网络安全

Courses	计算机网络
Done	☑
Status	Done

RSA算法

RSA算法生成公钥和私钥的步骤

1. 选择两个大素数p、q
2. $n = pq \quad and \quad z = (p-1)(q-1)$ （**计算两个数n和z**）
3. $chose\ a\ number\ e,\ \ e < n,\ gcd(e,z) = 1$ （**选择e与z互素**）
4. $given\ e\ chose\ d, ed\ mod\ z = 1$ （**计算d**）
5. 公钥为$K_B^+ = (n,e)$，私钥为$K_B^- = (n,d)$

Alice(Sdr)加密和Bob(Rcv)解密的过程

- pkt：整数m表示的比特组合(**m<n**)
- 执行运算得到明文m的加密值c，$c = m^e\ mod\ n$
- alice send pkt to bob.....
- 执行运算对密文c进行解密，$m = c^d\ mod\ n$

会话秘钥 Session key

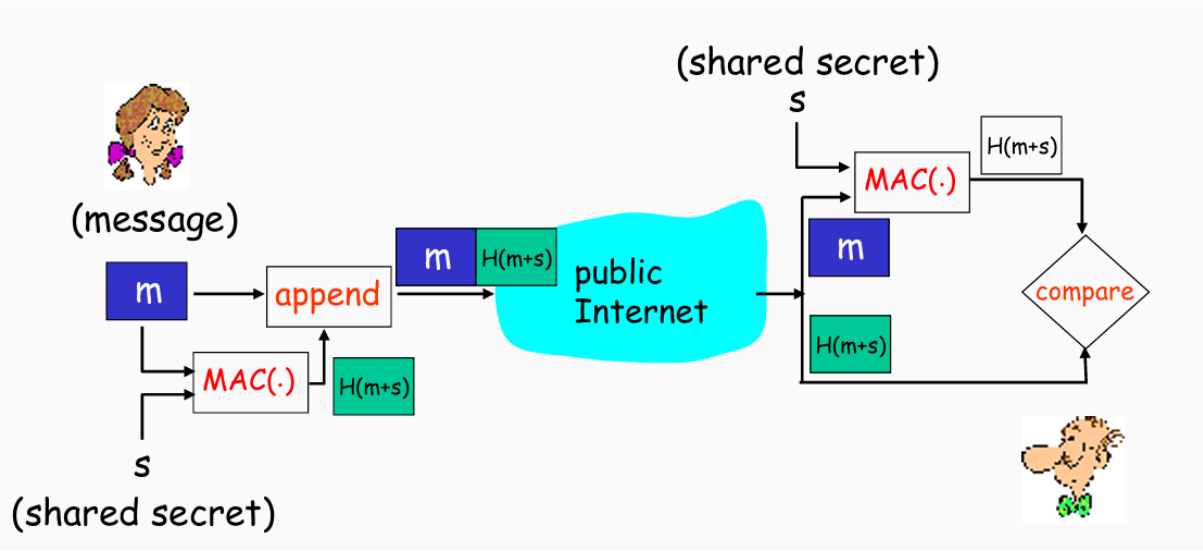
用RSA算法加密一个用于加密数据本身的秘钥K_s

RSA的工作原理

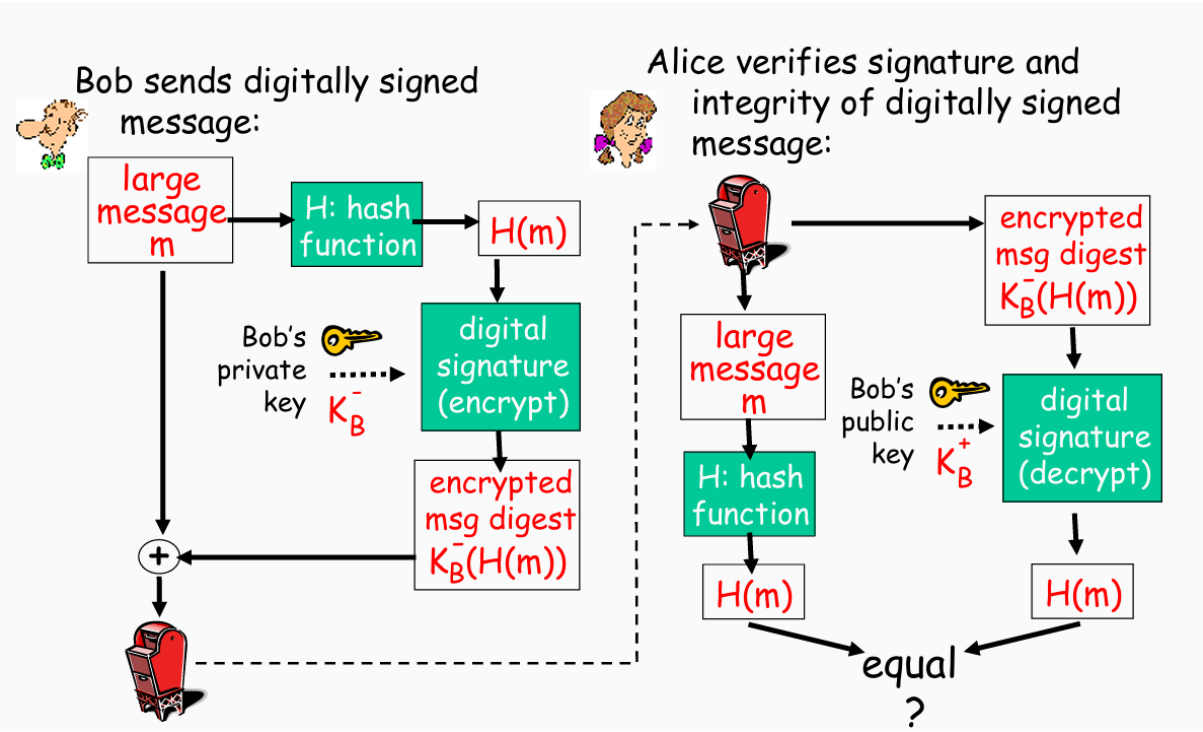
即证$m^{ed}\ mod\ n = m$，运用数论知识证明即可

报文完整性和数字签名

报文鉴别码MAC



数字签名Digital signature



公钥认证

认证中心CA

