Bài tập: Môn "Cấu trúc dữ liệu và giải thuật"

Lớp: IT003.O21.CTTN

Chủ đề: ***Mật mã học cơ bản***

Học kì II - Năm học: 2023-2024

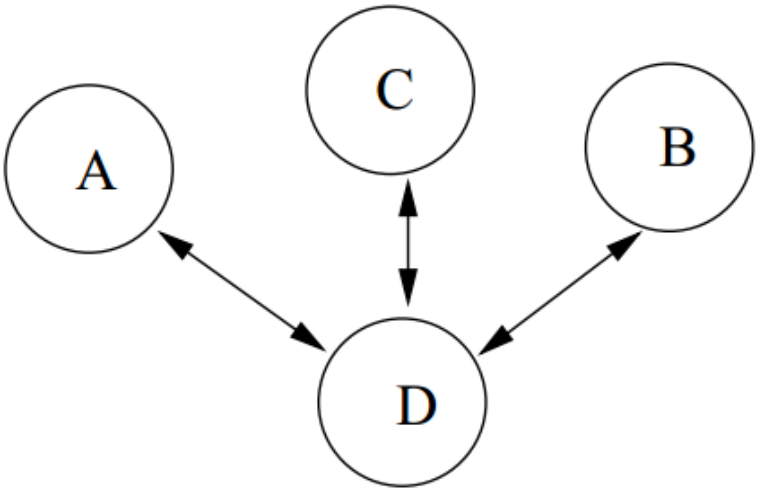
GV phụ trách chủ đề: ThS. Phan Thế Duy – Email liên lạc: duypt@uit.edu.vn

Yêu cầu chung:

+ Làm theo nhóm 03 thành viên, báo cáo bài nộp ghi đầy đủ MSSV – Họ tên của các thành viên trong nhóm.
+ Nộp theo deadline trên hệ thống https://courses.uit.edu.vn/
+ Bài nộp bao gồm: file báo cáo (định dạng word) + code chương trình (nếu có). Tất cả nén thành 01 file duy nhất có tên định dạng MSSV1_MSSV2_Ten1_Ten2. (ví dụ: 20521220_20521552_AnhKha_TranMinh)

Bài tập gồm 04 câu hỏi, tham khảo các tài nguyên bài giảng đã cung cấp và chỉ dẫn thích hợp trên CryptoHack để thực hiện bài tập này.

Câu 01: Giả sử có một hệ thống mã hóa bao gồm các nút A, B, C, và D như bên dưới (Hình 1).



Hình 1. Hệ thống mã hóa bao gồm 4 nút

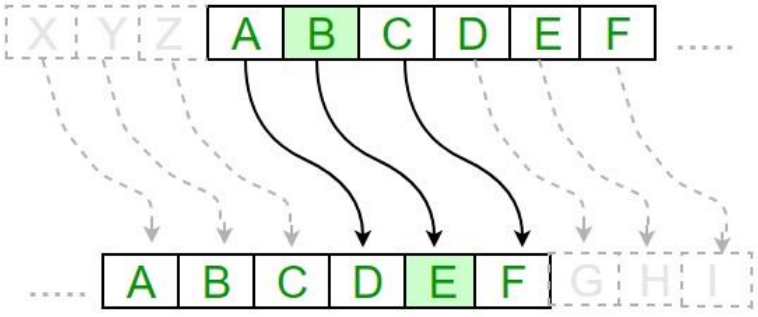
(a) Cần bao nhiêu chìa khóa đối xứng (symmetric key) được sinh ra để A, B, C có thể trao đổi thông tin 2 chiều an toàn với nút D sử dụng thuật toán mã hóa đối xứng?

(b) Thay thế thuật toán mã hóa đối xứng bằng hệ thống mã hóa công khai (mã hóa bất đối xứng). Cần bao nhiêu khóa công khai (public key) được tạo ra để đáp ứng yêu cầu giao tiếp an toàn giữa A, B, C với nút D?
(c) Như câu b, cần bao nhiêu chìa khóa công khai để mỗi nút trong mạng có thể giao tiếp an toàn với các nút còn lại?
(d) Giả sử chúng ta có 8 nút trong hệ thống như trên. Cần bao nhiêu chìa khóa đối xứng (symmetric key) để mỗi nút có thể giao an tiếp an toàn với các nút còn lại?
(e) Giả sử chúng ta mở rộng mạng lưới trên thêm một nút. Xác định số lượng các khóa cần phải tạo thêm để mỗi nút trong mạng có thể giao tiếp an toàn hai chiều (xét cả hai trường hợp: hình thức mã hóa đối xứng và mã hóa bất đối xứng)

Câu 02: Hình 2 mô tả hoạt động của mã hóa Caesar, một dạng mã hóa cổ điển cơ bản và đơn giản. Caesar là dạng mã hóa thay thế (substitution cipher), trong đó mỗi kí tự trong văn bản rõ (plaintext) được thay thế với một kí tự ở vị trí cố định tương ứng trong bảng chữ cái.

