**ÔN TẬP AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**Câu 1:** Hãy trình bày các giao thức thực hiện bảo mật, cách thức bảo vệ hệ thống khởi sự xâm nhập và phá hoại từ bên ngoài.

*Gợi ý: trình bày các giao thức thực hiện bảo mật (Keberos, X509, SSL, PGP và S/MIME, IPSET).*

*Các thức bảo vệ: khái niệm Control Access (kiếm soát truy cập) dùng cho việc bảo vệ này (chứng thực và phân quyền), đồng thời sử dụng Firewall hoặc các hệ thống phát hiện chống xâm nhập IDS/IPS, kiểm lỗi phần mềm.*

**Câu 2:** Trình bằng mô hình mã và giải mã khối Electronic Codebook – ECB, những ưu điểm và nhược điểm của ECB, CBC, CFB, OFB, CTR.

Ví dụ: ECB:

* Mô hình ECB.

Vẽ mô hình ra.

* Ưu điểm và nhược điểm

*Ưu điểm:*

* *Đơn giản*
* *Không cần đồng bộ hóa giữa bên gửi và nhận, nếu bên nhận không nhận đủ các khối, thì vẫn có thể giải mã các khối nhận được.*
* *Các bit lỗi sẽ không được đưa vào các khối kế sau.*
* *Vì các khối được mã hóa và giải mã hoàn toàn độc lập với nhau nên ECB cho phép mã hóa và giải mã đồng thời nhiều khối nếu có đủ phần cứng thực thi.*

*Nhược điểm:*

* *ECB về bản chất giống hệt với các mật mã bảng chữ cái cổ điển, chỉ có điều bảng chữ cái của ECB phức tạp hơn.*
* *Các khối bản rõ giống nhau sẽ được ánh xạ thành khối bản mã giống nhau (nếu dùng cùng 1 loại khóa), dẫn đến dễ tấn công bằng phương pháp thống kê tần suất.*
* *ECB dễ dàng bị phá nếu bản rõ lớn và có tính cấu trúc rõ ràng, từ đó ECB thường dùng để mã hóa những bản rõ ngắn như khóa bí mật.*
* *ECB song song hóa được, có cấu trúc quy luật -> độ an toàn yếu.*

**Câu 3:** Nêu các hình thức tấn công trong quá trình truyền thông tin trên mạng máy tính, cho ví dụ với từng hình thức tấn công.

*Gợi ý:*

* *Thay đổi thông điệp*
* *Mạo danh*
* *Phát lại thông điệp*
* *Ngăn chăn thông tin*

**Câu 4:** Hãy trình bày các yêu cầu của một hệ thống truyền thông tin an toàn và bảo mật, cho biết vai trò của mật mã học trong việc bảo vệ thông tin trên mạng.

*Gợi ý:*

*Tính bí mật (Confidentiality): bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép.*

*Tính toàn vẹn (Integrity): Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.*

*Tính sẵn sàng (Availability): Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu*

*Tính chống thoái thác (Non-repudiation): Khả năng ngăn chặn việc từ chối một hành vi đã làm*

*Vai trò: Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các dịch vụ như xác thực, bảo mật, toàn vẹn dữ liệu, chống chối bỏ*

**Câu 5:** Định nghĩa, định lý và tính chất của hàm Euler.

* Hàm phi euler
* Nếu φ (p) là số nguyên tố, dễ thấy φ(p)=p−1.
* Nếu φ (p^k) thì φ(p^k)=p^k−p^k−1
* Nếu φ (p1p2) (với p1≠p2) thì φ(p1p2)=φ(p1)×φ(p2)

<https://www.youtube.com/watch?v=re-zp5ObjXE>

  φ(29) = 28 (29 is prime)

