1. 公钥和私钥
    a. A send mag to B
    b. 计算mac(m)
2. public-key Encryption 公钥加密
    a.
    b.
3. CDH难，gap-CDH简单
4. RSA是同态加密
5. GenRSA
6. 硬核谓词：hard-core predicate
    a. 单向函数：损坏不可恢复
    b. 可以恢复一部分词语
    c. {0，1}* 任意长度的函数串
7. RSA-lsb这个实验敌手成功的概率是1/2：加密1bit信息
8. 加密不是1bit信息，
9. 函数与置换：
    a. 单射
    b. 满射
    c. 双射
10. 可证明安全的那一套思路
11. RO模型的秘钥封装机制
12. 1
    a. 查询时间 query
    b. 成功 success
13. 解封装预言机:
    a. 返回的是
14. program ability 可编程的

15. 数字签名
16. 数字签名可以实现三个性质：数据完整性，认证，不可否认性
17. 数字签名与公钥加密对应
    a. 数字签名对自己加密：公开可验证
    b. 指定验证人签名
    c. 签名符合特定的场景
18. 消息认证码：只能实现数据完整性，不是公开可验证的
19. 数字签名开销很大
20. 秘钥生成算法、签名算法（概率算法）、验证算法（输入公钥，消息，签名）
21. 数字签名的安全模型
    a. 敌手伪造合法的签名
    b. 敌手查询签名预言机
    c. 敌手查询的所有消息的集合
    d. 敌手成功输出消息的概率是可以忽略的
    e. 以上成为 existentially unforgettable under anadaptive chosen-message attach
22. RSA的签名与RSA的加密是一个相反的过程，签名用私钥，解密用公钥（不安全）
    a. 为什么不安全?
    b. 敌手是否可以伪造合法的签名对?