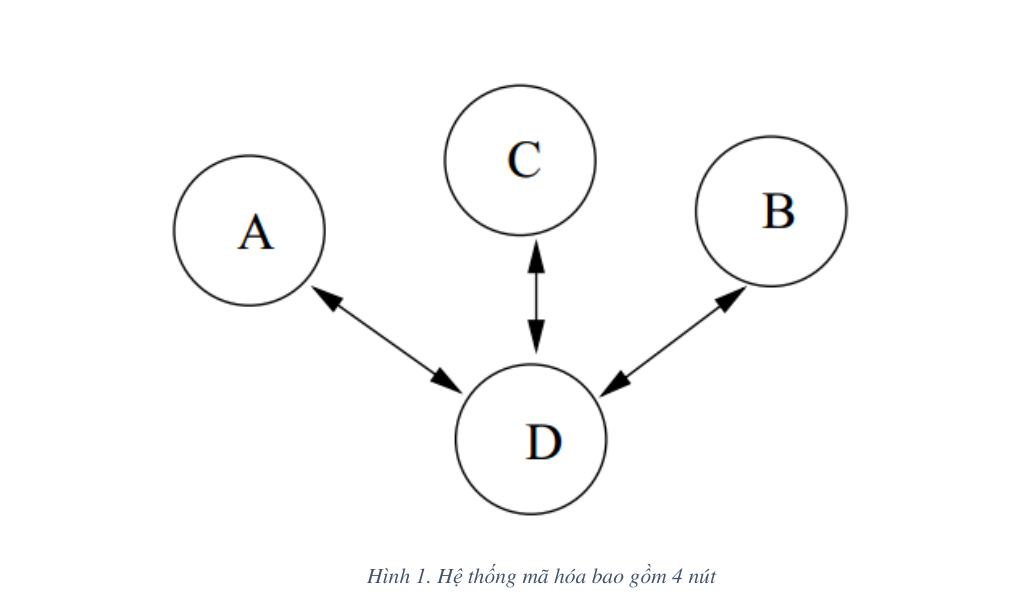
**Câu 01: Giả sử có một hệ thống mã hóa bao gồm các nút A, B, C, và D như bên dưới (Hình 1).**



1. 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?

Cần sử dụng 3 chìa khóa đối xứng để A, B, C có thể trao đổi thông tin 2 chiều an toàn với D vì mỗi kết nối (ví dụ A-D, C-D) sẽ cần 1 chìa khóa đối xứng.

1. 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?

Cần 4 chìa khóa công khai để đáp ứng được nhu giao tiếp an toàn giữa A, B, C với nút D vì mỗi nút sẽ cần có một public key để giao tiếp

(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?

Vẫn chỉ cần 4 chìa khóa công khai để mỗi nút trong mạng giao tiếp an toàn với các nút còn lại( mỗi nút sử dụng 1 chìa khóa công khai)

(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?

Vì mỗi nút sẽ giao tiếp với các nút còn lại, nên để giao tiếp an toàn thì mỗi kết nổi giữa 2 nút sẽ cần 1 chìa khóa đối xứng, do đó cần tổng cộng 8\*7/2 = 28 chìa khóa đối xứng.

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)

Trường hợp mã hóa đối xứng: khi thêm 1 nút nữa thì tổng cộng sẽ có 9 nút, mỗi nút sẽ giao tiếp với các nút còn lại nên sẽ cần 9\*8/2 = 36 chìa khóa đối xứng, tăng thêm 36-28 = 8 chìa khóa.

Trường hợp mã hóa bất đối xứng: khi thêm 1 nút nữa thì sẽ chỉ cần thêm 1 public key cho nút mới nên chỉ tăng 1 chìa khóa.

**Câu 2:**

Chương trình C++ được sử dụng như sau:

Khi chạy chương trình sẽ được prompt chọn 1 trong 3 mode:

+) Mode 1 là để encrypt một plaintext và shift cho trước( nhập plaintext trên 1 dòng và nhập shift trên 1 dòng).( Giải câu 2a)

Cách làm của mode này khá đơn giản, chỉ cần shift từng kí tự trong bảng chữ cái 1 số đơn vị cho trước( từ input). Không shift dấu “ “.

+) Mode 2 là decrypt sử dụng brute force và in ra mọi trường hợp có thể của text lúc chưa bị decrypt( nhập text trong 1 dòng) (1 cách giải câu 2b)

Cách làm của mode này cũng tương tự như mode 1, nhưng thử với tất cả các trường hợp shift có thể và in ra 25 trường hợp( xét theo bảng chữ cái tiếng anh có 26 chữ cái)

+) Mode 3 là decrypt sử dụng brute force và chỉ in ra 1 trường hợp có khả năng là text cần tìm cao nhất.( cách giải khác có thể tốt hơn của câu 2b)

Cách làm của mode này tương tự như mode 2 nhưng với mỗi text sau khi được shift thì ta sẽ xét từng từ trong text đó, text có nhiều số từ xuất hiện nhiều trong từ điển nhất sẽ được in ra. Ffile words được kèm theo gồm có 123985 từ trong tiếng anh. File words này thực ra là file ở đường dẫn /usr/share/dict/words