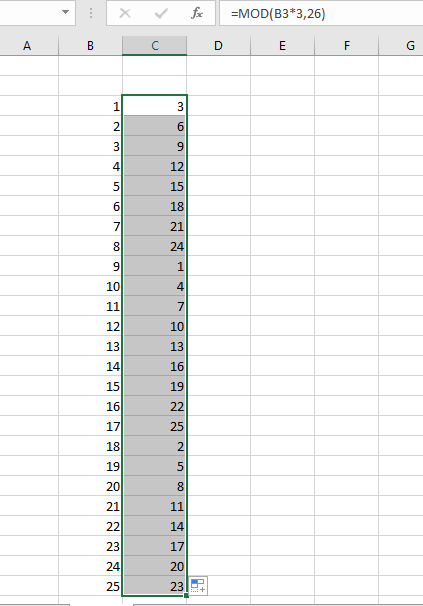
  φ(100) (định lý 2) = φ(4\*25) = φ(2^2\*5^2) = φ(2^2)\* φ (5^2) = 2^2-2^1 \* 5^2-5^1 = 2\*20=40

  φ(6) = φ(2\*3)

**Câu 6:** Học thuộc tập Z26, N\* là gì?

* Tìm phần tử nghịch đảo của 1 số trong tập 26

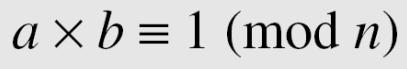
Mod(1->25\*socantim,26) = 1



Video tham khảo

<https://www.youtube.com/watch?v=D47Rya_CAgk>

Câu 7: Tìm tổng khả nghịch của 1 số có công thức

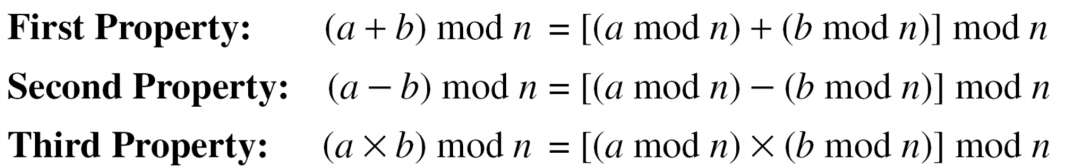


**Câu 8:** Định lý fermat và tính bài toán:

Dạng 1: Nếu P là số nguyên tố và a>0 không chia hết cho P thì ap-1 mod P dư 1

Dạng 2: nếu P là số nguyên tố và a>0 thì ap mod P dư a

Và triển khai nhớ áp dụng các



**Câu 9:** trao đổi khóa Diffie Hellman

* Khởi tạo khóa như thế nào?
* Các bước trao đổi khóa như thế nào?

Các bước trao đổi khóa:

B1: A và B sẽ thống nhất chọn hai số a(anpha) và Q.

B2: A và B chọn hai số ngẫu nhiên xa và xb.

B3: A tính Ya = a(anpha)xa mod Q

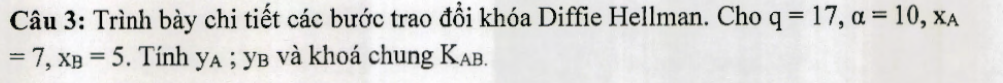
B4: B tinh Yb = a(anpha)Xb mod Q.

B5: A gửi Ya cho B và B gửi Yb cho A.

B6: A tính YbXa mod Q.

B7: B tính YaXbmod Q.

Ví dụ:



