计算机密码学理论与应用

基于口令的密钥交换类协议

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Y^d \bmod N$$

基于口令的安全协议(1)

- 一个设计错误的例子：*Challenge-Response*协议

(E,D)是安全保密的对称加密方案

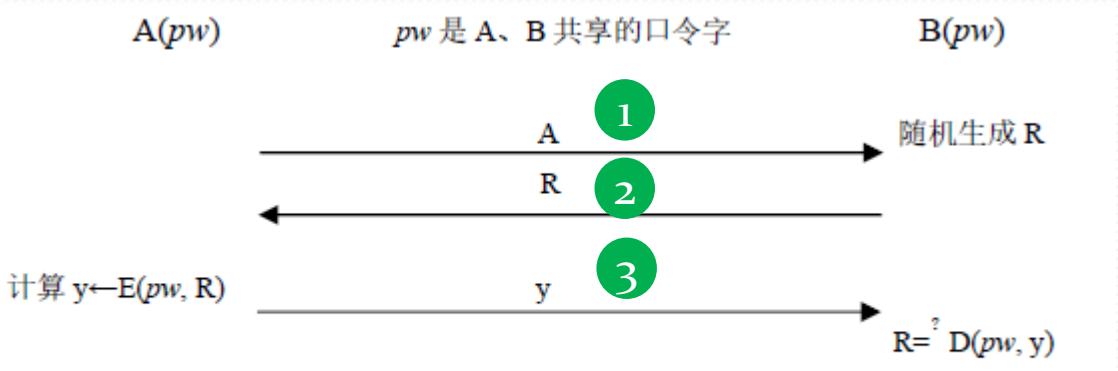


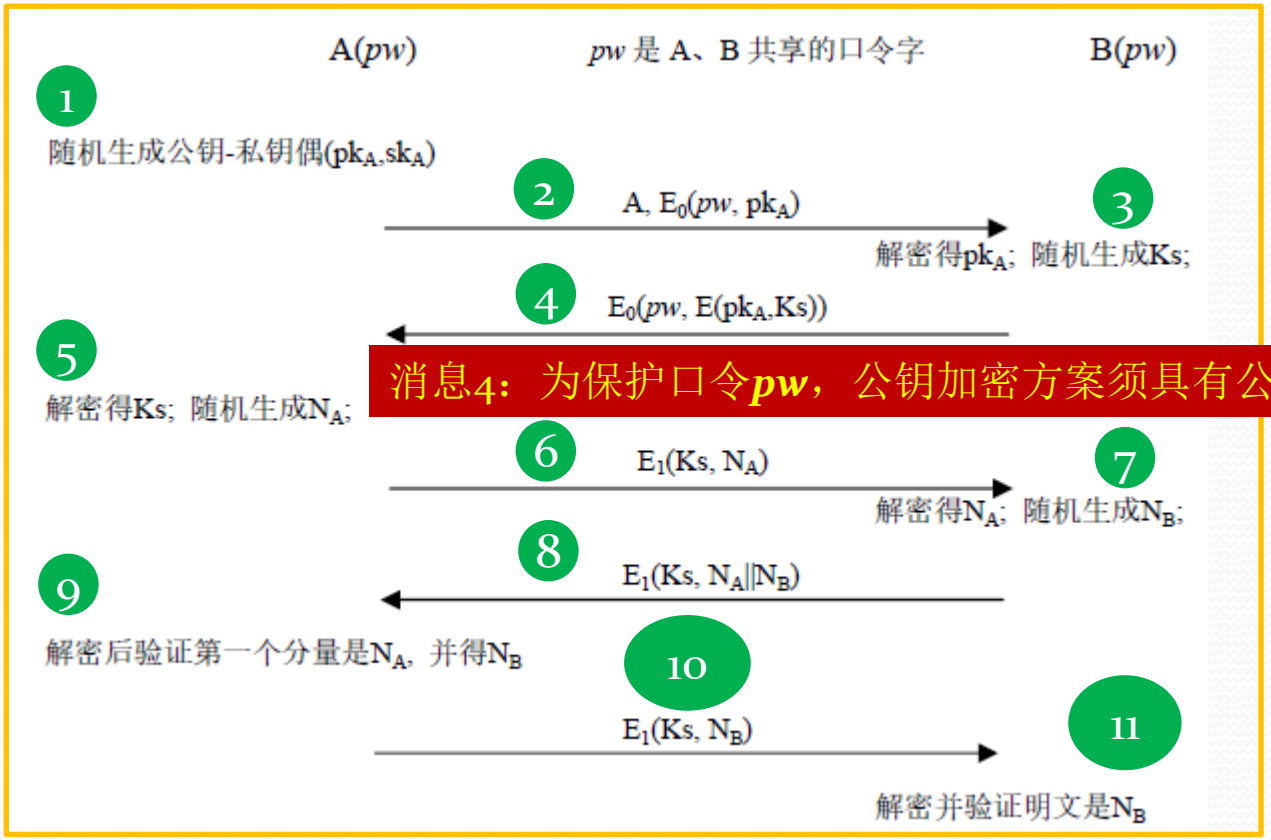
图 11-1　一个不能抵抗字典攻击的基于口令的身份认证协议

- 字典攻击
- 第一步：生成候选口令的集合D（口令字典）。由于口令的现实特点，
- P[*pw*出现于D]=100%且D的大小可在现实时间内被遍历！
- 第二步：对每个候选口令pw*，检验R=D(pw*,y)是否成立。
- 第二步总时间正比于字典D大小，因此也具有现实复杂度。

基于口令的安全协议(2)

- 带双向身份认证的密钥生成协议(*Bellovin-Merit*，1992)

