计算机密码学理论与应用

*Diffie-Hellman*密钥交换协议

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

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

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

密钥交换协议(1)

- 协议安全目标的基本概念

- 直观地说，带身份认证的密钥交换协议(*Authenticated Key Exchange*）需要同时完成两类目标：
- (1) 在线认证协议当前参与方的身份，其中某些协议只追求一方认证
- 另一方的身份(单向认证)，另一些协议追求互相认证(双向认证);
- (2) 在协议双方之间生成一个密钥K_s，K_s用于接下来对一切需要保密
- 的数据进行对称加密。

- 更精确地说，这类协议的安全目标包括以下须同时满足的三点：
- (1) 如果协议任何一方A(B)按照协议的逻辑判定对方的身份是B(A)，则
- 当前实际参与协议的对方确实是B(A)，即抗身份欺诈性质。
- (2) 如果协议任何一方A(B) 按照协议的逻辑判定当前与之会话的对方是
- B(A)，则对方也必定判定当前与之会话的对方是A(B)，即一致性。
- (3) 除合法参与方之外，协议所生成的会话密钥K_s使任何第三方(无论
- 被动或主动攻击者)无法(用P.P.T.算法)有效推断出来，即密钥保密性。

Diffie-Hellman密钥交换协议(1976)

公钥参数：大素数p、p的原根g。

他俩生成的共享秘密 $g^{xy} \bmod p =$ ？

随机生成x

$U=g^x \bmod p$

“真有点提心吊胆，那狗东西能看见我们全部的消息，还知道协议进程的逻辑”

U →

← V

随机生成y

$V=g^y \bmod p$

“没关系，有离散对数问题这个障碍呢，我们的素数p可是1000位呀”

$K=V^x \bmod p$

$K=U^y \bmod p$

密钥交换协议(2)