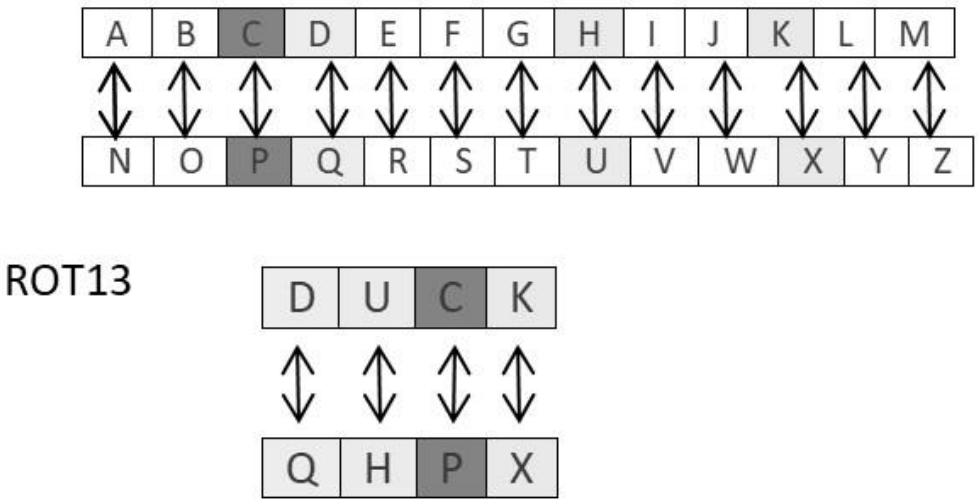
Yêu cầu:

(a) Viết mã chương trình C++ cho phép thực hiện mã hóa Caesar trên dữ liệu đầu vào là plaintext và shift pattern (độ dịch chuyển) trong bảng chữ cái.
(b) Giải mã thuật toán mã hóa Caesar bằng kỹ thuật vét cạn (Brute Force attack). Mô tả cách làm và viết chương trình C++ minh họa.



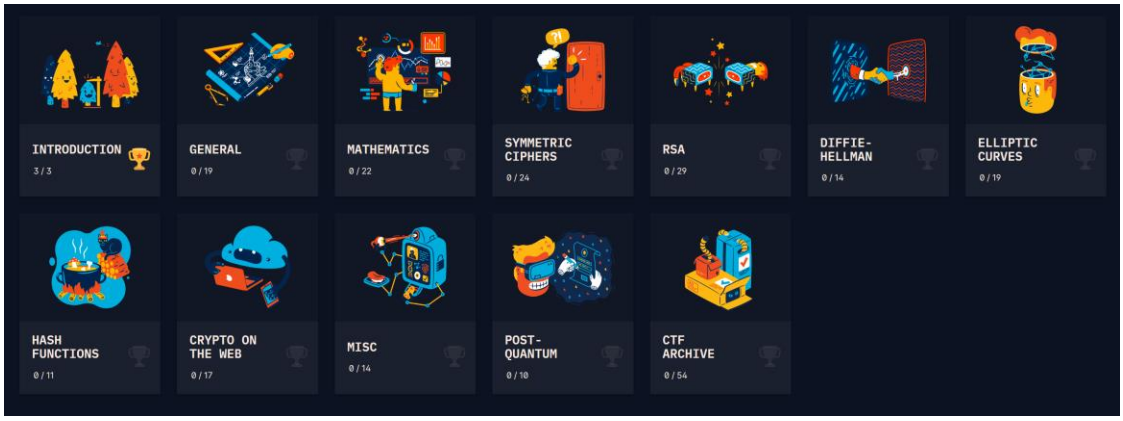
Hình 2. Mã hóa Caesar

Câu 03: Kỹ thuật mã hóa ROT13 (Rotate by 13 places) là một trường hợp đặc biệt của mã hóa Caesar với độ dời cố định luôn là 13. Mỗi chữ cái được dịch chuyển 13 vị trí để mã hóa và giải mã thông điệp (Hình 03). Viết chương trình C++ cho phép thực hiện mã hóa và giải mã thông điệp bằng thuật toán ROT13. Xác định số trường hợp cần phải thử khóa để giải mã. Nhận xét về khả năng bị bẻ khóa, thám mã.



Hình 3. Mã hóa ROT13

Câu 04: Đăng ký tài khoản trên trang web: https://cryptohack.org/, sau đó thực hiện các yêu cầu bên dưới (trình bày rõ ràng kết quả, phân tích từng bước và ảnh chụp màn hình trong quá trình thực hiện - nếu có).



Hình 4. Một số dạng thử thách trên trang CryptoHack

Phần này có một số câu yêu cầu kĩ năng lập trình Python cơ bản.

(a) Sinh viên hoàn thành các Thử thách nằm ở các mục Introduction, General, Mathematics để làm nền tảng, phát triển kỹ năng cho chủ đề mật mã học.
(b) Hoàn thành các thử thách trong mục SYMMETRIC CIPHER, bao gồm: Block Ciphers, Stream Ciphers.
(c) Hoàn thành các thử thách trong mục RSA, với các tiểu mục nằm trong STARTER, PRIMES PART 1, PUBLIC EXPONENT, PRIMES PART 2, PADDING, SIGNATURES PART 1, SIGNATURES PART 2.
(d) Hoàn thành tất cả các thử thách trong mục DIFFIE-HELLMAN.
(e) Hoàn thành các yêu cầu trong Hash Functions

(f) Các mục khác: Sinh viên tự thực hành thêm để phát triển kỹ năng về thuật toán mã hóa (không bắt buộc)

Hình 5. Hệ thống thực hành mã hóa CryptoHack

-HẾT-