(Eo,Do)和(E1,D1)是CPA-安全的对称加密方案， (E,D)是CPA-安全和匿名的公钥加密方案。



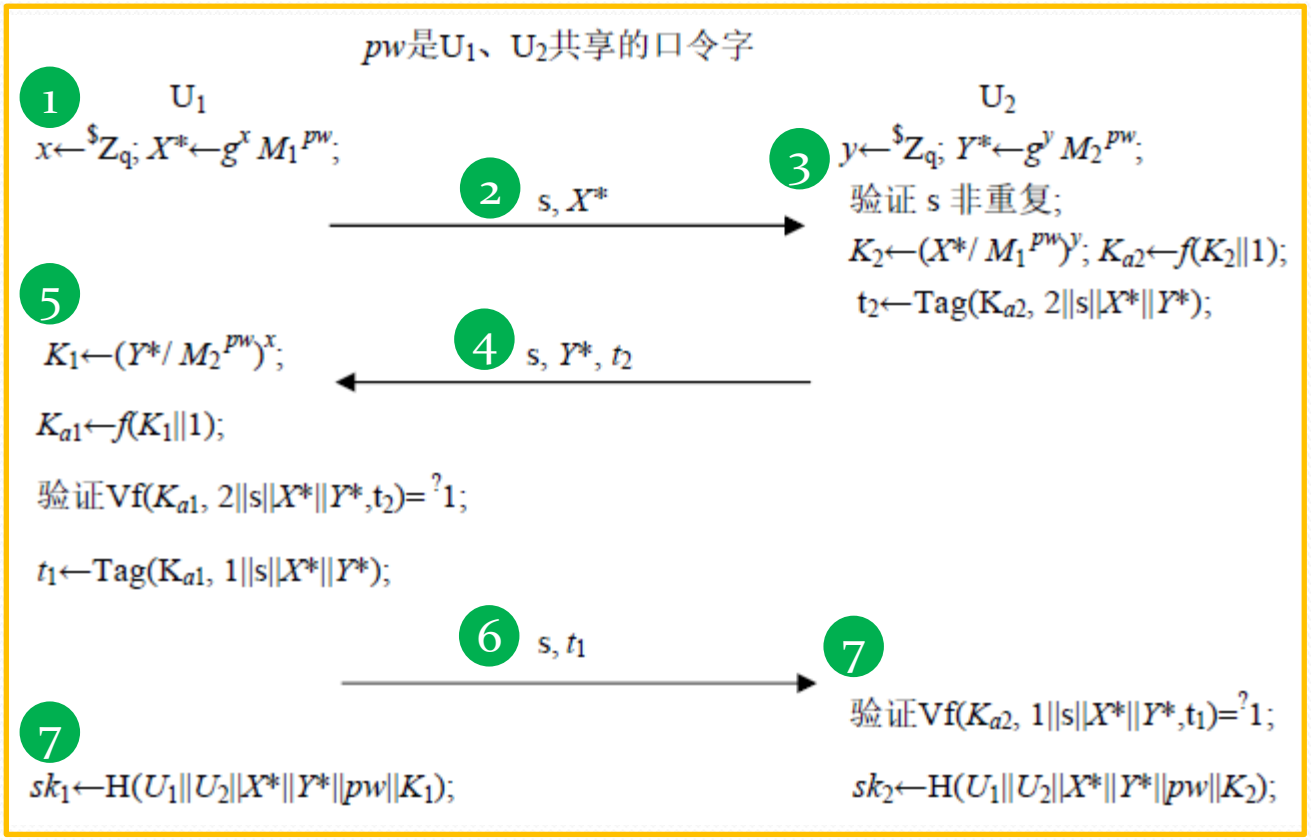
【习题】（当公钥加密方案具有匿名性时）为什么字典攻击不再有效？

【注】具有公钥匿名性质的实例：OAEP/RSA、Cramer-Shoup、Fujisaki-Okamato方案等。

基于口令的安全协议(3)

- 带双向身份认证的密钥交换协议(*Abdalla-Pointcheval*，2005)

*M1,M2,g*是公开的整数，*p*是公开的素数，所有运算均为*mod p*运算；
*s*是会话标识号； *f*是单向散列函数，*(Tag,Vf)*是安全的MAC方案。