Ya = 10^7 mod 17 = 5

Yb = 10^5 mod 17 = 6

Tính khóa chung của A: 6^7 mod 17 =14

B: 5^5 mod 17 = 14

**Câu 10:** Nêu nhược điểm của mã hóa khóa công khai?

**Câu 11:** Trình bày quá trình tạo khóa và mã hóa của RSA ?

**Câu 12:** Trình bày các giải pháp trao đổi khóa công khai? Cho biết hoàn cảnh áp dụng từng giải pháp?

**Câu 13:** Giải thích tính an toàn của giải pháp trao đổi khóa bí mật sử dụng hệ mã hóa công khai ?

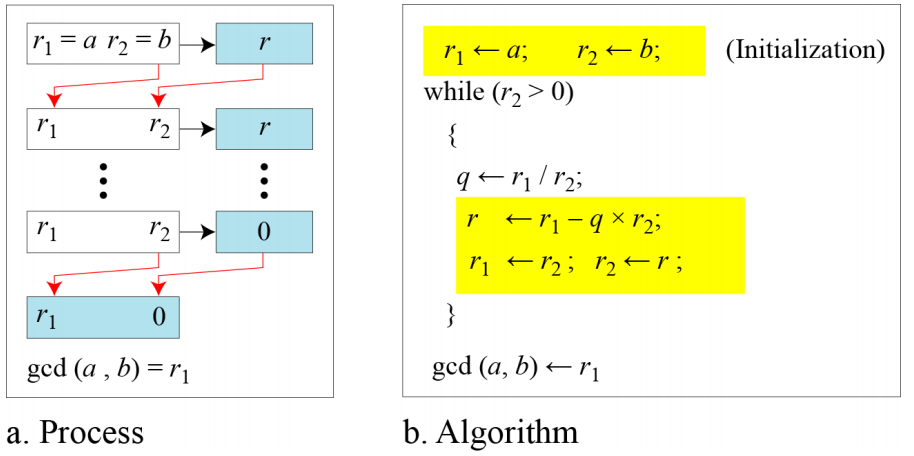
**Câu 14:** Các phương pháp Ceasar, mã hóa đơn bảng, đa bảng, one-time pad dùng nguyên tắc gì để mã hóa?

**Câu 15:** Phương pháp hoán vị dùng nguyên tắc gì để mã hóa?

**Câu 16:** Tại sao phương pháp mã hóa đơn bảng có thể bị tấn công phá mã dùng thống kê tần suất?

**Câu 17:** Định lý RSA, cách phát sinh khóa RSA, mã hóa và giải mã trong RSA?

Câu 18: sử dụng thuật toán Euclidean để tìm tổng khả nghịch:

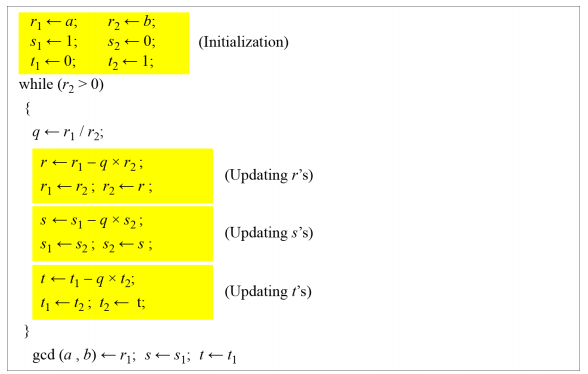


**Ví dụ:**

Find the greatest common divisor of 2740 and 1760?

Find the greatest common divisor of 25 and 60?

Câu 19: thuật toán euclidean mở rộng (Extended Euclidean Algorithm)



**Ví dụ:**

Given a = 161 and b = 28, find gcd (a, b) and the values of s and t

Câu 20: **Hàm Euler-Phi:**

(φ (1)=0,

φ (p) = p-1: nếu p là số nguyên tố, (DL1)

φ (a\*b) = φ a \* φ b (a và b là 2 số nguyên tố cùng nhau là 2 số nguyên có ước chung lớn nhất là 1, ví dụ: 3 và 5 ước lớn nhất là 1, 125 và 8 có ước lớn nhất là 1) (DL2)

φ (P^a) = P^a – P^a-1 nếu P là số nguyên tố và a là số nguyên dương) (DDL3)

Câu 21: **Định lý Euler:**

Dạng 1: nếu a và n là số nguyên tố cùng nhau thì a ^ φ (n) == 1 (mod n)

Dạng 2: Nếu a và n là 2 số nguyên thì a^( φ (n)+1) ==a (mod n)

Câu 22: Định lý nhỏ Fermat:

Nếu P là số nguyên tố, a số bất kỳ >0 và không chia hết cho P thì có a^p-1 mod p = 1.

Nếu P là số nguyên tố, a>0 thì a^P mod P = a.

