计算机密码学理论与应用

SIGMA密钥交换协议及其变体

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

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

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

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。

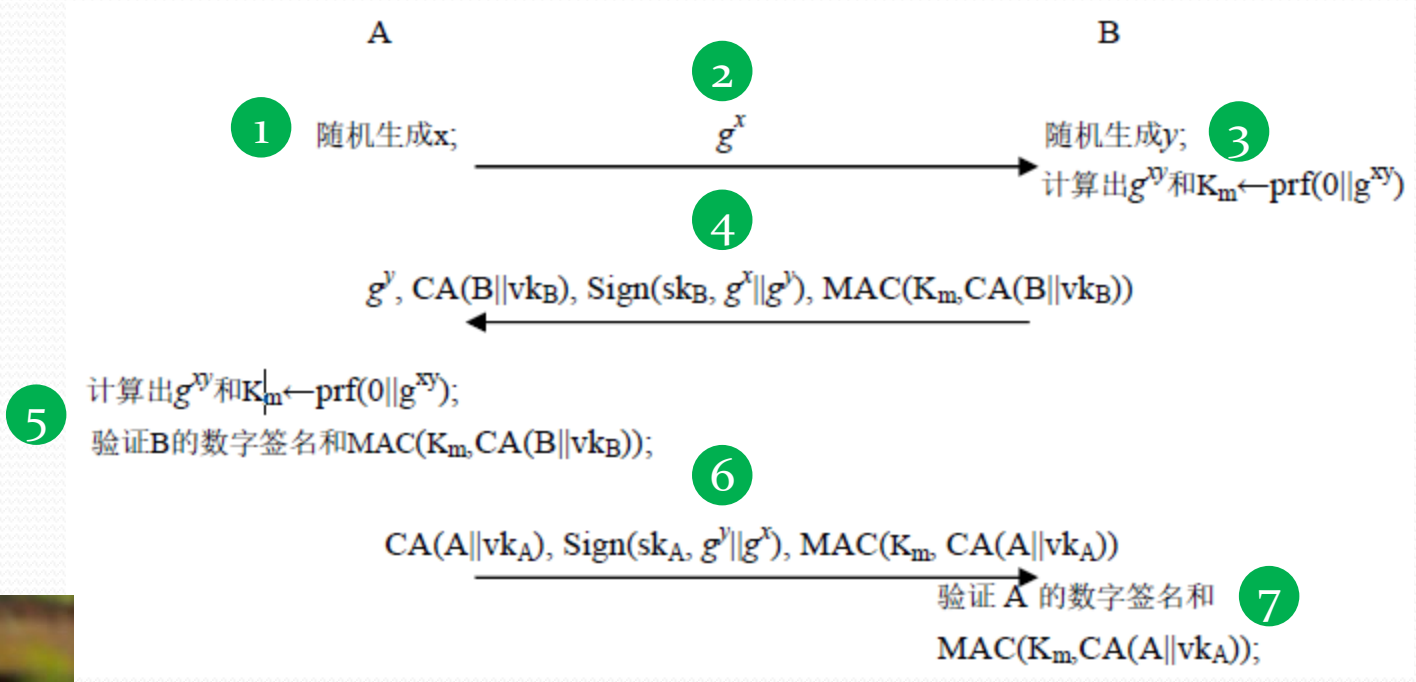
密钥交换协议(4)