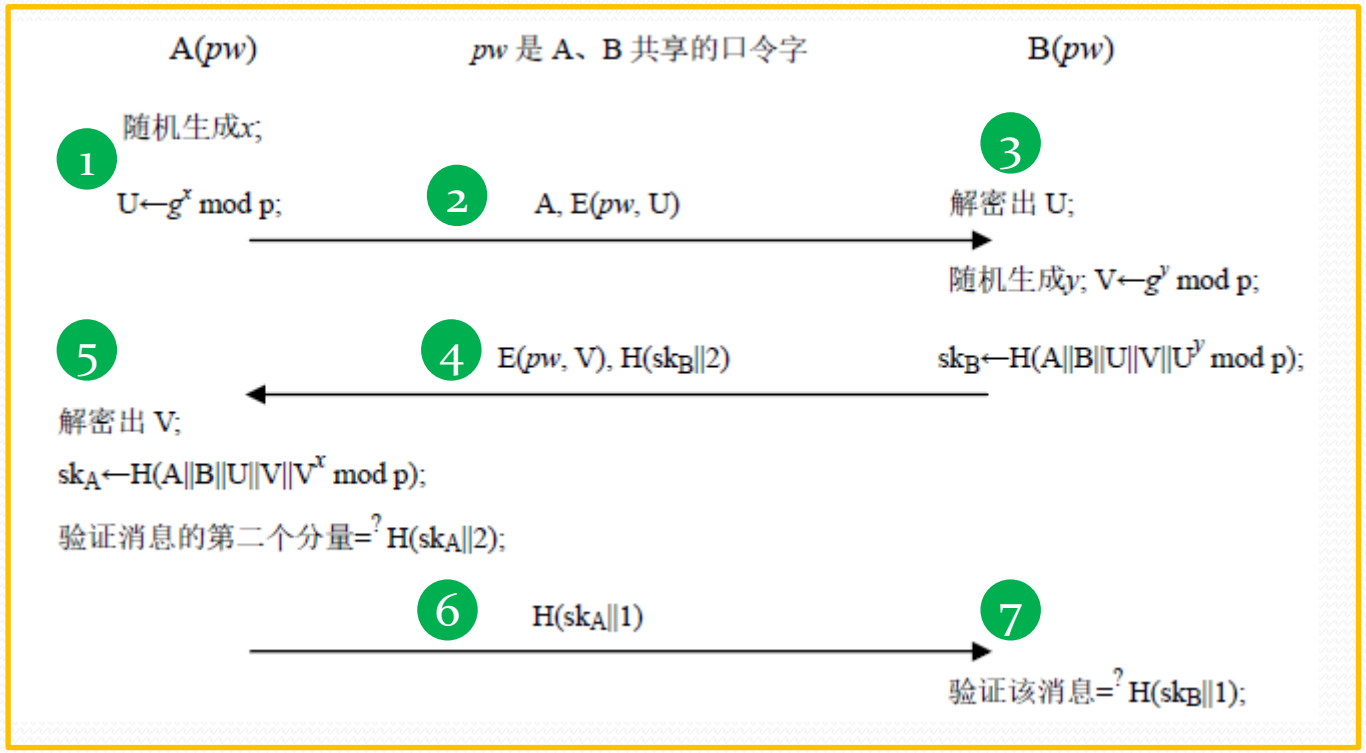


(1)字典攻击不再有效；(2)双方生成的共享密钥是$K_{a1}=K_{a2}$.

基于口令的安全协议(4)

- 带双向身份认证的密钥交换协议(*Bellare-Rogaway*，2001)

约定的参数，p是素数、1<g<p、H是单向散列函数(例如MD5 或SHA/SHA1)；E是对称加密方案的加密算法。A、B通过该协议认证对方的身份并计算出共同的会话密钥 $K_S=H(A\|B\|U\|V\|g^{xy} \bmod p)$。



【习题】如果H不是单向函数，而是一个容易被计算出逆映像的函数，以上协议不能抵抗字典攻击，为什么（试给出一种攻击方案）？

