**Chapter 03: Mã hóa key công khai**

Người dùng sẽ có 2 khóa 1 public và 1 private.

**Khi A gửi dữ liệu cho B**, **A sẽ dùng public key của B để mã hóa**. B sẽ dùng private key của B để giải mã dữ liệu nhận được.

Khi A muốn ký chữ ký số cho mình: A sẽ dùng private key cuả mình ký vào, bên B sẽ dùng public key của A để kiểm tra chữ ký số.

Ngày nay, thường dùng khóa công khai để mã hóa key của mã hóa đối xứng**. Vì giải thuật mã hóa khóa công khai sử dụng tốt khi mã hóa lượng dữ liệu nhỏ, dữ liệu lớn thường tốn nhiều thời gian**.

Giải thuật RSA dựa trên độ khó của việc “phân tích số nguyên tố”.