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 khỏi 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 (kiểm 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 3.1: Cách thức hoạt động của tấn công ransomware thường là:

- Xâm nhập vào hệ thống: Kẻ tấn công thường sử dụng các phương tiện như email lừa đảo, trang web độc hại, hoặc lợi dụng các lỗ hổng trong phần mềm để xâm nhập vào hệ thống của nạn nhân.

- Mã hóa dữ liệu: Sau khi xâm nhập vào hệ thống, ransomware sẽ bắt đầu mã hóa dữ liệu trên máy tính hoặc hệ thống, bao gồm tất cả các tệp tin, hình ảnh, tài liệu và các loại dữ liệu khác mà nạn nhân có trên máy tính.

- Yêu cầu tiền chuộc: Khi dữ liệu đã bị mã hóa, kẻ tấn công sẽ hiển thị thông điệp yêu cầu tiền chuộc trên màn hình của nạn nhân, thông báo về việc mã hóa dữ liệu và yêu cầu nạn nhân trả một khoản tiền chuộc để nhận được khóa giải mã.

- Giao dịch tiền chuộc: Nếu nạn nhân chấp nhận trả tiền chuộc, kẻ tấn công sẽ cung cấp cho họ khóa giải mã để khôi phục dữ liệu của mình. Tuy nhiên, không có đảm bảo rằng nạn nhân sẽ thực sự nhận được khóa giải mã sau khi đã thanh toán tiền chuộc.

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^$^{k-1}$ (p là số nguyên tố)
- Nếu φ (p1p2) (với p1≠p2) thì φ(p1p2)=φ(p1)×φ(p2) (p1 và p2 là số nguyên tố)

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

✔ φ(29) = 28 (29 is prime)

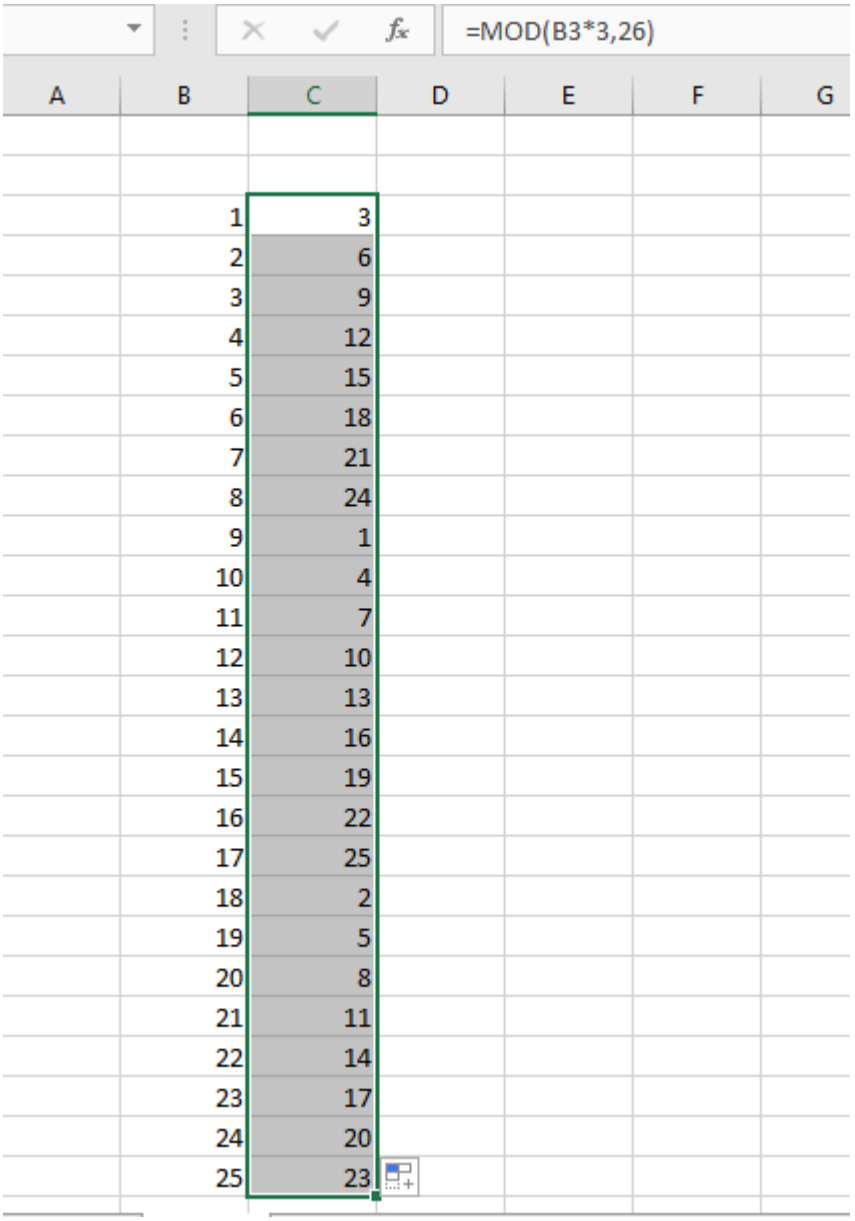
✔ φ(100) (định lý 2) = φ(4*25) = φ(2^2*5^2) = φ(2^2)* φ (5^2) = 2^2-2^1 * 5^2-5^1 = 2*20=40