- *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

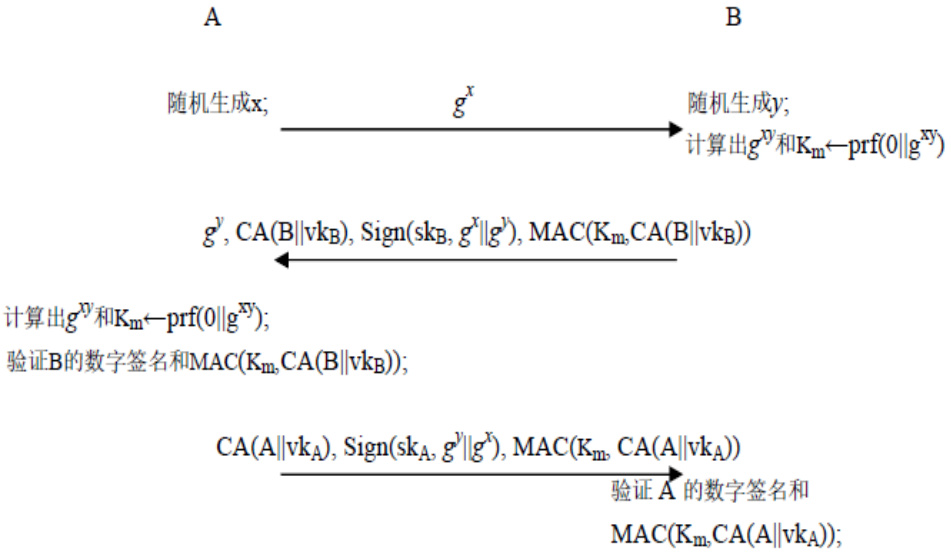


密钥交换协议(6)

- *SIGMA*协议：关于显式采用公钥证书的说明
- **与*Diffie-Hellman*协议不同，公钥证书显式出现于*SIGMA*协议的消息之中，目的是针对这样的应用情形，即协议参与方之一事先未知当前需要与之对话的对方。**
- 例一，在大规模分布式计算系统中，一个客户进程A需要请求特定的服务时，未必总按照事先的安排访问特定的服务器(B)，而是在网络环境中广播请求，任何能够提供服务的、可信任的服务器都可以成为协议的对方。
- 例二，在无线移动网络环境中，A需要与访问接入点或基站建立协议会话，这时A尤其无法事先明确究竟将与哪个对方(B)进行协议会话，只能在线认证对方的身份。
- **既然A不能事先明确B究竟是“谁”，因此A在第2条消息中待明确看到身份标识“B”之后，根据B提供的公钥证书$CA(B||vk^B)$来验证B的数字签名$Sign(sk^B, g^x||g^y)$。**
- **B对A的身份认证也采取同样的处理方法。**

密钥交换协议(7)

- *SIGMA*协议： 消息认证码$MAC(K_m,CA(A||vk^A))$和$MAC(K_m,CA(B||vk^B))$的作用



$MAC(K_m,CA(A||vk^A))$的作用：

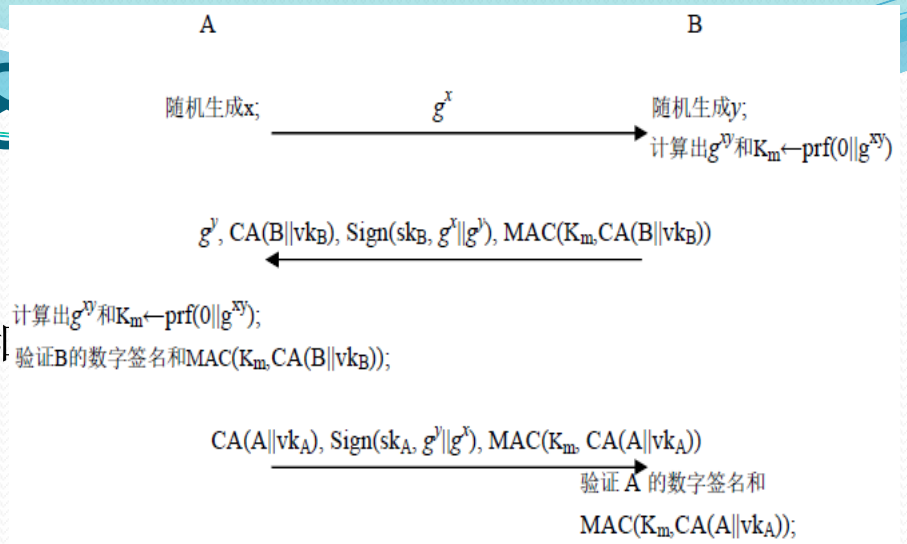
假如第3条消息不包含分量$MAC(K_m,CA(A||vk^A))$，一个攻击者P在A接收到第2条消息后向B发送第3条消息(CA(P||vk_P), Sign(sk_P, $g^y||g^x$))，于是B据此判定当前与之对话的对方是P(而非A)，但同时A在接收到第2条消息后却判定当前对方是B，A、B双方对对方身份的判别不一致，破坏了协议应该满足的安全性质之一(一致性)。

