpha r} \delta^{\log_\alpha \varepsilon}$ 即可解出 x 即为 MTI 问题的结果。