✔ φ(6) = φ(2*3)

Câu 6: Học thuộc tập Z_{26}, 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

$$a \times b \equiv 1 \pmod{n}$$

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 a^{p-1} mod P dư 1

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

Và triển khai nhớ áp dụng các

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

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 x_a và x_b.

B3: A tính $Y_a = a(anpha)^{x}_{a}$ mod Q

B4: B tinh $Y_b = a(anpha)^{X}_{b}$ mod Q.

B5: A gửi Y_a cho B và B gửi Y_b cho A.

B6: A tính Y_b^{Xa} mod Q.

B7: B tính Y_a^{Xb} mod Q.

Ví dụ:

Câu 3: Trình bày chi tiết các bước trao đổi khóa Diffie Hellman. Cho q = 17, α = 10, x_A = 7, x_B = 5. Tính y_A ; y_B và khoá chung K_{AB}.

Y_a = 10^7 mod 17 = 5

Y_b = 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 ?

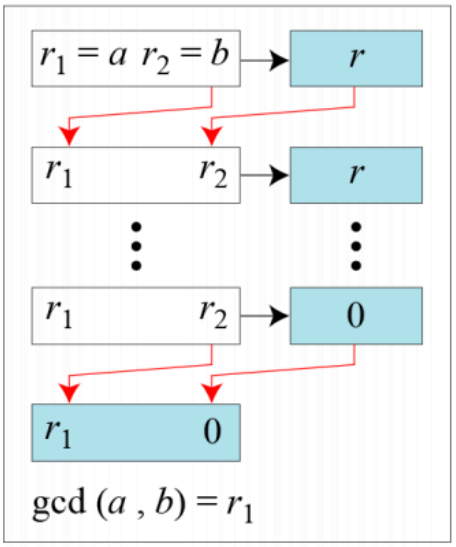
Câu 14: Các phương pháp Ceasar, mã hóa đơn bảng, đa bảng, one-time pad dùng nguyên tắc gì để mã hóa?

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:



a. Process

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

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)

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$

$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$ (Initialization)

$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$

$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2;$ $t_2 \leftarrow t;$ (Updating t's)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

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.

- ✔ $(5^{15} \bmod 13) =$
- ✔ $(15^{18} \bmod 17)$
- ✔ $(7^{51} \bmod 18)$
- ✔ $(15^{59} \bmod 23)$
- **159^{137} mod 31 =16**