【思考】或许有同学认为该攻击似乎无害，毕竟密钥Ks并未泄露，P并不能破译A或B接下来将要发送的明文消息。

试想象以下应用场景：B是服务器、A是客户，A与B协商密钥的目的是为了向B转帐。在以上攻击发生后，A开始向B发送以刚刚生成的会话密钥Ks加密的帐务数据用以支付某种款项，而B却判定该支付行为来自P(而非A！)，尽管P对消息内容无从得知，但实际后果如何？

密钥交换协议(8

- *SIGMA*协议：
- 消息认证码$MAC(K_m,CA(A||vk^A))$和
-



$MAC(K_m,CA(B||vk^B))$的作用

这是针对一类特殊的攻击，即所谓证书替换攻击。

假如第2条消息不包含$MAC(K_m,CA(B||vk^B))$，这时一个攻击者P在看到来自B的消息(g^y, $CA(B||vk^B)$, $Sign(sk^B, g^x||g^y)$)后可以向公钥证书服务器CA请求一个包含自己的名字P和B的签字公钥vk^B的证书$CA(P||vk^B)$，P将这一(虽然并非伪造但却不正确的)公钥证书替换原来消息中的$CA(B||vk^B)$，然后将(g^y, $CA(P||vk^B)$, $Sign(sk^B, g^x||g^y)$)作为第2条消息发送到A；A在接收到这一消息后，因为能够正确验证“P”的数字签名$Sign(sk^B, g^x||g^y)$从而判定当前的对方“确实是P”，而实际上对方并非P而是B，破坏了协议应该满足的一致性！

就P在线欺骗证书服务器而言，上述攻击有些理想化，同学们有理由怀疑在实际中能否行得通。但无论如何，以上分析表明这是一个应该避免的安全漏洞。

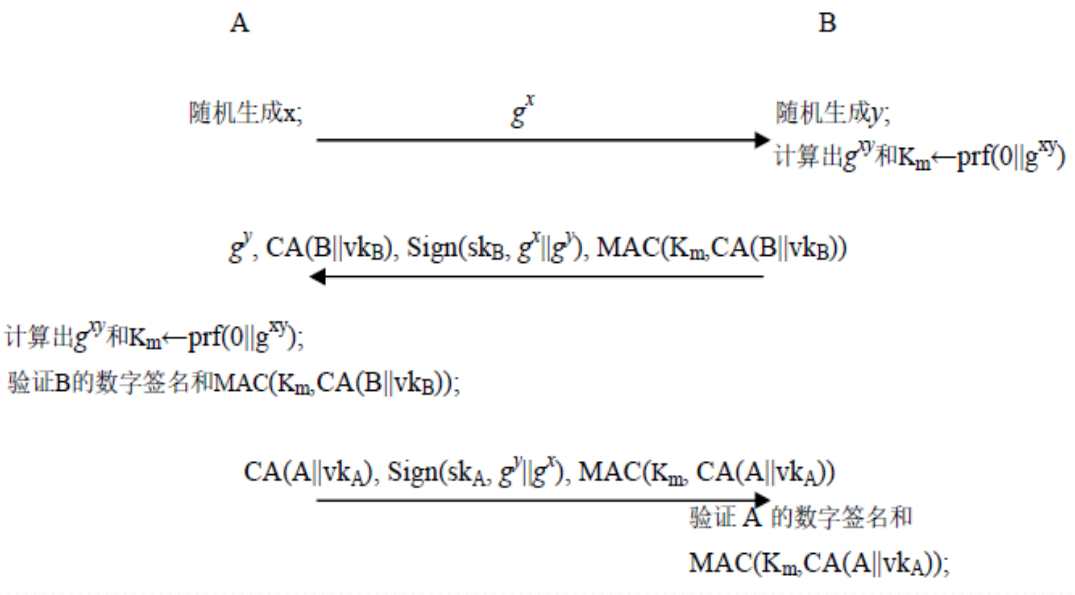
【思考】当第2条消息带上$MAC(K_m,CA(B||vk^B))$，P的上述攻击还能凑效吗？

【解答】因为P无法有效计算出K_m，所以不能有效伪造出$MAC(K_m,CA(P||vk^B))$，这样一来以上证书替换攻击就不再有效。

小结：从上述分析可以看出，$MAC(K_m,CA(A||vk^A))$和$MAC(K_m,CA(B||vk^B))$起着对公钥证书的在线签字作用，用以向对方证实自己确实是证书的持有者，为此这两个数据项都不可或缺。

