身份认证

口令：会被窃听

加密口令：可能遭受回放（重放）攻击

加密一次性随机数：可能遭受中间人攻击（Bob给Alice的随机数R被Trudy截获，然后用Trudy的私钥加密并把他的公钥发给Bob，则Bob会认为对方就是Alice）

