MẬT MÃ KHÓA CÔNG KHAI

Giáo viên: Phạm Nguyên Khang
pnkhang@cit.ctu.edu.vn

Hệ mật mã khóa công khai

- Các giải thuật mật mã khóa công khai sử dụng một khóa để mật hóa và một khóa khác có liên quan để giải mật. Chúng có các đặc điểm:
  - Không thể tính lại khóa giải mật nếu biết trước giải thuật mật hóa và khóa dùng mật hóa.
  - Một trong hai khóa đều có thể dùng để mật hóa và khóa còn lại dùng đề giải mật.

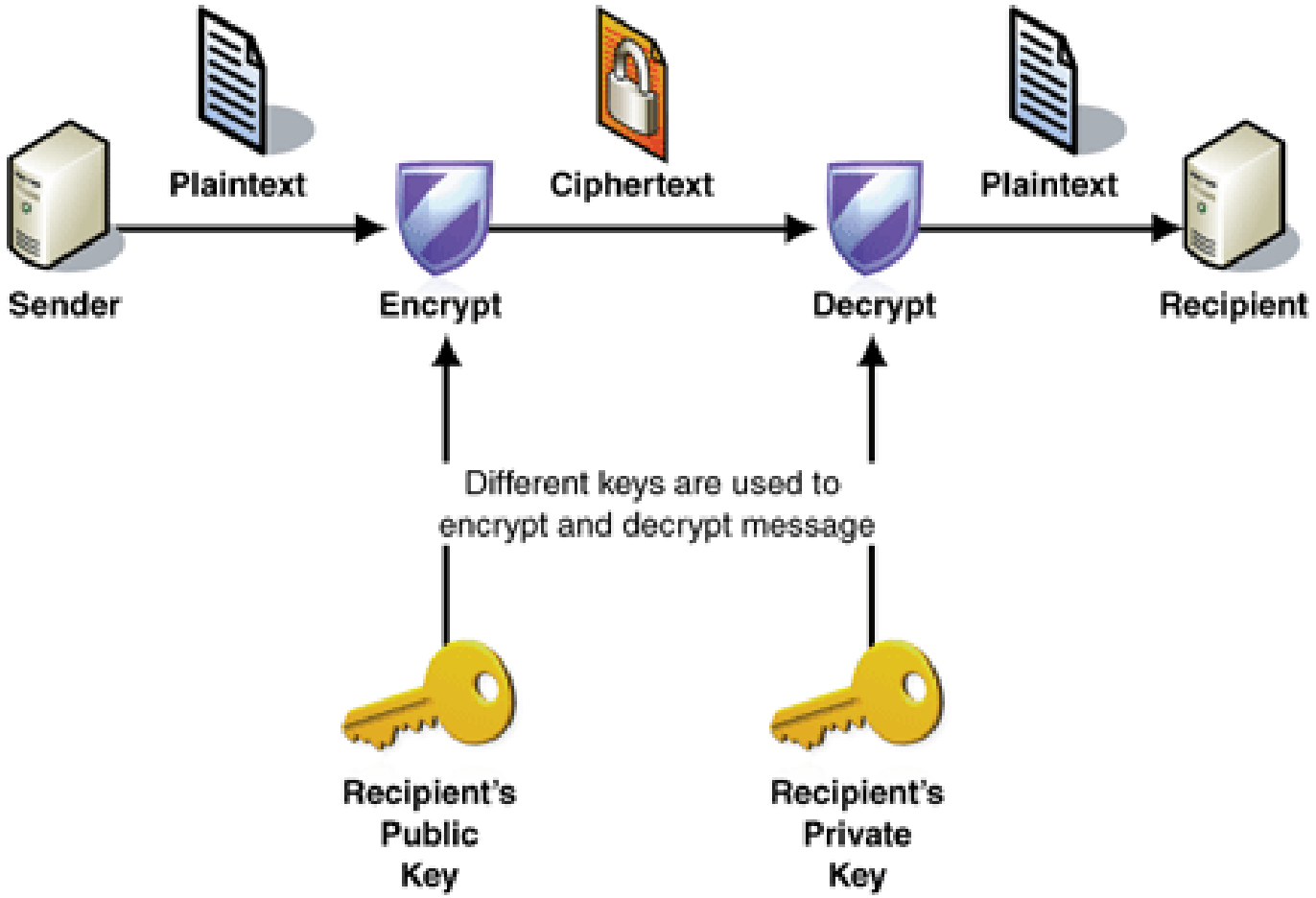
Hệ mật mã khóa công khai

- Giải thuật khóa công khai gồm 6 thành phần:
  - Bản rõ: thông điệp có thể đọc, đầu vào của giải thuật
  - Giải thuật mật hóa
  - Khóa công khai và bí mật: một cặp khóa được chọn sao cho 1 khóa dùng để mật hóa và 1 khóa dùng để giải mật.
  - Bản mật: thông điệp đầu ra ở dạng không đọc được, phụ thuộc vào bản rõ và khóa. Nghĩa là với cùng một thông điệp, 2 khóa khác nhau sinh ra 2 bảng mã khác nhau
  - Giải thuật giải mật

Hệ mật mã khóa công khai

- Các bước thực hiện:
  - Mỗi người dùng tạo một cặp khóa để mã hóa và giải mã
  - Mỗi người dùng đăng ký một trong 2 khóa làm **khóa công khai** sao cho mọi người đều có thể truy cập được. Khóa còn lại được giữ **bí mật**.
  - Ví dụ:
    - Nếu Bob muốn gởi một thông điệp mật đến Alice, anh ta mã hóa thông điệp bằng khóa công khai của Alice.
    - Khi Alice nhận thông điệp, cô ta giải mã thông điệp bằng khóa bí mật của mình. Không ai ngoài Alice có khả năng giải mã vì chỉ Alice có khóa bí mật của mình.

Hệ mật mã khóa công khai



Hệ mật mã khóa công khai

- Các yêu cầu:
  - Dễ dàng tính được cặp khóa công khai K_p và bí mật K_s
  - Dễ dàng tính được bảng mã với bảng rõ và khóa công khai cho trước:
    - $C = E_{Kp}(M)$
  - Dễ dàng tính được bảng rõ từ bảng mã và khóa bí mật cho trước:
    - $M = D_{Ks}(C) = D_{Ks}[E_{Kp}(M)]$
  - Không thể tính được K_s từ K_p cho trước.
  - Không thể tính được bảng rõ M từ khóa K_p và bản mã cho trước
  - Mật mã hóa và giải mã được thực hiện theo một trong hai quá trình:
    - $M = D_{Ks}[E_{Kp}(M)] = D_{Kp}[E_{Ks}(M)]$

Giải thuật RSA

- Được phát triển bởi Rivest, Shamir và Adleman.
- Mật mã hóa và giải mật mã được tính theo công thức:
  - $C = M^e \bmod n$
  - $M = C^d \bmod n$
- Các yêu cầu:
  - Có thể tìm được các giá trị e, d, n sao cho
    - $M^{ed} \equiv M \pmod n$ với mọi $M < n$
  - Dễ dàng tính được M^e và C^d với mọi $M < n$
  - Không thể tính được d từ e và n

Giải thuật RSA

- Giải thuật:
  - Chọn 2 số nguyên tố lớn p và q
  - Tính n = p * q
  - Tính φ(n) = (p-1) * (q-1)
  - Chọn e sao cho USCLN(e, φ(n)) = 1 với 1 < e < φ(n)
  - Tính d sao cho ed ≡ 1 (mod φ(n))

Giải thuật RSA

- Khóa công khai $K_p = \{e, n\}$
- Khóa bí mật $K_s = \{d, n\}$

- Ví dụ: tìm cặp khóa bí mật và công khai với p=7 và q=19. Thực hiện mã hóa và giải mã với M=6.

Giải thuật tính a^c mod n

```
1. c = 0;
2. d = 1;
3. for i = k downto 1 do
6.   if b_i = 1 then
4.     c = c × 2 + 1;
5.     d = (d × d × a) mod n;
6.   else
7.     c = c × 2;
8.     d = (d × d) mod n;
9. return d;
```

Ứng dụng

- SSL (Secure Socket Layer)
  - Giao thức **https**
- SSH (Secure shell)