哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

密码学基础（8）

RSA的理论依据?

- 必须满足：$c^d \bmod n = m$，其中$c = m^e \bmod n$
- 可以证明：对于任意x和y，有$x^y \bmod n = x^{(y \bmod z)} \bmod n$
  - 其中$n = pq$，$z = (p-1)(q-1)$
- 因此：

$$
\begin{aligned}
c^d \bmod n &= (m^e \bmod n)^d \bmod n \\
&= m^{ed} \bmod n \\
&= m^{(ed \bmod z)} \bmod n \\
&= m^1 \bmod n \\
&= m
\end{aligned}
$$

RSA: 另一个重要性质

下列性质将非常重要:

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

利用公钥加密，可以利用私钥解密

利用私钥加密，可以利用公钥解密

结果相同!

为什么？

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{de} \bmod n$$

$$= (m^d \bmod n)^e \bmod n$$

RSA为什么安全?

- RSA的安全性建立在“大数分解和素性检测”这个数论难题的基础上
  - 既将两个大素数相乘在计算上容易实现，而将该乘积分解的计算量相当大
- 假设已知Bob的公钥(n,e)，那么有多大难度确定d，即私钥(n,d)?
- 本质上需要在不知道两个因子p和q的前提下，找出n的因子
  - 分解一个大数是很困难的!

RSA的实际应用

- RSA的幂运算强度很大
- DES至少比RSA快100倍
- 实际应用中：
  - 利用公钥加密建立安全连接，然后建立第二个密钥-对称会话密钥，用于加密数据

会话密钥(session key, K_S)

- Bob与Alice利用RSA交换对称会话密钥K_S
- 一旦双方确认K_S，则利用会话密钥加密/解密会话数据

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！