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（7）

公钥密码学

对称密钥加密：

- 需要发送方与接收方知道共享的秘密密钥
- Q: 最初如何商定密钥（尤其“素未谋面”）？

公开密钥加密

- 完全不同的方法 **[Diffie-Hellman76, RSA78]**
- 发送方与接收方无需共享秘密密钥
- 公开密钥（公钥）完全公开
- 私有密钥（私钥）只有接收方知道

公钥加密算法

需求:

① 公钥加密 $K_B^+(-)$ 和私钥解密 $K_B^-(-)$ 需要满足：

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

② 给定公钥 K_B^+，不可能计算得到私钥 K_B^-

RSA: Rivest, Shamir, Adelson algorithm

前提条件：模运算

- x mod n = x除以n的余数
- 事实上：

  [(a mod n) + (b mod n)] mod n = (a+b) mod n

  [(a mod n) − (b mod n)] mod n = (a−b) mod n

  [(a mod n) * (b mod n)] mod n = (a*b) mod n
- 因此：

  $(a \bmod n)^d \bmod n = a^d \bmod n$
- 例如：x=14, n=10, d=2，则

  $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$

  $x^d = 14^2 = 196 \quad x^d \bmod 10 = 6$

RSA: 预备知识

- 报文/信息(message): 仅仅是一个比特模式(bit pattern)
- 每个比特模式可以表示为一个唯一的整数
- 因此，加密一个报文就等价于加密一个数

例如:

- m= 10010001，可以唯一地表示为十进制数145
- 为了加密m，我们可以加密对应的数(145)，得到一个新的数（即密文）

RSA: 生成公钥/私钥对

1. 选择2个大质数*p*和*q*。(e.g., 1024bits的大质数)

2. 计算$n = pq$，$z = (p-1)(q-1)$

3. 选择*e* (满足$e<n$)，使e与z 之间没有公因子，即*e*, *z*互质(relatively prime)

4. 选择*d*使得*ed*-1刚好可以被*z*整除，(即: $ed \bmod z = 1$).

5. 公钥：$\underbrace{(n,e)}_{K_B^+}$；私钥：$\underbrace{(n,d)}_{K_B^-}$.

RSA: 加密、解密

0. 给定公钥 (n,e)和私钥(n,d)

1. 加密报文m $(m<n)$时，计算

$$c = m^e \bmod n$$

2. 解密密文c时，计算

$$m = c^d \bmod n$$

不可思议
事情发生!

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

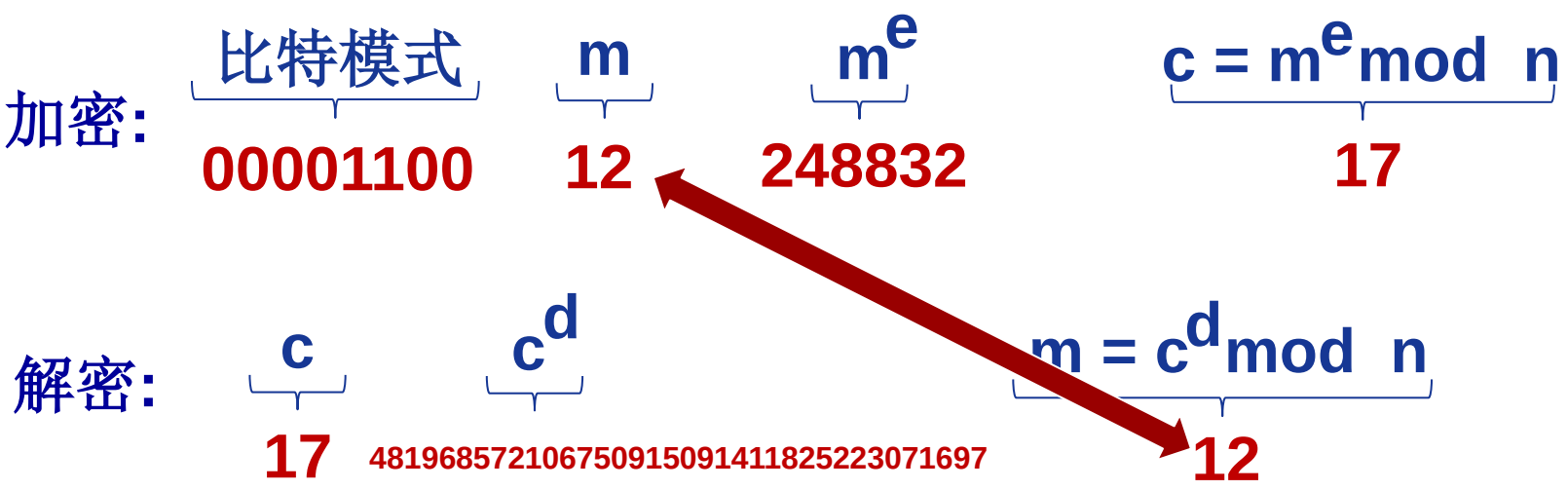
RSA举例

Bob选择p=5, q=7. 于是n=35, z=24.

e=5 (e, z互质).

d=29 (ed-1刚好被z整除).

加密8-bit报文（e.g. 1个字符）。



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！