**THE PROVABLE SECURITY MINDSET**

*1. Các kiến thức cần có:*

- Logs & Exponents

- Modular Arithmetic (n|x nghĩa là x = kn với vài số nguyên k)

- Modulo Operation

- Binary Strings - {0,1}n là tập hợp các chuỗi nhị phân n-bits

. - Xác suất:

+ Phân phối: gán xác suất cho mỗi kết quả.

+ Phân phối đồng đều: :Pr[𝑥]= 1 |𝒳| với tất cả 𝑥∈𝒳

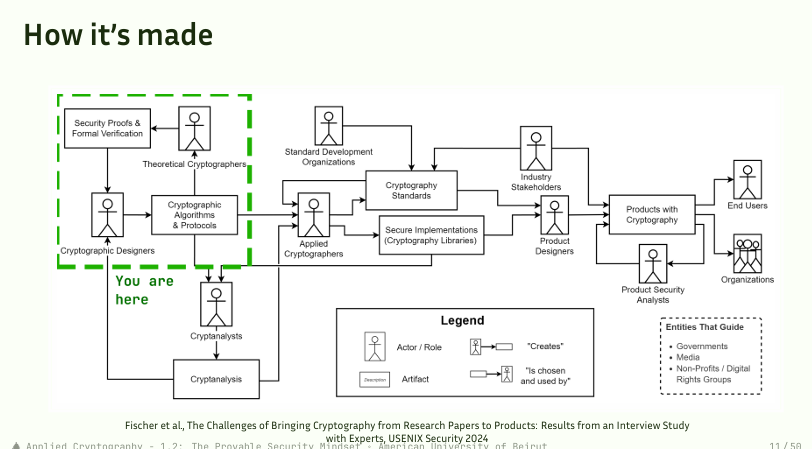
- Chú thích của mã giả:

+ 𝑥 ↞ 𝒳: lấy mẫu x đồng đều từ tập hợp

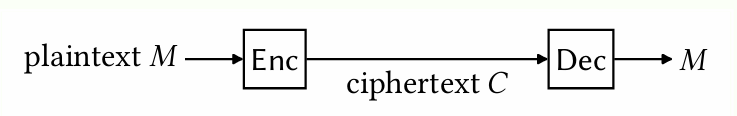
+ 𝑥 := 5: gán 5 vào biến 𝑥

+ 𝑥  y: kiểm tra nếu x bằng y (trả về true/false)

*2. Cách mà Cryptography được tạo ra:*



*3. Cách mà Cryptography hoạt động:*



- Một **văn bản thường M** đi qua **công cụ mã hóa Enc** sẽ cho ra kết quả một **đoạn text đã được mã hóa C**, cũng từ **C đi qua công cụ giải mã Dec** sẽ cho ra kết quả là **một văn bản gốc M trước khi được mã hóa**.

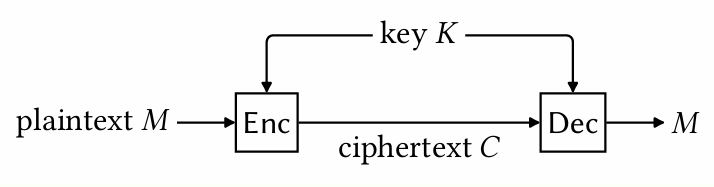
- Ưu điểm: Kẻ tấn công không biết cách mà mật mã hoạt động

- Nhược điểm:

+ Nếu tìm được cách hoạt động có nghĩa là đã bẻ khóa thành công.

+ Không được để lộ mật mã công khai.

+ Mọi người cần tạo mật mã của riêng mình.



- Với cấu trúc này:

+ Mật mã có thể công khai, được dùng bởi bất cứ ai.

+ Thiết kế được công khai bất cứ lúc nào ngoại trừ khóa là bí mật.

+ Đây là cách hầu hết mọi phương pháp mật mã được thiết kế ngày nay.

*4. One-time pad:*

**- Khái niệm:** OTP, sổ mật mã một lần, là một loại kỹ thuật mã hóa có độ bảo mật hoàn hảo về mặt lý thuyết. Đây là hệ mật mã duy nhất được chứng minh là không thể bị bẻ khóa. Hoạt động bằng cách kết hợp văn bản gốc (plaintext) với một khóa ngẫu nhiên, bí mật và chỉ được sử dụng duy nhất một lần.

**- Điều kiện để hệ thống OTP đạt được sự an toàn tuyệt đối:**

+ Khóa phải được tạo ra một cách hoàn toàn ngẫu nhiên.

+ Khóa là duy nhất và không bao giờ được sử dụng lại cho bất kỳ văn bản gốc nào khác.

+ Khóa phải có độ dài ít nhất bằng với độ dài văn bản gốc.

+ Khóa phải được giữ bí mật hoàn toàn giữa người gửi và người nhận.

**- Cách để chứng minh được tính bảo mật:**

+ Mật mã được coi là an toàn nếu kẻ phản biện không thể phân biệt được đầu ra từ các cuộc gọi tới ATTACK với những dữ liệu ngẫu nhiên.

+ Nếu khóa là ngẫu nhiên thì đầu ra sẽ được phân phối đồng đều