Câu 23: Mã hóa Ceasar: Ý tưởng lấy từng ký tự của bảng rõ + với khóa K để ra bản mã

mã hóa: C = (p + k) mod 26

Giải mã: p = (C – k) mod 26

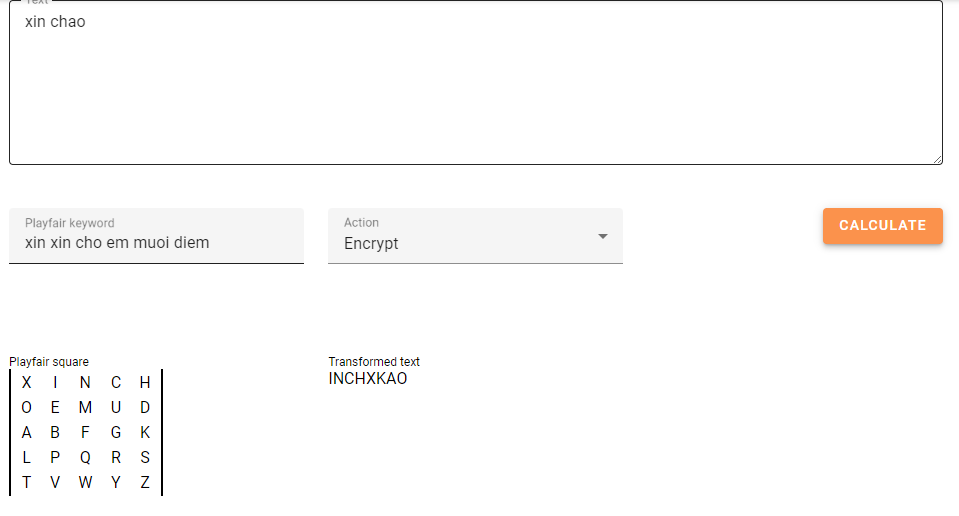
Ví dụ: meet me after the toga party

K=3

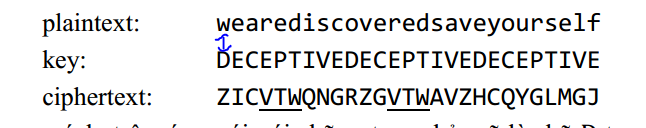
Z26 = A B C D E F G H I J K L M N O P Q S R T U V W X Y Z

Bảng mã: PHHW PH DIWHU WKH WRJD SDUWB

Câu 24: Mã Playfair: Mã hóa Playfair xem hai ký tự đứng sát nhau là một đơn vị mã hóa, hai ký tự này được thay thế cùng lúc bằng hai ký tự khác. Playfair dùng một ma trận 5x5 các ký tự keyword như sau: (chỉ lấy những ký tự không trùng nhau trong khóa, khi mã hóa lấy từng cặp của bảng rõ đi so sánh trong bảng 5x5 theo nguyên tắc: 2 ký tự cùng hàng thì sẽ lấy 2 ký tự kế tiếp, nếu cùng cột thì 2 ký tự kế tiếp trong cột, nếu là đường chéo thì lấy đường chéo lại)



Câu 25: Mã hóa Vigenere: Tạo ra bảng 26x26 chữ cái. Cho bảng rõ và khóa (khóa sẽ được lặp lại cho đến khi bằng chiều dài bảng rõ). Sau đó lấy ký tự bảng rõ (Cột) so với khóa (dòng) để tìm ký tự giao nhau:



Câu 26: Mã Rail Fence: Ý tưởng ghi các ký tự theo từng hàng trong bảng có số cột bằng khóa. Ghi từ trên xuống

Ví dụ:  
CHAOCACBANHOCMONANTOANBAOMATTHONGTIN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| C | H | A | O | C | A |
| C | B | A | N | H | O |
| C | M | O | N | A | N |
| T | O | A | N | B | A |
| O | M | A | T | T | H |
| O | N | G | T | I | N |

Bảng mã C = CCCTOO HBMOMN …..