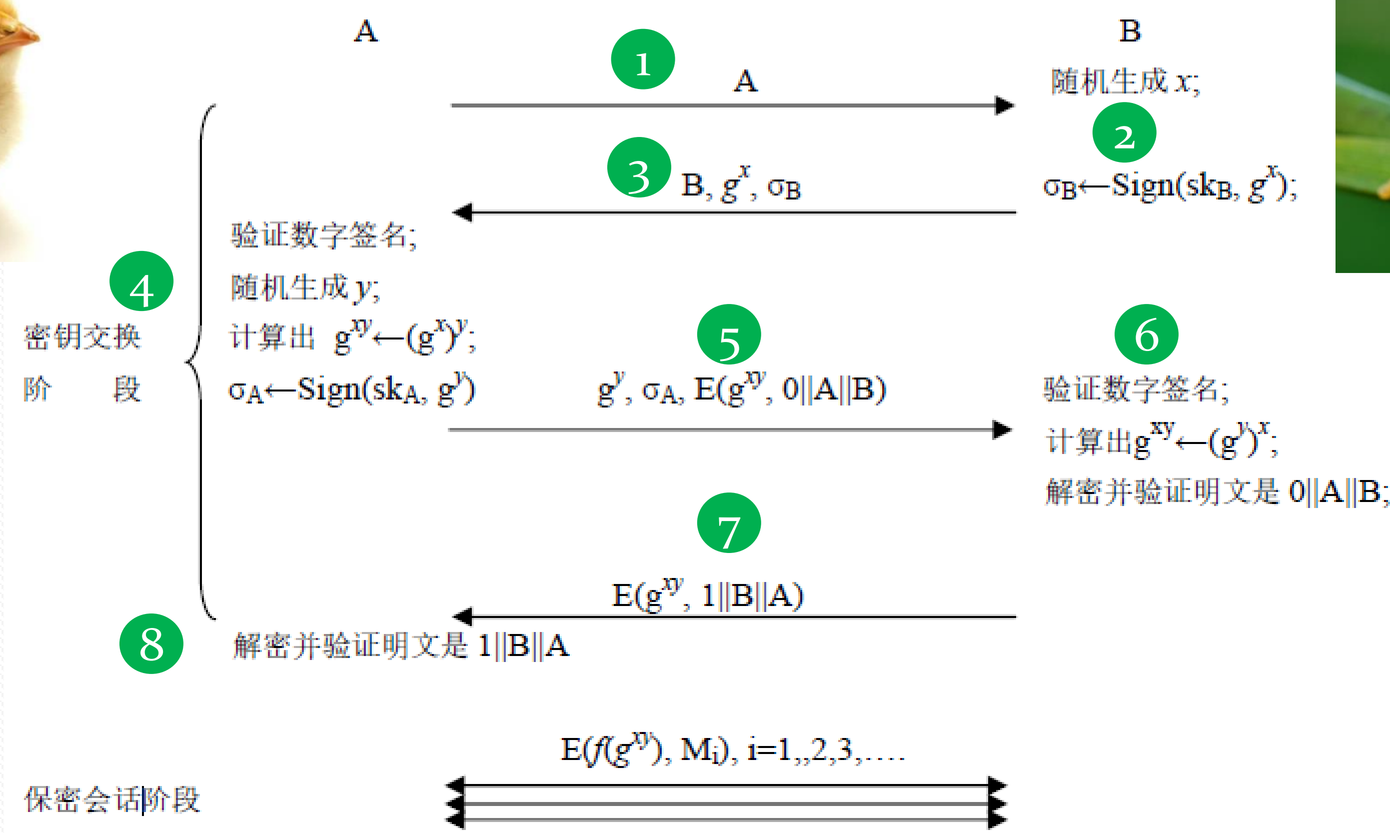
- *Diffie-Hellman*协议(1995)：参数和基础方案

- (1) G是循环群，例如F_p^*(p是大素数)，g是其公开的生成子。
- G上的判定性*Diffie-Hellman*问题是指任给U=g^x、V=g^y和W三个元素，判定$W \stackrel{?}{=} g^{xy}$是否成立。
- (2) *Diffie-Hellman*协议的安全性要求G上的判定性*Diffie-Hellman*
- 问题难解，即不存在P.P.T.算法A能对任何输入U(=g^x)、V(=g^y)
- 和W以显著偏离1/2的概率判定$W \stackrel{?}{=} g^{xy}$。
- (3) SIG=(KG, Sign, Vf)是抗伪造的数字签名方案.
- (4) Π=(KG^e,E,D)是CPA-保密的对称加密方案。
- (5) f是任何一种单向散列函数。

密钥交换协议(3)

- *Diffie-Hellman*协议：工作过程

(vk^A,sk^A)和(vk^B,sk^B)分别是A和B的签字公钥和私钥；假定A和B事先已从可信任的途径—如公钥基础设施中的数字证书—获得了对方的签字公钥vk^B和vk^A。



【习题】 假如该协议去掉两个密文分量$E(g^{xy}, 0||A||B)$和$E(g^{xy}, 1||B||A)$，请对这样一个协议给出完整的攻击过程，使攻击者成功地对A冒充B，或者对B冒充A。提示：可考虑重放攻击。

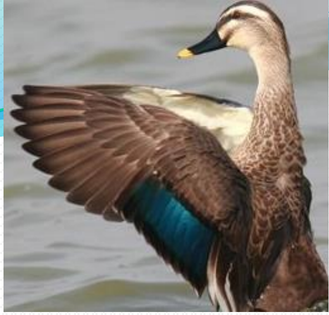
【习题】 该协议的两个密文分量$E(g^{xy}, 0||A||B)$和$E(g^{xy}, 1||B||A)$能用同一个明文的密文代替吗(例如都用$E(g^{xy}, 0||A||B)$)？

密钥交换协议(4)

