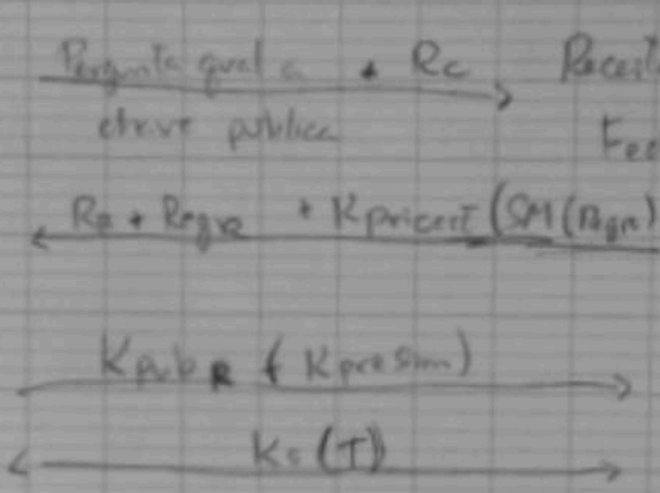
Questão Aberta
Luiza Ávila



Legenda:
Rc - Desafio do cliente
Rr - Desafio da Receita Federal
Rsgn - Registro de R
Kpricert - chave privada da certificadora
T_m - texto
Kpubr - chave pública da receita
Kpresim - chave pré-simétrica
Ks - chave simétrica

O que eu propunha assim que recebesse do cliente a pergunta com o desafio, a receita federal deve mandar o seu desafio, seu registro e sua assinatura (chave privada da certificadora fechando o sumário). A assinatura garante autenticação. O cliente abrirá usando a chave pública da certificadora, confirmará se o registro está correto, e, se estiver, responderá fechando com a chave pública da Receita, uma chave pré-simétrica, que, junto com os 2 desafios, formará a chave simétrica para a comunicação.