Câu 27: Thuật toán RSA

Câu 28: Thuật toán DES

Câu 29: Thuật toán AES

**Bài tập:**

**Câu 1:**  gián các số cho các ký tự (in hoa) (A = 0, B = 1, …, Z = 25), tìm và giải thích:

  (A + N) mod 26 = (0+13) mod 26 = 13 => N

  (A + 6) mod 26

  (Y − 5) mod 26

  (C − 10) mod 26 =

  ((K − 2) mod 26 + (T − 10) mod 26) mod 26

  ((G − 10) mod 26 + (X − 17) mod 26 + (L − 15) mod 26)mod 26

Câu 2: Liệt kê các cặp số theo tổng khả nghịch (multiplicative inverse) modulus 20, 40, 30…

modulus 20: (1,1),(3,7),(9,9), (11,11),(13,17),(19,19)  
Các giải: euclidean, Dùng excel mod(1-25\*1-25,26)=1

Câu 3: Sử dụng hàm Euler-Phi, tìm:

  φ(29) = 28 (29 is prime)

  φ(100) (định lý 2) = φ(4\*25) = φ(2^2\*5^2) = φ(2^2)\* φ (5^2) = 2^2-2^1 \* 5^2-5^1 = 2\*20=40

  φ(6) = φ(2\*3)

Câu 4: Sử dụng định lý nhỏ Fermat, tìm:

  (515 mod 13) = (513+2 mod 13) = ((513 mod 13)\* (52 mod 13))mod 13 = (5\*12)mod 13 =8

  (1518 mod 17)

  (751 mod 18)

  (1559 mod 23)

**159137 mod 31 =16**

Câu 5: Alice chọn p=11 & q=3, e = 3 hãy tính khóa KRU và KRA, Đồng thời mã hóa và giải mã với M =15 (theo mật mã bảo mật và mật mã chứng thực).

B1: Tính N = q\*P = 11\*3 = 33

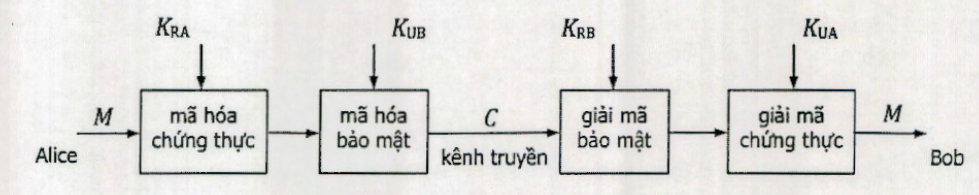
B2: φ(n)=(p-1)\*(q-1) = 20

B3: ng ta cho biết e rồi = 3

B4: d : d.e mod φ(n) dư 1 => d.3 mode 20 dư 1 -> d =7

B5: khóa công khai Ku=(e,N) = (3,33), khóa riêng bí mật Kr = (d,p,q) = (7,11,11)

Ý 2: B1: mã hóa chứng thực



C’ = E(M,Kra(alice)) = Mda mod N = 15^7 mod 33 = 27

B2: mã hóa bảo mật

C = E(C’,Kua(alice)) = C’ea mod N = 27^3 mod 33 =15

B3: giải mã bảo mật

M’ = D(C,Kra(alice)) = Cd mod N = 15^7 mod 33 =27

B4: giải mã chứng thực

M’’ = D(M’,Kua(alice)) = M’e mod N = 27^3 mod 33 = 15

* M và M’’ bằng nhau nên mã hóa và giải mã thành công.

Câu 6: Alice chọn p=15 & q=8, e = 5 hãy tính khóa KRU và KRA, Đồng thời mã hóa và giải mã với M =15 (theo mật mã bảo mật và mật mã chứng thực).

Câu 7: Cho p = 5, q= 11, e = 7. Tính khóa riêng (d, N) trong phương pháp RSA.

