2. HỆ MẬT MÃ RSA

2. Thuật toán RSA

- ***Giai đoạn tạo khóa RSA***
- Chọn ngẫu nhiên 2 số nguyên tố p, q khác nhau
- Tính: $n = p * q$ và $\varphi(n) = (p-1) * (q-1)$
- Chọn số nguyên e sao cho: $1 < e < \varphi(n)$ và là số nguyên tố cùng nhau với $\varphi(n)$, tức là: $\gcd(e, \varphi(n)) = 1$
- Tính d theo công thức: $d = e^{-1} mod\ \varphi(n)$
- Xác định khóa:
  - Khóa công khai: $K_p = \{e, n\}$
  - Khóa bí mật: $K_s = \{d, n\}$

2. HỆ MẬT MÃ RSA

2. Thuật toán RSA

- ***Giai đoạn mã hóa RSA***
- Thông điệp ban đầu M, sao cho: $0 < M < n$
- Sử dụng khóa công khai $K_p = \{e, n\}$ để tính thông điệp mã hóa C (ciphertext):

$$C = M^e mod\ n$$

2. HỆ MẬT MÃ RSA

2. Thuật toán RSA

- ***Giai đoạn giải mã RSA***
- Dữ liệu cần giải mã: bản mã hóa C
- Sử dụng khóa bí mật $K_s = \{d, n\}$ để tính lại thông điệp gốc M từ thông điệp đã mã hóa C:

$$M = C^d mod\ n$$

Ví dụ minh họa

2. HỆ MẬT MÃ RSA

2. Thuật toán RSA

- *Ví dụ 2.1*: Cho hai số nguyên tố p, q và e có giá trị như sau:

  $p = 11$, $q = 17$, $e = 7$, M = 88

Tính khóa công khai, khóa bí mật ?

Thực hiện mã hóa, giải mã ?

Giai đoạn sinh khóa	Ví dụ:
Chọn p, q là 2 số nguyên tố khác nhau	Cho: p = 11, q = 17
Tính: $n = p * q$	n = p*q = 11*17 = 187
Tính: $\varphi(n) = (p-1) * (q-1)$	φ(n) = (p- 1)*(q-1) = (11-1)*(17-1) = 160
Chọn số nguyên e sao cho: $1 < e < \varphi(n)$ và gcd $(e, \varphi(n)) = 1$	Cho: e = 7, thỏa mãn: gcd $(7, 160) = 1$
Tính: $d = e^{-1} mod\ \varphi(n)$	$d = 7^{-1} mod\ 160 = 23$
Khóa công khai: $K_p = \{e, n\}$	$K_p = \{7, 187\}$
Khóa bí mật: $K_s = \{d, n\}$	$K_s = \{23, 187\}$

Giai đoạn mã hóa	Ví dụ:
Bản rõ M, với $M < n$	M = 88
Bản mã $C = M^e mod\ n$	$C = 88^7 mod\ 187 = 11$

Giai đoạn giải mã	Ví dụ:
Bản mã C	$C = 11$
Bản rõ $M = C^d mod\ n$	$M = 11^{23} mod\ 187 = 88$