Chapter 3 Symmetric&Public Key Cryptography

2017年3月13日　　10:36

By LSY

1. Symmetric(shared key/secure key) Key对称密钥加密算法
   - 加密解密的密钥相同
   - 加密解密双方都需要知道密钥
   - 密钥需要被保密

2. Block Cipher 块加密算法/分组加密
   - 首先是分成固定长度的input块
   - 然后再对块进行组合

3. Feistel Cipher structure
   - Diffusion 扩散——密文和明文统计关系复杂
   - Confusion 扰乱 ——密文和加密关系复杂
     - Block size
     - Key length
     - Number of rounds
     - Sub-key……

4.
   - DES Algorithm
   - Triple DES
     - Backward compatibility

5.mode of Operation
   - ECB:
     - 逐块加密
     - 可能一整块被替代
   - CBC:
     - 与之前的进行异或
     - 与之前的信息有联系，不能被整块修改
   - Stream Cipher 流加密
     - Pseudo-random stream 伪随机流

6. the key distribution problem
   - A can select a key and physically deliver it to B
   - ….

7.Public Key Cryptography 公钥密码学
   - 解决的问题：
     - 密钥触发
     - 数字签名
   - 公钥和私钥不能互相推算，公钥公开，私钥保密

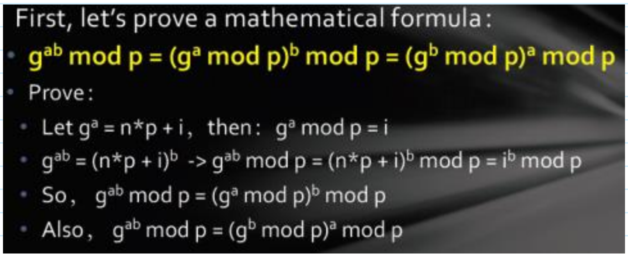
2017/3/15 8:10
Public Key Cryptography
8.
   - 加密是用对方的公钥加密，对方用自己的私钥解密
   - 签名是用自己的私钥签名，对方是用发送者的公钥进行验证
   - 只需要一对公钥和私钥就可以了

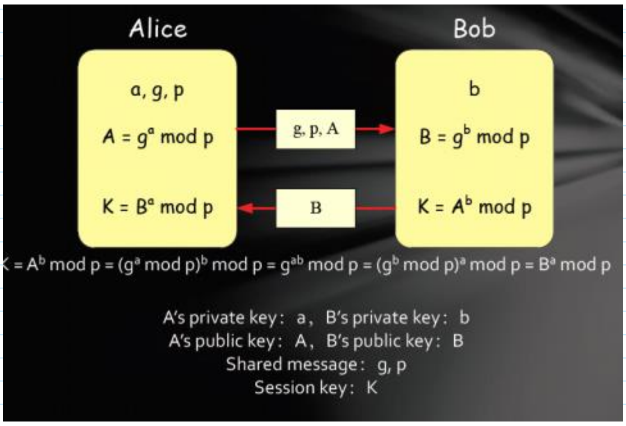
9.
   - Plaintext
   - Public key KU
   - Private key KR
   - Encryption Algorithm
   - Ciphertext
   - Decryption Algorithm

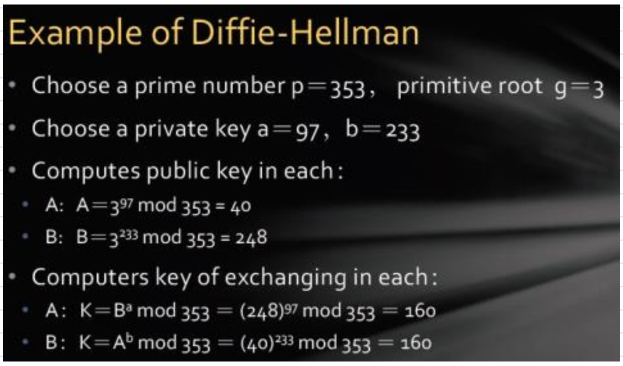
10. requirements:
   - key generation is easy
   - Encryption is acceptable in time
   - Decryption is acceptable in time
   - 知道公钥，不可以推算出私钥
   - 知道公钥和密文，不可以推算出明文
   - 既可以使用在加密，也可以实用在签名

10. one-way function(正向计算很容易，反向计算不可行）
   - Diffie-Hellman Algorithm
     - 缺陷：
       - 至少300-digit
       - 中间可能出现中间人，两边通讯，且双方意识不到

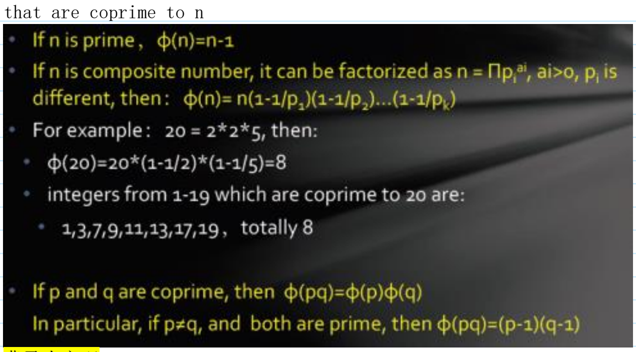
Calculating the remainder of the power of an integer dividing a prime is relatively easy, but calculating the discrete logarithm is very hard:



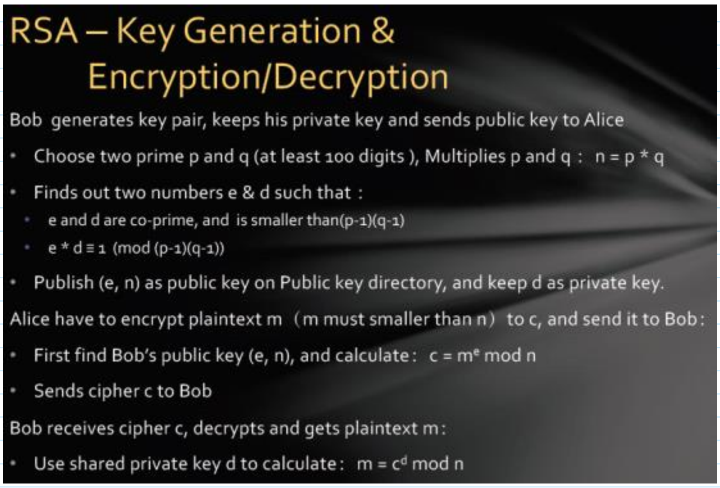




- RSA Algorithm
  - Euler Number: the number of positive integers less than n that are coprime to n



  - 费马小定理
  - Encryption/Decryption
  - RSA证明！！！



2017/3/20 9:58/

1. secure?

- 物理获取私钥或物理肉机之类的
- Marvin knows mis a number between 1 and n, so he couldsearch bruteforcely
- Marvin can try to compute Bob' s private key d from (e, n), and then use Approach 1.

2. 对称密钥 VS 非对称密钥

- 对称
  - 好处：
    - cheap and fast
    - 用硬件很快处理
  - 坏处：
    - 密钥分发
- 非对称
  - 好处：
    - 密钥分发安全性
  - 坏处：
    - expensive and slow
    - 用硬件处理困难，价格高
- 误解
  - 公开密钥加密在防范密码攻击上比常规更加安全（错误）——取决于密钥长度和解密的计算工作量
  - 公开密钥加密使得常规加密过时（错误）——都存在好处和坏处，同时在运用