密钥交换协议(9)

- *SIGMA*协议：匿名性质



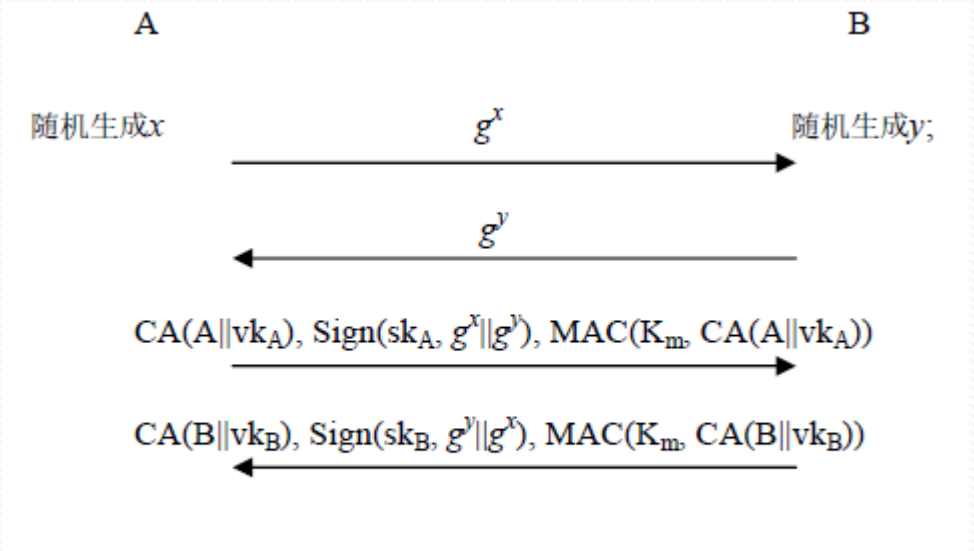
*SIGMA*协议还具有这样的特点：B先向A出示自己的身份(第2条消息)，而A仅在认证B的身份后，才向B表明自己的身份(第3条消息)。

在实际应用中，这给了协议发起方A一个机会，一旦对方不属于自己所信任的实体，A将立刻终止协议而不向B暴露自己的身份。

以上是所谓第一类匿名性质，即协议的参与方之一总是在另一方的身份被完全认证之后才出示自己的身份。具体而言，是***A***具有对***B***的后验身份认证性质。

密钥交换协议(10)

