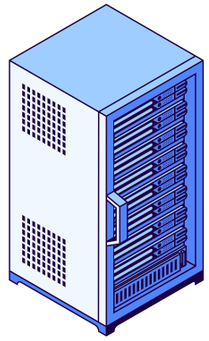
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

Bob



Server

Alice

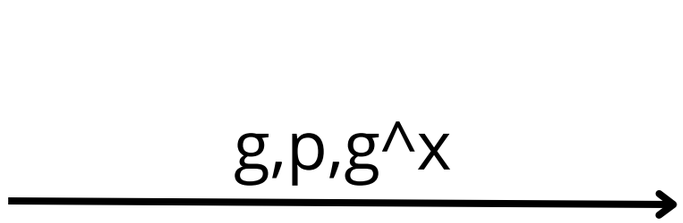
Bob envia Mensagem a Alice.

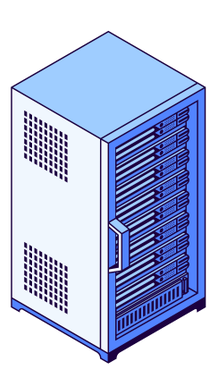
Pressuposto: O servidor conhece os certificados dos membros da rede

g^x

Bob

g,p,g^x



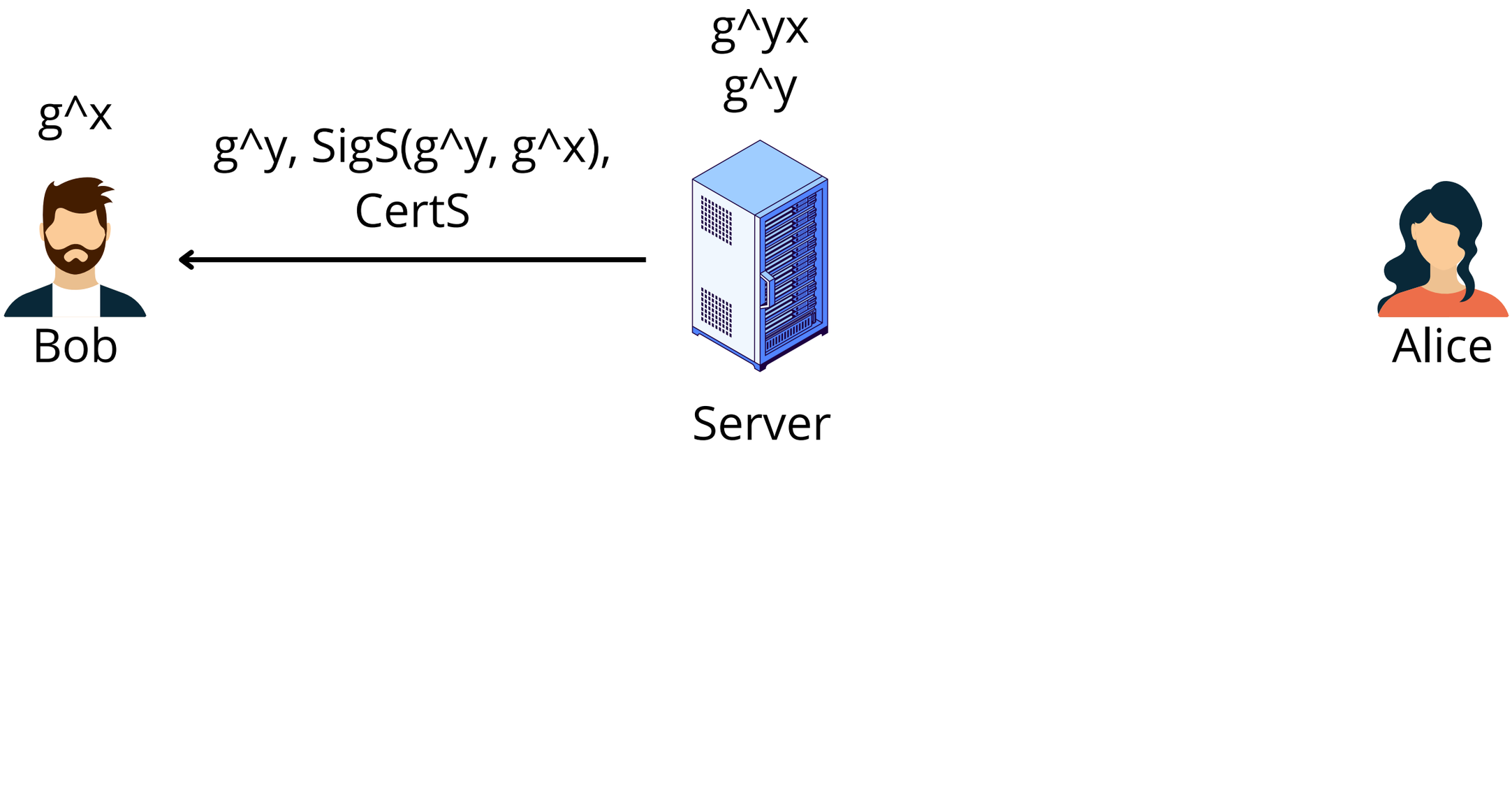


Server

Alice

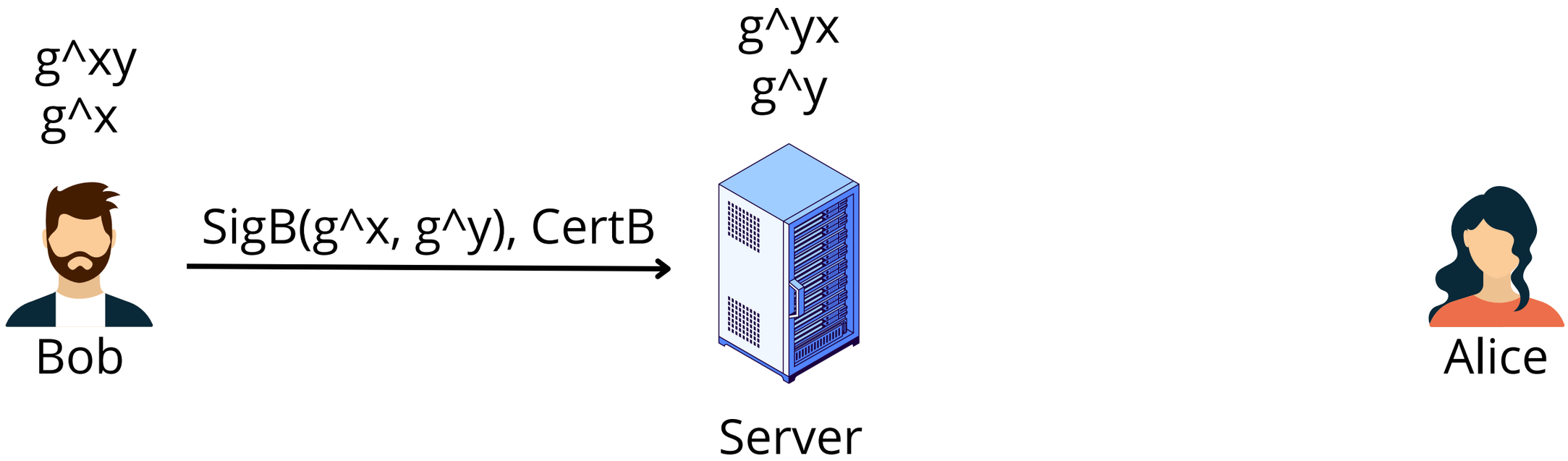
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob envia Mensagem a Alice.

