HW3

1、基于口令：静态口令，动态口令。

基于智能卡：如 USB Key，

基于物理特征：如指纹识别、掌纹识别、手形识别、人用金识别、虹膜识别、视网膜识别、声音识别、签名识别，

2、证书又称数字标识，是互联网通讯中标志通讯各方身份的数字认证，可以在网上用来识别对方身份。

功能：保证信息和数据完整性与安全性，含有拿握密钥的持证者的确切身份或其他属性，分为个人、企业和开发者数字证书。

3、X.509包含：①版本号：区分合法证书的不同版本

②序列号：一个整数，由签发该证书的CA给定，起唯一标识该证书。

③签名算法标识：证书中计算签名的算法，包括一个标识别算法的子标识和算法的可选参数

④签发者 ⑤有效期用 ⑥证书主体名 ⑦证书主体公钥的信息

⑧签发者唯一标识 ⑨证书主体唯一标识 ⑩扩展 ⑪签名

4、信任模型是提供用户双方相互信任机制的框架

PKI信任模型有：层次模型：有严格的层次结构

交叉模型：

混合模型

桥CA模型

信任列表模型