- *SIGMA*协议：匿名变体协议 I



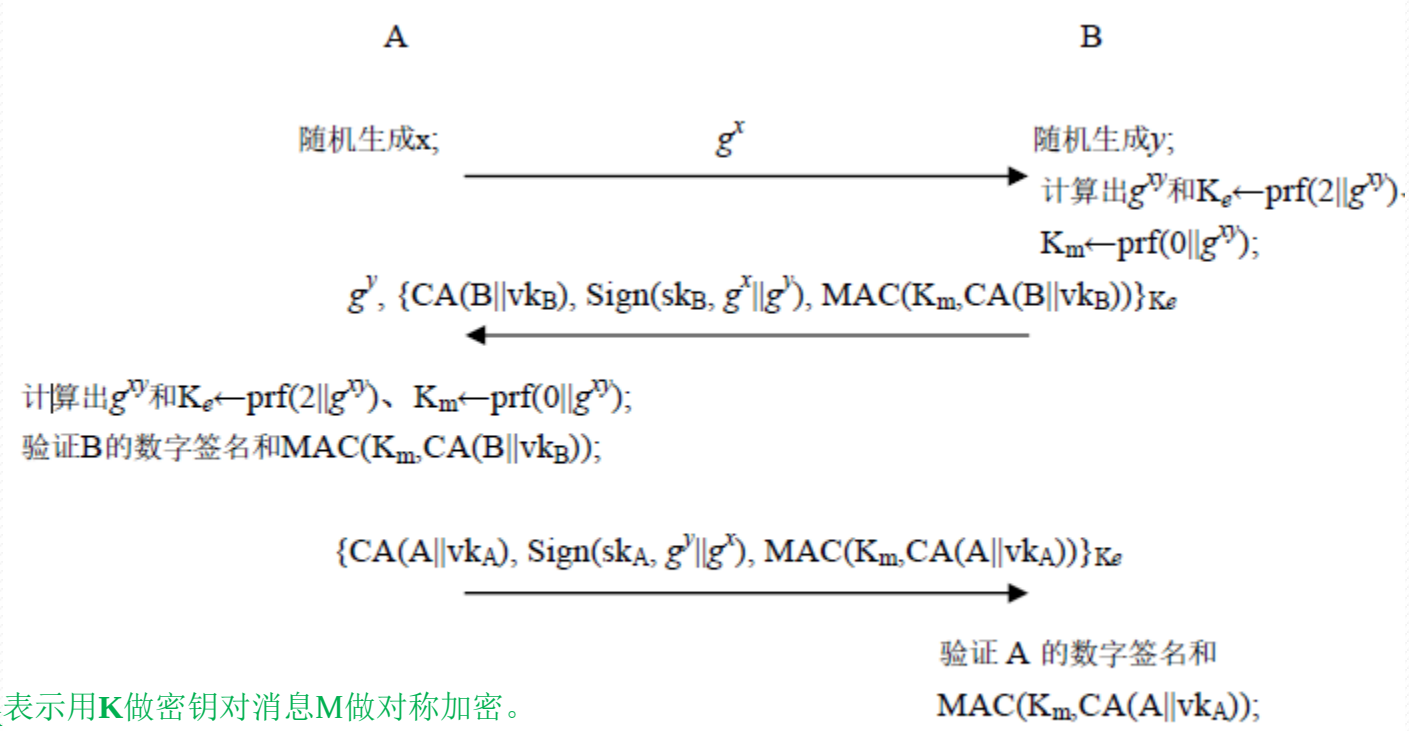
*SIGMA*协议-匿名变体I使**B具有对A的后验身份认证性质**，即A先出示自己的身份，在完全认证A的身份之后，B才出示自己的身份，从而给予B保护自己身份的机会。

【练习】详细描述进程A、B的处理动作，以及认证码$MAC(K_m, CA(A||vk^A))$和$MAC(K_m, CA(B||vk^B))$的作用。

【思考】如果既要保证协议具有抗身份欺诈性质，还要同时保证协议双方都具有后验身份认证性质，这是不可能的，为什么？

密钥交换协议(11)

