MetaCP Protocol Designer - Any Web Browser

File Edit Help

MetaCP Load Save Export

Knowledge

$g \in \mathbb{Z}_p$

Alice's initial knowledge

```
<knowledge entity="Alice">
    <variable id="g" type="constant"></variable>
</knowledge>
```

Alice

Bob

$x \in_R \mathbb{N}$

$gx \leftarrow g^x$

gx

Knowledge

$x \in \mathbb{N}$

$gx \in \mathbb{Z}_p$

$g \in \mathbb{Z}_p$

$gy \in \mathbb{Z}_p$

gy

$y \in_R \mathbb{N}$

$gy \leftarrow g^y$

$k_B \leftarrow gx^y$

```
<event type="send">
  <variable id="gy"></variable>
</event>
<channel></channel>
<event type="receive">
  <variable id="gy"></variable>
</event>
```

types/sets

statements

x <$ N

y <$ N

gx <- exp(g,x)

gy <- exp(g,y)

kA <- exp(gy,x)

kB <- exp(gx,y)

+ assignment

constants

variables

functions