B：服务器

A：客户端

k(A,B)：A与B的共享密钥

Na 客户端生成的随机数

Nb客户端生成的随机数

1. A -> B : A

2. B -> A : Nb

3. A -> B : Na,H(k(A,B),(Na,Nb,A))

4. B -> A : H(k(A,B),Na)

3.2.1角色提取

通过对MS-CHAP 协议分析, 客户端和服务器的两个角色被提取。根据协议消息的来源、消息的内容和参与主体, 客户端和服务器的角色提取表示为:

（1）客户端（协议的发起者）

role chap\_Init (A,B : agent,代理

(chap Init握手协议发起方身份标识)

Kab : symmetric\_key,对称密钥

H : hash\_func,哈希函数

Snd, Rcv : channel(dy))信道

(Snd ,Rcv是发送信道和接收信道)

played\_by A

定义：

local State : nat,

(这句定义又什么作用,local State和nat是什么意思?)

Na, Nb : text

const sec\_kab1 : protocol\_id()

init State := 0(记录状态，通过状态机对协议运行进行描述和记录)

（2）服务器（协议的接收者）

role chap\_Resp (B,A : agent, 代理

Kab : symmetric\_key, 对称密钥

H : hash\_func, 哈希函数

Snd, Rcv : channel(dy)) 信道

played\_by B

定义：

local State : nat,

Na, Nb : text

const sec\_kab2 : protocol\_id

init State := 0(不懂有什么作用,为什么等于0.)

（3）角色会话提取

role session(A,B : agent,代理

Kab : symmetric\_key,对称密钥

H : hash\_func)哈希函数

定义：

local SA, SB, RA, RB: channel (dy)

(4个信道)

Composition(角色构成)

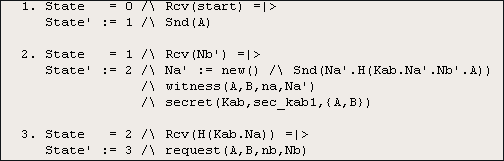
chap\_Init(A, B, Kab, H, SA, RA)

/\ chap\_Resp(B, A, Kab, H, SB, RB)

(“/\”这个符号是什么：and和)

转换规则：

（1）客户端：



(转换规则默认第一个就是客户端吗?是

State与State’ :有什么区别?不同操作

“/\”的作用是什么?and

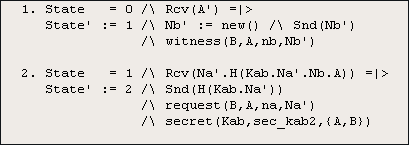
State=0,State=1中”0”,”1”是代表不同的阶段吗?是

第二行Snd(A)意思是客户端给服务器发送A的身份吗?是

每小段的开头1. 2. 3.这三个标号必须有吗?这个说不准，不同工具不一样，你可以控制变量法尝试一下

Rcv(….)是什么意思接收)

（2）服务器：



攻击者描述：

role environment()

定义：

const a, b : agent,

kab, kai, kbi : symmetric\_key,

h : hash\_func,

na, nb : protocol\_id

攻击者知识= {a, b, h, kai, kbi }

composition

session(a,b,kab,h) /\

session(a,i,kai,h) /\

session(b,i,kbi,h)