- *SIGMA*协议：匿名变体协议 II



【注】符号$\{M\}_K$表示用K做密钥对消息M做对称加密。

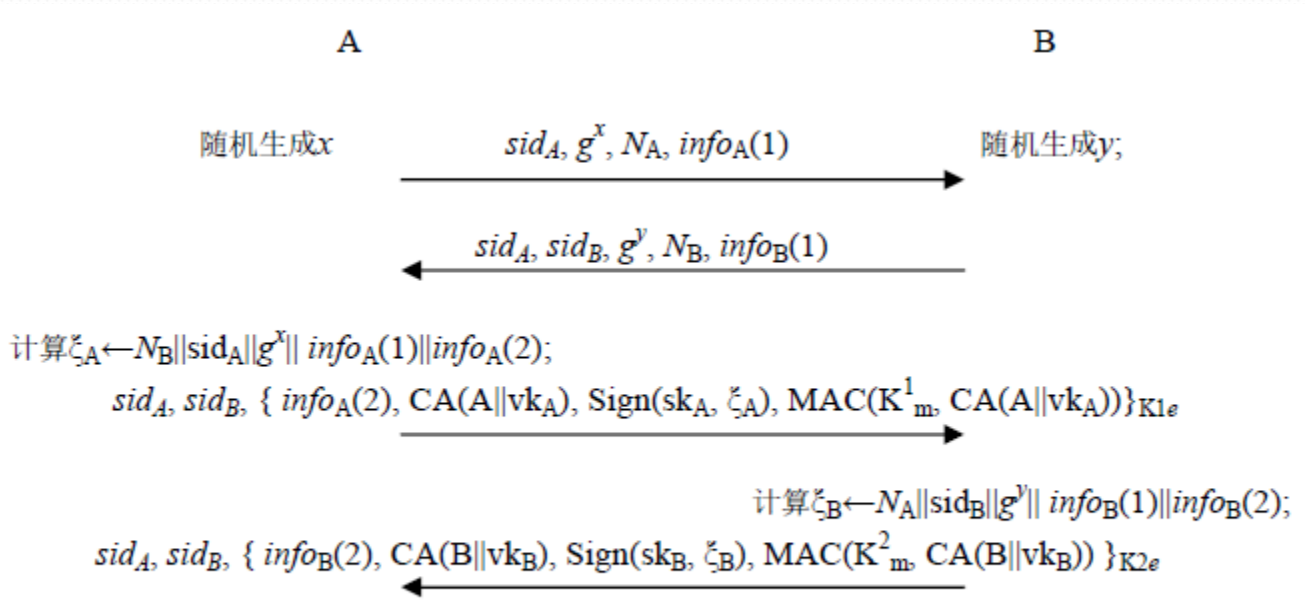
第二类匿名性质，即协议双方对任何非参与方完全匿名。

这一性质在当代无线网络环境中非常有用：通讯双方不仅需要保密其传输的数据，而且经常期望不向任何第三方暴露自己的身份，以免暴露自己的行踪。

*SIGMA*协议略加修改即可满足以上要求，基本办法是对含身份标识的消息进行对称加密，而加密密钥来自当前协议会话生成的随机数。这样，仅仅协议的合法参与方才能解密从而看到对方的身份标识，

密钥交换协议(12)

- *SIGMA*协议：完整的设计
- 以下协议(*SIGMA-R*)具有前述的全部安全性质，而且还具有B对A的后验身份认证性质(第一类匿名)，同时A、B对任何第三方完全匿名(第二类匿名)。



*SIGMA-R*增加以下一些实际应用中需要用到的元素。

sid^A、sid^B分别是由A、B随机生成的会话号，每条消息都带上该编号，这些编号还出现在数字签名中，目的是使当A、B之间并发存在多个同类协议会话时，总能由sid^A和sid^B共同唯一确定每个消息属于哪个会话实例，以抵抗并发-交错攻击。

N_A、N_B分别是由A、B随机生成的随机数，目的是使得每个协议会话都具有唯一的$N_A||N_B$，把这种唯一的随机数结合进协议消息以抵抗重放攻击。

生成的密钥Ks也与这两个随机数相关，目的是使破译密钥更加困难。

$Info_A(1)$、$info^A(2)$、$info^B(1)$和$info^B(2)$是一些信息块，根据具体应用情形赋予特定的内容。

密钥交换阶段用来实现对第三方匿名和验证消息认证码的对称密钥一共有4个：K_{1m}、K_{2m}、K_{1e}、K_{2e}，每个方向一个，而不是象原来那样两个方向共享一个，这样做也是为了提高攻击的难度。

密钥交换协议(13)

- 其他的例子：SSL/TLS协议

- 参见Stallings 第6版 第十七章
- W.Mao《现代密码学理论与应用》(2005)
- 等著作
- OpenSSL：开源SSL协议的C代码；
- 包含一个内容丰富的密码方案算法库。