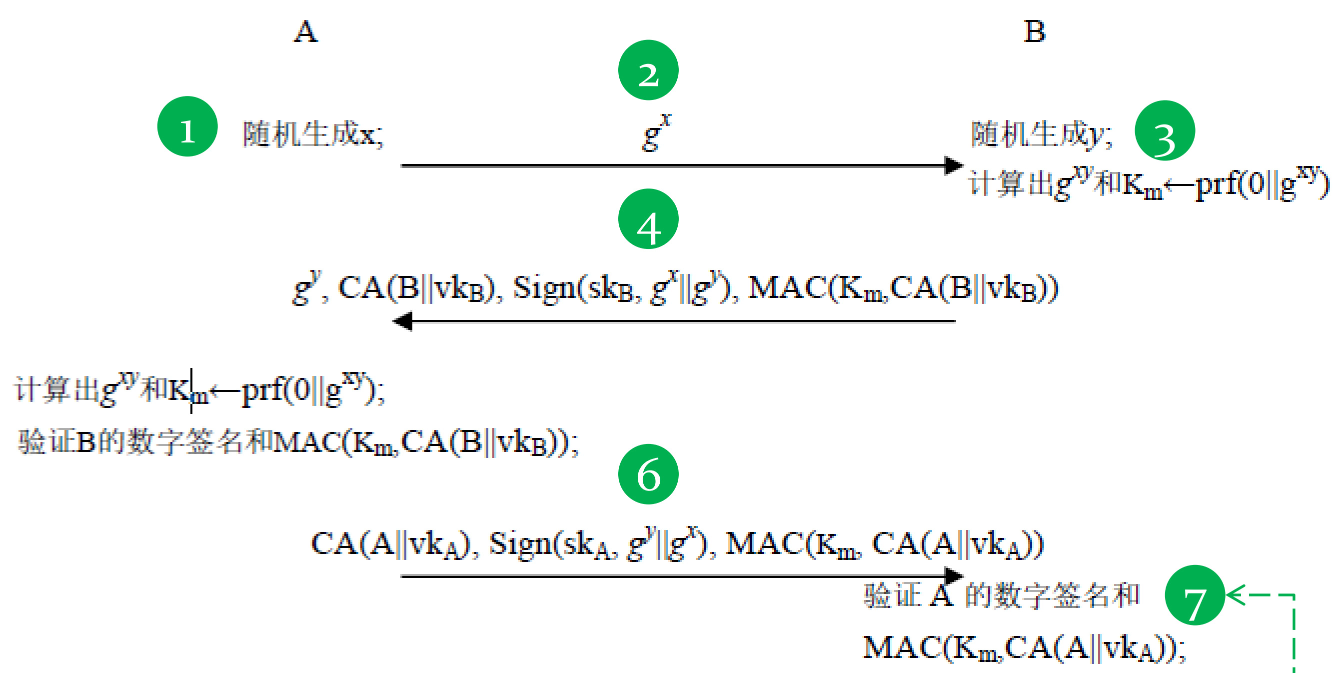
- *SIGMA*协议(1996)：基本参数和基础方案

- *SIGMA*协议是对前述*Diffie-Hellman*协议的优化，也是一类基于判定性*Diffie-Hellman*问题难解性的密钥交换协议。
- *prf*表示拟随机函数(在目前阶段暂将其理解为单向散列函数即可)。
- $SIG=(KG_s, Sign, Vf)$是抗伪造的数字签名方案。
- $MAC=(KG_m, MAC, MVf)$是抗伪造的消息认证码方案。
- 循环群G以g为公开的生成子，G上的判定性*Diffie-Hellman*问题难解。
- $CA(A||vk^A)$和$CA(B||vk^B)$表示A和B的签字公钥证书。

密钥交换协议(5)



- *SIGMA*协议：工作过程
-



【思考】通过验证数字签名，A能肯定B当前在线生成了g^y，为什么？

【思考】通过验证数字签名，B能肯定A当前在线生成了g^x，为什么？

密钥交换类协议

$g^{xy} \bmod p =$?

$V = g^y \bmod p$

$U = g^x \bmod p$

U

$\longrightarrow$

$\longleftarrow$

V

$K = V^x \bmod p$

$K = U^y \bmod p$