Võ Nguyên Chương – 21520011

Liêu Minh Nhật – 21520377

Bài tập 1:

a) **Trả lời**: Cần **4 khóa đối xứng** để A, B, C trao đổi thông tin 2 chiều an toàn với D. Vì nếu D dùng chung khóa đối xứng với (giả sử) A và B thì B hoàn toàn giải mã được thông điệp giữa A và D (ngược lại A cũng có thể giải mã thông điệp giữa B và D)

b) **Trả lời**:
   - Giao tiếp **2 chiều**: Để A, B, C có thể giao tiếp 2 chiều an toàn với D thì mỗi người cần có một bộ khóa công khai riêng, suy ra cần ít nhất **4 bộ khóa** bất đối xứng. Khi đó nếu muốn gửi thông điệp cho (giả sử) A thì mã hóa thông điệp bằng public_key của A, và A muốn giải mã sẽ dùng private_key của mình (A là người duy nhất sở hữu)
   - Giao tiếp **1 chiều**: Để A, B, C có thể gửi thông điệp cho D thì chỉ cần **1 bộ khóa** công khai của D là đủ.

c) **Trả lời**: Cũng như ý b giao tiếp 2 chiều giữa các nút trong mạng muốn an toàn thì mỗi nút đều có bộ khóa (pulic_key, private_key) riêng nên đáp án là **4**

d) **Trả lời**: Cũng như ý a, để 2 nút bất kì giao tiếp an toàn với nhau bằng khóa đối xứng thì khóa chung giữa các cặp nút phải khác nhau (nếu trùng thì nút khác có thể dùng khóa đó để giải mã) vậy đáp án là: 8C2 = 8*(8-1)/2 = **28** (khóa)

e) **Trả lời**:
   - Dùng khóa đối xứng: cần ít nhất: 5C2 = 5*(5 – 1)/2 = **10** (khóa)
   - Dùng khóa bất đối xứng: cần ít nhất: **5** (khóa)

Bài tập 2:

a) Chương trình mã hóa Caesar: (file caesar.cpp)

b) Ý tưởng giải mã Caesar bằng bruteforce: vì có tất cả 26 chữ cái (xét bảng chữ cái tiếng Anh) nên ta chỉ cần thử key từ 0 tới 25 để giải mã, xem thử văn bản nào có nghĩa thì đó chính là văn bản gốc cần tìm.
   Chương trình giải mã Caesar bằng bruteforce: (file brute_caesar.cpp) trong file có ví dụ minh họa

Bài tập 3:

- Chương trình mã hóa ROT13: đây chỉ là trường hợp đặc biệt của mã Caesar nên ta dùng chương trình caesar.cpp với key = 13 để mã hóa ROT13. Việc giải mã hoàn toàn như mã hóa vì:

$c = p + 13 \pmod{26}$

$\Rightarrow c + 13 = p + 13 + 13 = p \pmod{26}$

Bài tập 4:

- Toàn bộ code trong Folder Cryptohack (có tải lên github: https://github.com/vnc1106/Crypto-IT003)
- Profile cryptohack: https://cryptohack.org/user/__VNC__/