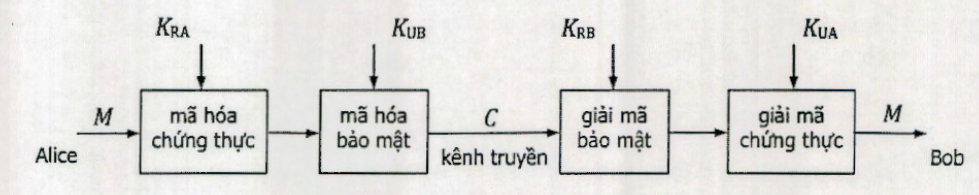
Câu 8: Cho p = 11, q= 13, e = 11. Tính khóa riêng (d, N) trong phương pháp RSA

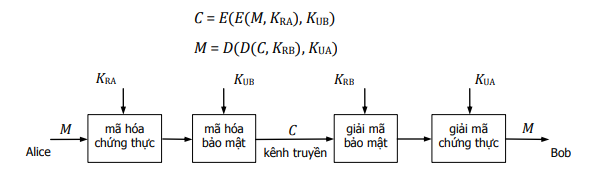
Câu 9: Thực hiện mã hóa và giải mã bằng phương pháp RSA với p = 3, q = 11, e = 7, M = 5 theo hai trường hợp mã hóa bảo mật và mã hóa chứng thực.

Câu 10: Alice chọn p = 7, q = 11, e = 17, Bob chọn p = 11, q = 13, e = 11:

a. Tính khóa riêng KRA của Alice và KRB của Bob

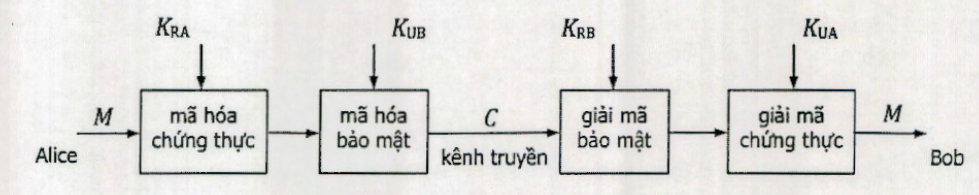
b. Alice muốn gởi cho Bob bản tin M = 9 vừa áp dụng chứng thực và bảo mật như ở sơ đồ dưới. Hãy thực hiện quá trình mã hóa và giải m.





Câu 11: Alice chọn p = 7, q = 11, e = 17, Bob chọn p = 11, q = 3, e = 3:

a. Tính khóa riêng KRA của Alice và KRB của Bob

b. Alice muốn gởi cho Bob bản tin M = 9 vừa áp dụng chứng thực và bảo mật như ở sơ đồ dưới. Hãy thực hiện quá trình mã hóa và giải m.

Câu 12: cho q = 71, anpha = 7, XA = 5, XB = 12 hãy tính YA, YB và khóa chung KAB.

Câu 13: cho q = 11, anpha = 2, XA = 9, XB = 3 hãy tính YA, YB và khóa chung KAB.

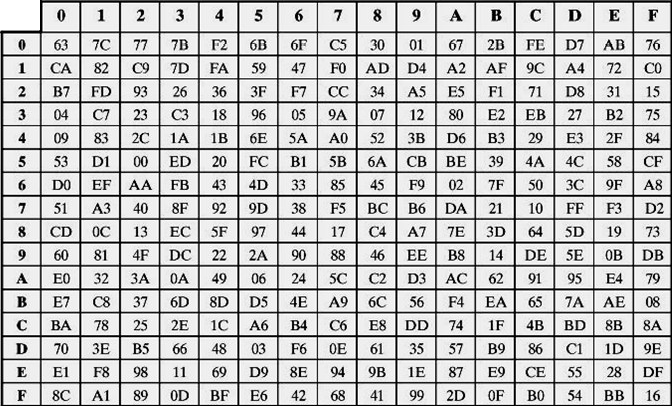
Câu 14: cho q = 17, anpha = 10, XA = 7, XB = 5 hãy tính YA, YB và khóa chung KAB.

Xét thuật toán tạo sub-key trong AES, Sub-key trong Vòng 7 là:

{AA1E2662 24BEC276 006D5115 09AC4E89}

Hãy tính Sub-key trong vòng 8?

Cho S-Box:



Hằng số vòng:

