COURSE TECHNOLOGY
CENGAGE Learning™

AN TOÀN BẢO MẬT THÔNG TIN

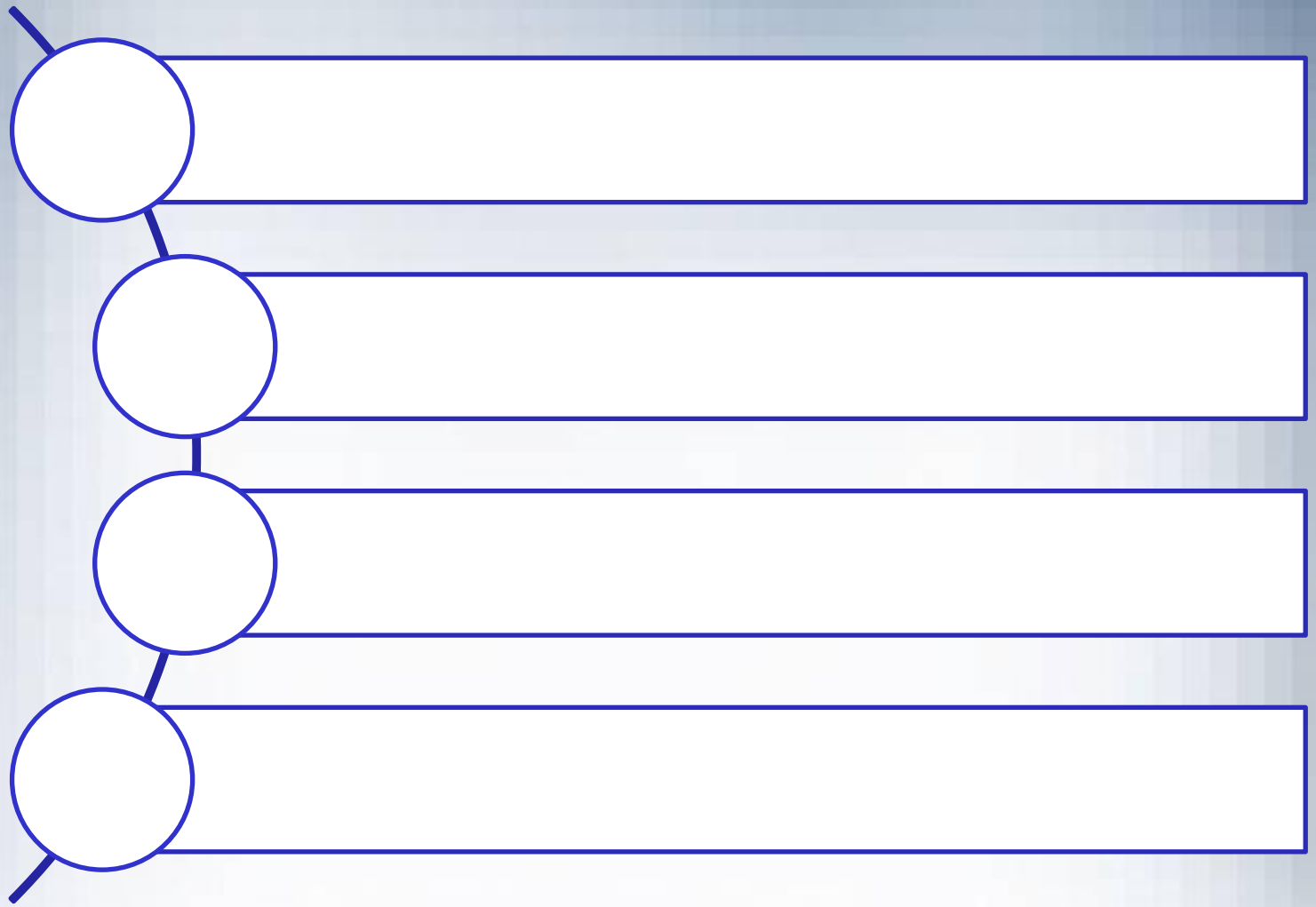
Đàm Quang Viễn

COURSE TECHNOLOGY
CENGAGE Learning™

Chương 4

MẬT MÃ KHÓA CÔNG KHAI

NỘI DUNG



Hệ mã hoá RSA

Để mã hoá mẩu tin, người gửi:

- ✔ Lấy khoá công khai của người nhận KU={e, N}Tính $C=M^e \bmod N$, trong đó $0 \le M < N$. Để giải mã hoá bản mã, người sở hữu nhận:
- ✔ Sử dụng khóa riêng KR={d, p, q} Tính $M=C^d \bmod N$ Lưu ý rằng bản tin M < N, do đó khi cần chia khối bản rõ.

Hệ mã hoá RSA

Ví dụ

1. Chọn các số nguyên tố: p=17 & q=11.
2. Tính $N = pq$, N = 17×11=187
3. Tính $\Phi(N)=(p-1)(q-1)=16\times10=160$
4. Chọn e: gcd(e, 160)=1; Lấy e=7
5. Xác định d: $de=1 \bmod 160$ và $d < 160$

Giá trị cần tìm là d=23, (vì 23×7=161= 1×160+1)

6. In khoá công khai KU={7, 187}
7. Giữ khoá riêng bí mật KR={23, 17, 11}

Hệ mã hoá RSA

Ví dụ áp dụng mã RSA trên như sau:

- Cho mẩu tin M = 88 (vậy 88<187)
- Mã $C = 88^7 \bmod 187 = 11$
- Giải mã $M = 11^{23} \bmod 187 = 88$
- Có thể dùng định lý phần dư Trung Hoa để giải mã cho nhanh như sau:

Hệ mã hoá RSA

Định lý Trung Hoa để A mod M

- Phân tích $M=m_1 \times m_2 \times m_3 \times \ldots \times m_k$
  - Tính $M_i = M/m_i$ với i=1, 2,…,k
  -Tính $a_i = A \bmod mi.$ với I =1, 2,…,k
  - Tính $c_i = M_i \times (M_i^{-1} \bmod m_i)$ $1 \le I \le k$

Sau đó sử dụng công thức

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) \bmod M$$

Hệ mã hoá RSA

Ta có $m_1 = 11, m_2 = 17, M_1 = 17, M_2 = 11$

a. Tính $a_1 = 11^{23} \bmod 11 = 0$

Tính $a_2 = 11^{23} \bmod 17 = (-6)^{23} \bmod 17 =$

$(-6)^{16}(-6)^4 (-6)^2 (-6)^1 \bmod 17 = 1.\ 4.\ 2\ .(-6) \bmod 17 = 3$

Vì $(-6)^2 \bmod 17 = 2$, nên $(-6)^4 \bmod 17 = 4$,

$(-6)^8 \bmod 17 = -1$ nên $(-6)^{16} \bmod 17 = 1$

b. $M_1^{-1} = 17^{-1} \bmod 11 = (6)^{-1} \bmod 17 = 2$

$M_2^{-1} = 11^{-1} \bmod 17 = (-6)^{-1} \bmod 17 = 14$

nên $c_1 = 17.(17^{-1} \bmod 11) = 17.2$

nên $c_2 = 11.(11^{-1} \bmod 17) = 11\ (14 \bmod 17) = 154$

Vậy $M = 0.34 + 3.154 \bmod 178 = 462 \bmod 187 = 88$

Lược đồ trao đổi khóa Diffie – Hellman

Giả sử p là số nguyên tố đủ lớn, α là phần tử nguyên tử trong Z_p. Khi đó lược đồ trao đổi khóa giữa A và B như sau:

- Bước 1: A chọn ngẫu nhiên (bí mật) một số nguyên được ký hiệu là r_A ($0 \le r_A < p-2$)
- Bước 2: A tính $\alpha^{r_A} \bmod p = S_A$ và gửi cho B
- Bước 3: B chọn ngẫu nhiên (bí mật) một số nguyên được ký hiệu là r_B ($0 \le r_B < p-2$)
- Bước 4: B tính $\alpha^{r_B} \bmod p = S_B$ và gửi cho A
- Bước 5: A tính $K_A = S_B^{r_A} \bmod p$, B tính $K_B = S_A^{r_B} \bmod p$

Bài tập của học viên

Câu 1: Cho hệ mã hóa RSA với p=3, q=11, e=3

a. Hãy tìm khóa công khai KU và khóa bí mật KR
b. Hãy thực hiện mã hóa chuỗi M=4 và giải mã ngược lại bản mã có được.

Bài tập của học viên

Câu 2: Cho hệ mã hóa RSA với p=5, q=7, e=5

a. Hãy tìm khóa công khai Ku và khóa bí mật Kr

b. Hãy thực hiện mã háo chuỗi “secure” và giải mã ngược lại bản mã có được.

Câu 3 Cho hệ mã hóa RSA có p = 103, q = 113, e = 71. Hãy tìm khóa công khai Ku và khóa bí mật Kr của hệ mã trên. Sau đó mã hóa thông điệp X= 1102 và giải mã ngược lại kết quả nhận được.