需要证实你具有的公钥实际上就是你要进行通信的实体的公钥。

证书包括Bob的**公钥**、**身份信息**和**CA的数字签名**

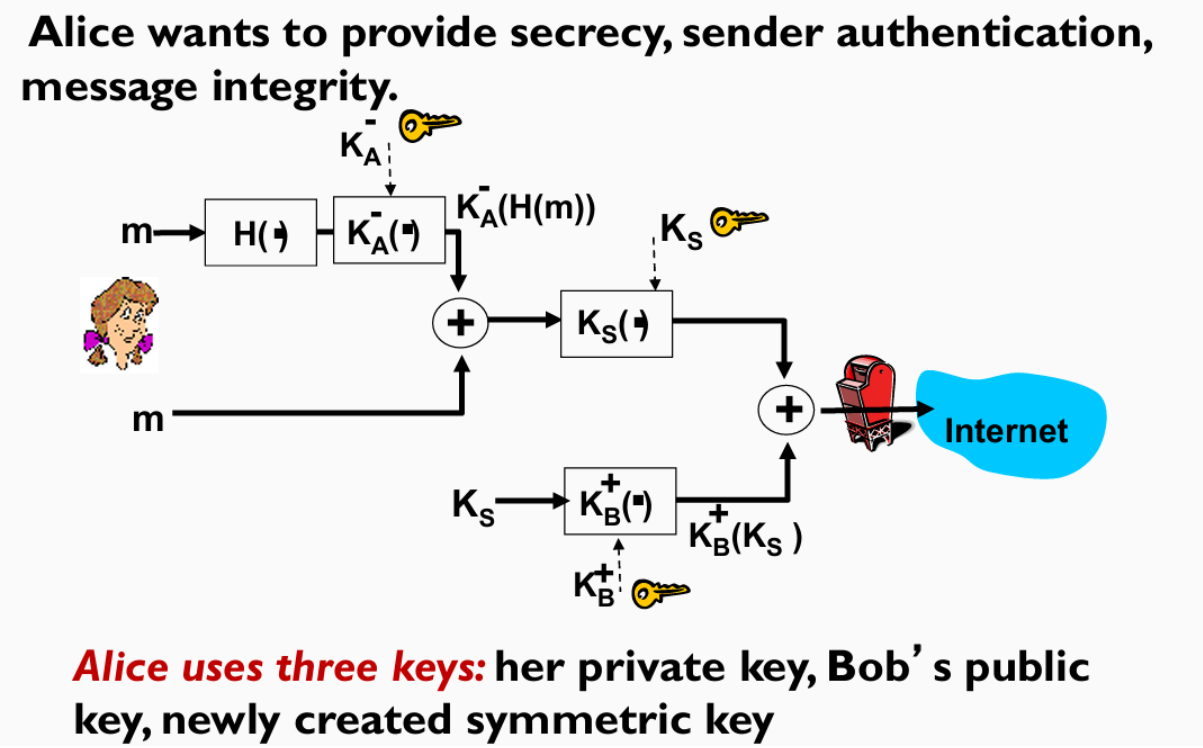
Diffie-Hellman Key Exchange

过程：

- p是一个大素数
- $Z_p^* = \{1, 2, ..., p-1\}(mod\ p)$
- 计算一个`generator` **g**属于ZP*（为全世界所知），g的条件为：$\forall a \in Z_p^*, \exists k \in Z,\ a = g^k (mod\ p)$
- Alice从ZP*中随机选择一个数X，将$g^X\ (mod\ p)$发送给Bob
- Bob同样的随机选择一个Y，将$g^Y\ (mod\ p)$发送给Alice
- A和B的对称密钥即为$g^{XY}\ (mod\ p)$

安全电子邮件

原理：三把密钥



PGP-pretty good privacy

散列函数：MD5/SHA-1

对称密钥加密：CAST、三重DES、IDEA

公开密钥加密：RSA

使TCP连接安全：SSL

HTTPS —使用了SSL

三个阶段：握手、密钥导出、数据传输

握手

三次握手—发送SSL hello—回复证书—交换主密钥MS

密钥导出

安全起见，每个人使用不同的密钥，加密和完整性的检查也使用不同的密钥

四把密钥：

E_B ：Bob→Alice 会话加密密钥

M_B : Bob→Alice 会话MAC密钥

.....