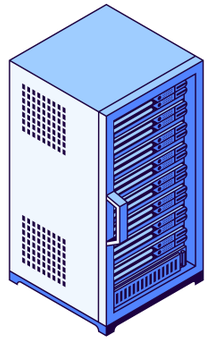
Pressuposto: O servidor conhece os certificados dos membros da rede

g^xy
g^x

Bob

Conexão estabelecida

g^yx
g^y

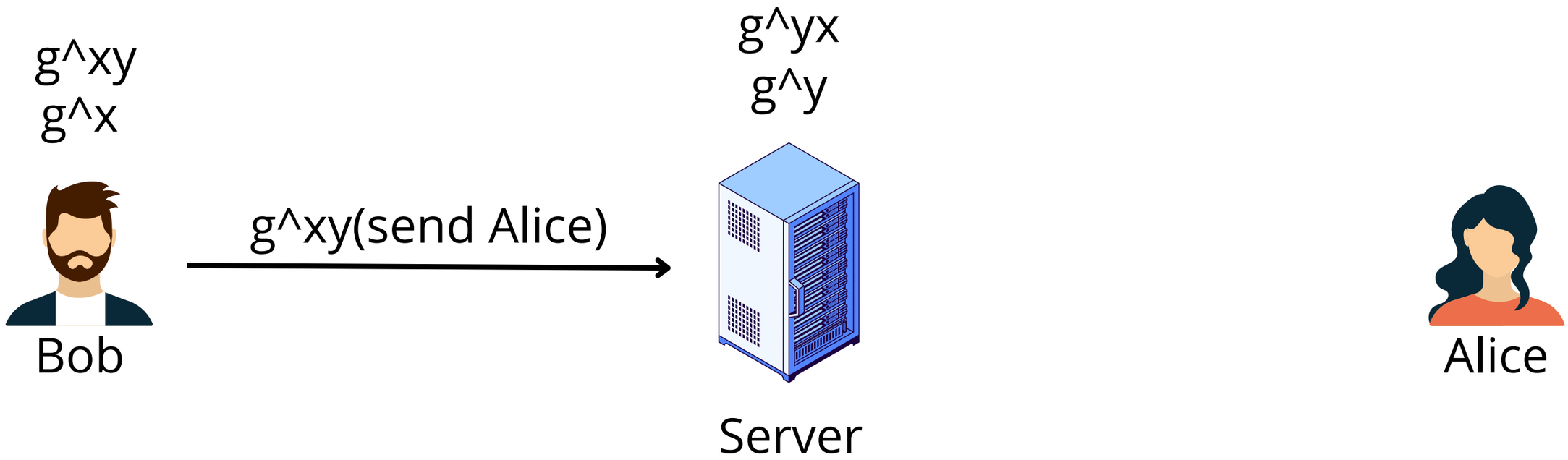


Server

Alice

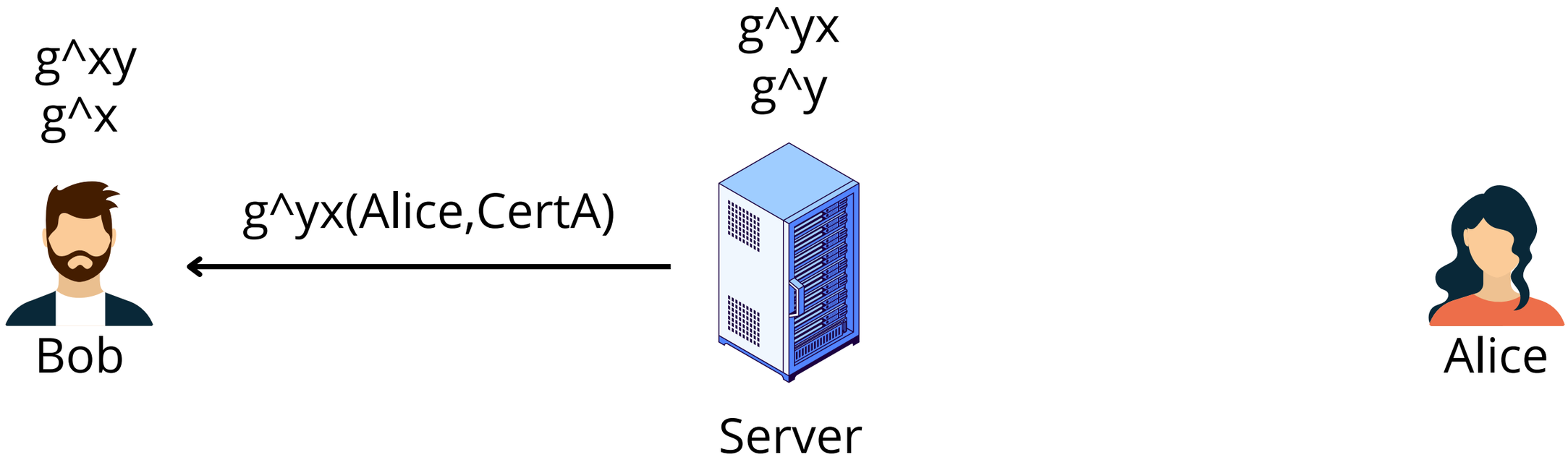
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



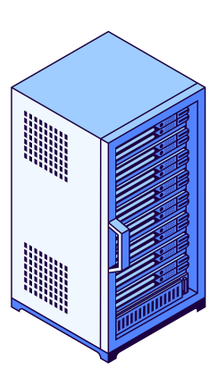
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

g^xy
g^x

g^yx
g^y

Bob



Server

Alice

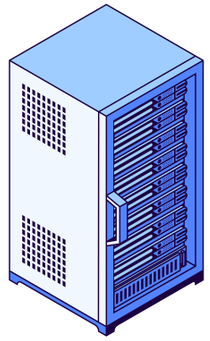
g^xy(CifA(message),Sig(CifA(message)))
Ciframos a mensagem com o certificado da Alice

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

1,CifA(message),Sig(CifA(message))

Bob



Server

Alice

Bob envia Mensagem a Alice.

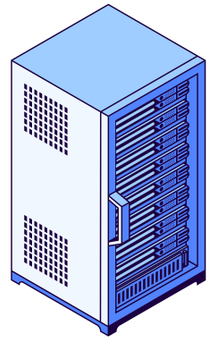
Pressuposto: O servidor conhece os certificados dos membros da rede

1,CifA(message),Sig(CifA(message))

g^wz

g^zw

Bob



Server

Alice

Alice estabelece a conexão

Bob envia Mensagem a Alice.

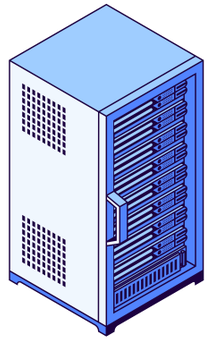
Pressuposto: O servidor conhece os certificados dos membros da rede

1,CifA(message),Sig(CifA(message))

g^wz

g^zw

Bob



Server

g^zw(getMsg)

Alice

Bob envia Mensagem a Alice.

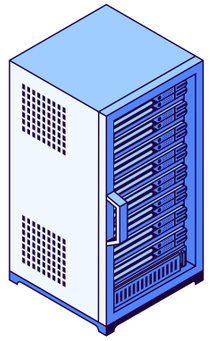
Pressuposto: O servidor conhece os certificados dos membros da rede

1,CifA(message),Sig(CifA(message))

g^wz

g^zw

Bob



Server

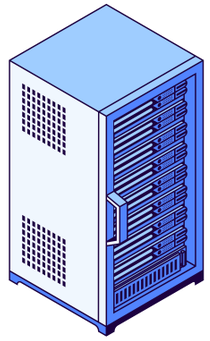
Alice

g^wz(CifA(message),Sig(CifA(message))),CertB

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

Bob



Server

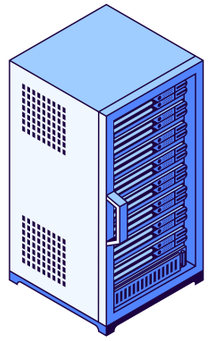
Alice

Alice pode verificar a assinatura do Bob, e pode decifrar a mensagem com a sua chave privada

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

Bob



Server

Alice

Assim, o servidor não consegue ler as mensagens do Bob para a Alice