Introduction to cryptography(To warm up)

1. 基于属性的加密 Attribute-base eng……（ABE）
2. 指定访问控制的策略（防止冗余，一个秘钥多人使用）
    a. 生成各自属性的私钥集合，可以对应解密
    b. 数字电视的加密：不同频道的加密解密（用户可能泄露私钥，取消泄露私钥的用户权限）
       如果对数字电视进行属性加密呢?
    c. 如何验证与云服务器是否完整
3. 例子：医疗中的传感系统
    a. 手机传送病人的数据到云端；
    b. 医生对数据判断（疾病类型F1、F2、F3），如何在过程中保护隐私；
        i. 需要保护的隐私：病人身份信息，诊断结果，诊断函数；
        ii. 即：输入、输出、计算过程；
4. 如何验证云计算返回的结果是否正确
    a. 验证过程必须是高效
5. 同态加密：加法同态，减法同态，全同态加密（包括加法和减法）
    a. 加法同态
    b. 乘法同态
    c. 全同态加密
6. 确定性加密与概率加密
    a. 确定性加密：多次加密得到同一个密文（安全级别低）
    b. 概率加密：每次加密都得到不同的密文（安全级别高）
7. 假设要越少才越好，即假设越弱越好。
8. DLP、CDHP、DDHP
    a. DLP：(g，g^a -> a)　　难

b. CDHP：(g，g^a，g^b -> g^ab)　　中

c. DDHP：(g，g^a，g^b -> g^ab)；(g，g^a，g^b -> g^c)　　易

9. 数据的保护方面
    a. 机密性：加密
    b. 完整性：数字签名，消息认证
    c. 鉴别（认证）：数字签名
    d. 抗抵赖性（不可否认性）：数字签名
10. 密码学分支：密码编码学、密码分析学
11. 保密通信模型
12. 攻击类型
    a. 惟密文攻击　　弱
    b. 已知明文攻击　　中
        i. 前K次的明文和密文已知，推断后面的明文
        ii.
    c. 选择明文攻击 CPA：选择适应性的明文　　强
    d. 选择密文攻击 CCA：选择适应性的密文　　很强
13. 熵：定义不确定性 H(m | c) = H(m)
14. 评估安全性
    a. 无条件安全性
    b. 计算安全性：攻破他需要的计算水平高出攻击者的计算水平
    c. 可证明安全性
15. 密码体制
    a. 单向函数密码体制
        i. one-way function：
        ii. one-way trapdoor function：单向陷门函数
    b. 双向函数密码体制
16. 对称密码体制与非对称密码体制

    a. 对称非对称混合使用
        i. A -> B
        ii. K：特指消息
17. privateKeyGenerator：私钥生成器
    a. certificateless cugrte
    b. secert sharing
18. 明天的内容（6/8）秘钥管理，公钥加密，数字签名