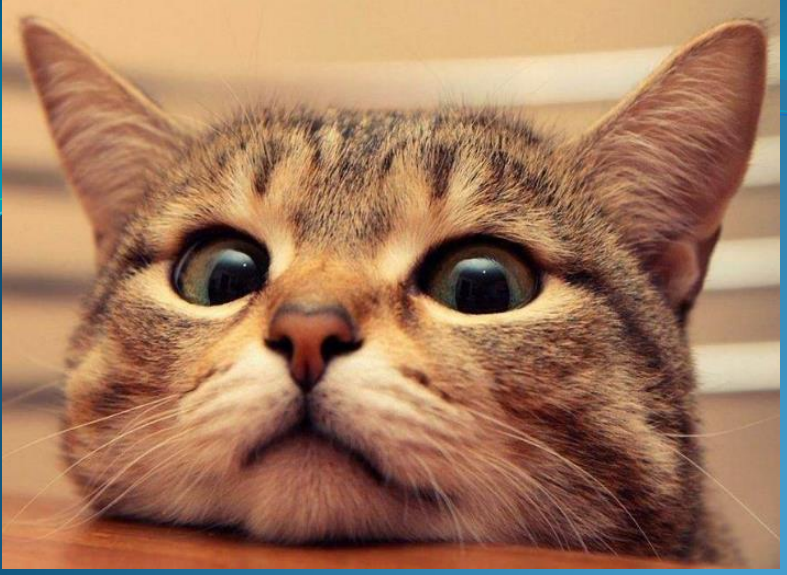
基于口令的安全协议(5)

- 基于口令的安全协议的安全性定义

- 对一个基于口令的协议Π，如果在针对Π的全部
- 攻击途径中，直接猜测口令的攻击具有相对最低的计算
- 复杂度，那么定义Π是口令安全的。

“听上去莫名其妙，为什么这样定义...口令安全性”

【习题】选择本课所述三种协议之一，准确、完整地表述进程A、B的动作。



“告诉你爸爸，今后再不要用猫主子的生日做口令啦”。

基于口令的密钥交换类协议

参考书：田园 网络安全教程，人民邮电出版社，2009，第十章