Bài 2 Ví dụ về khoảng cách duy nhất trong mật mã

Nhân Nguyễn Văn

April 2025

Bối cảnh

Chúng ta đang phân tích tính an toàn của hệ thống mã hoá bí mật. Trong đó, **khoảng cách duy nhất** (unicity distance) cho biết số lượng ký tự bản mã tối thiểu mà kẻ tấn công cần có để phá mã bằng cách thử hết tất cả các khóa (brute-force).

Thông số giả định

- Entropy của khoá: $H(k) = 40$ bits.
  Nghĩa là có khoảng 2^{40} khóa khác nhau có thể được dùng.
- Độ dư thừa thông tin của ngôn ngữ: $D = 2$ bits/ký tự.
  Vì ngôn ngữ tự nhiên (như tiếng Việt, tiếng Anh) thường có từ, cụm từ lặp lại → không phải ký tự nào cũng mang thông tin mới.

Tính toán khoảng cách duy nhất

$$U = \frac{H(k)}{D} = \frac{40}{2} = 20$$

Kết quả: Kẻ tấn công chỉ cần có đủ **20 ký tự bản mã** là đã có thể phá mã bằng brute-force.

Ví dụ đời thực dễ hiểu

Giống như chơi trò **"đoán mật khẩu"**:

- Nếu bạn chỉ thấy 2–3 ký tự đầu tiên, bạn có quá nhiều lựa chọn → không thể đoán đúng.
- Nhưng nếu bạn thấy **đủ 20 ký tự được mã hóa**, bạn sẽ có đủ thông tin để loại bỏ tất cả các mật khẩu sai.
- Khi đó, chỉ còn lại đúng một khoá phù hợp → bạn có thể giải mã toàn bộ tin nhắn.

Kết luận đơn giản

- Khoảng cách duy nhất U là ngưỡng an toàn: dưới mức này, mã vẫn an toàn; vượt ngưỡng này, hacker có thể phá mã.
- Cần thiết kế hệ thống sao cho U thật lớn $\rightarrow$ dù hacker có nhiều bản mã, cũng không thể tìm ra khóa đúng.