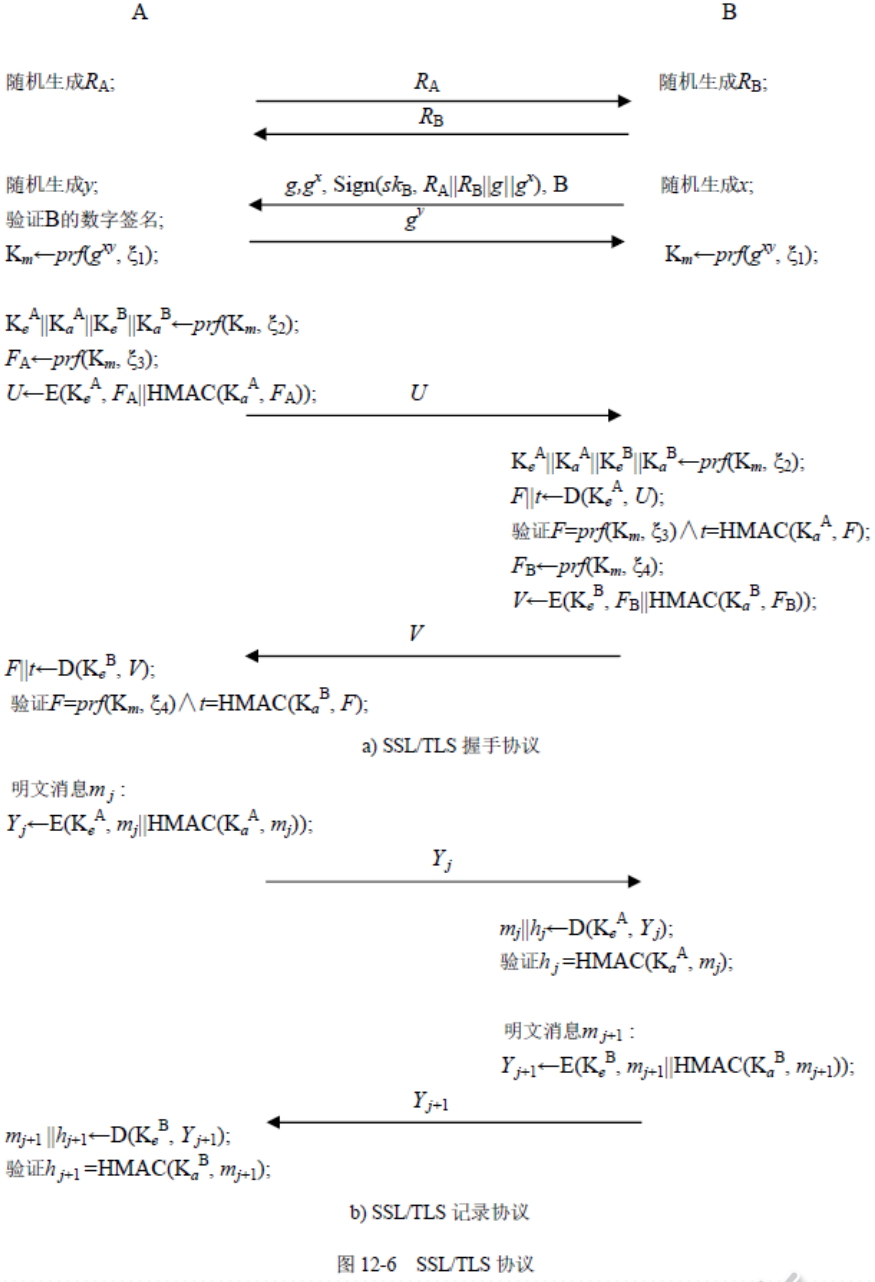


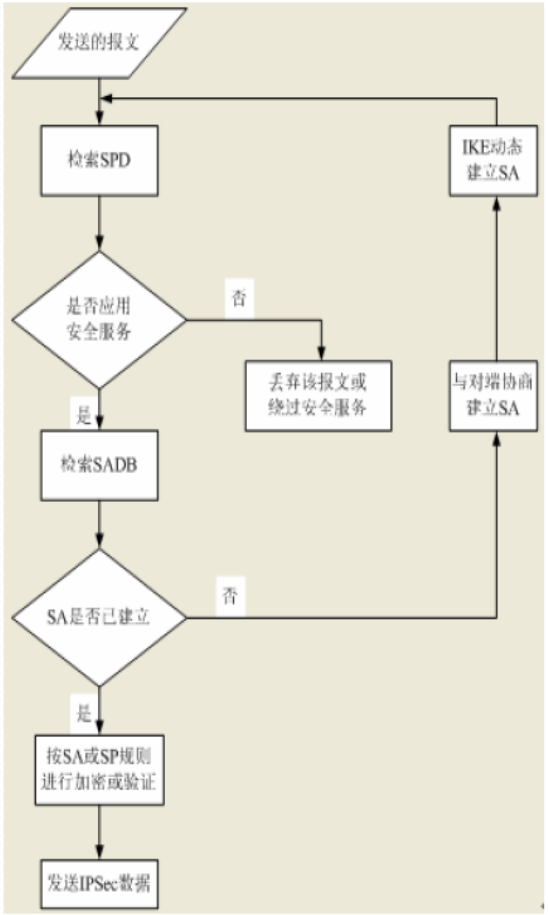
图 12-6 SSL/TLS 协议

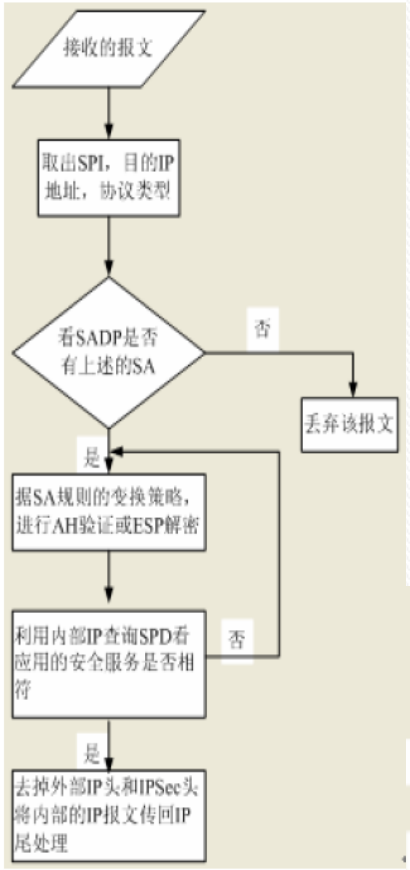
密钥交换协议(14)

其他类型的安全方案及协议

- 密钥分配型协议：
- 通过可信任的第三方对多方完成密钥分配
- 广播/组播型数据保密方案
- 组群身份认证类协议
- 组群密钥交换协议
- 各类应用层安全协议等
-

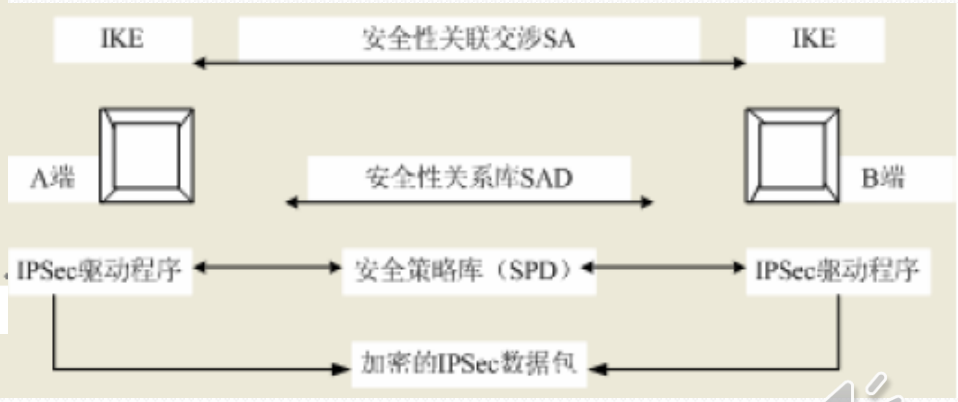
密钥交换协议(15)





密钥交换类安全协议的应用

- 生成VPN安全隧道
- (ISAKMP/IKE, IPSec#RFC2412,RFC2409, 1999)
- 参阅
- **IPSec：** *Stallings* 第六版 第二十章



密钥交换协议(5)

- 附录：*SIGMA*协议工作过程概述
-

A

B

1 随机生成x;

2 g^x

随机生成y; 3

计算出g^{xy}和$K_m \leftarrow prf(0||g^{xy})$

4 g^y, $CA(B||vk_B)$, $Sign(sk_B, g^x||g^y)$, $MAC(K_m, CA(B||vk_B))$

5 计算出g^{xy}和$K_m \leftarrow prf(0||g^{xy})$;

验证B的数字签名和$MAC(K_m, CA(B||vk_B))$;

6 $CA(A||vk_A)$, $Sign(sk_A, g^y||g^x)$, $MAC(K_m, CA(A||vk_A))$

验证 A 的数字签名和 7

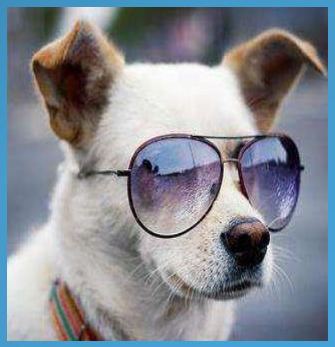
$MAC(K_m, CA(A||vk_A))$;

【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

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



$U=g^x \bmod p$

$K=V^x \bmod p$

U

V

$V=g^y \bmod p$

$K=U^y \bmod p$