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

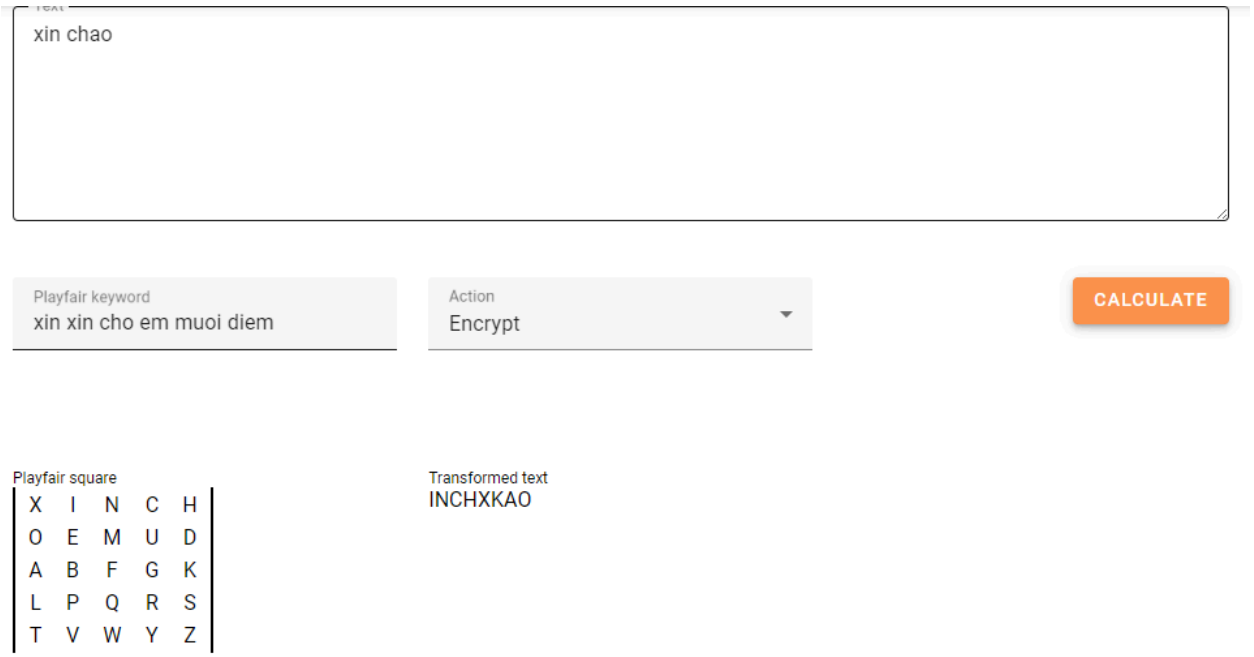
Ví dụ: meet me after the toga party

K=3

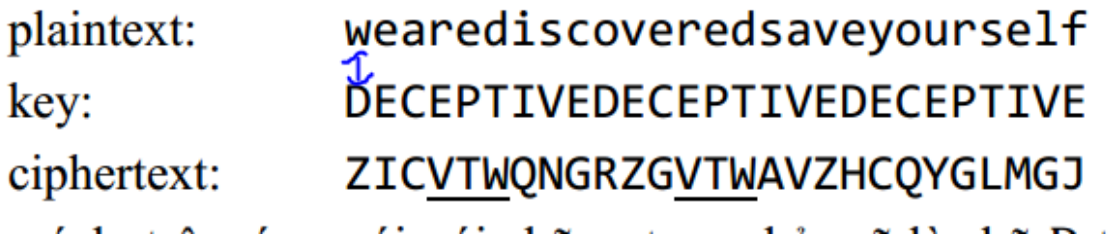
Z26 = A B C D E F G H I J K L M N O P Q S R T U V W X Y Z

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 (bỏ)

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:

✔ (5^{15} mod 13) =

✔ (15^{18} mod 17)

✔ (7^{51} mod 18)

✔ (15^{59} mod 23)

159^{137} mod 31 =16

Câu 5: Alice chọn p=11 & q=3, e = 3 hãy tính khóa K_{RU} và K_{RA}, 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

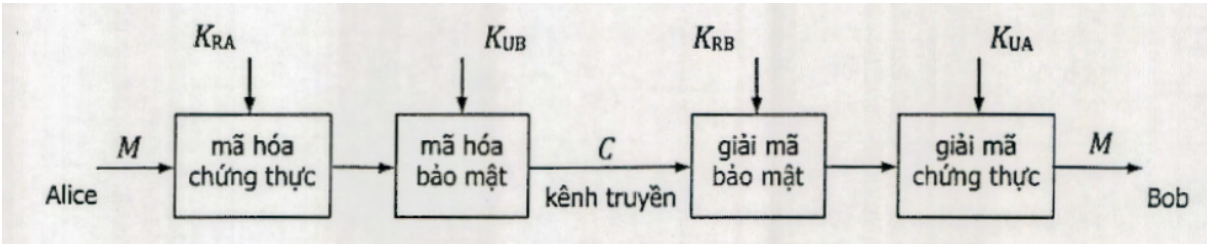
B2: φ(n)=(p-1)*(q-1) = 20

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)) = M^{da} 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)) = C^{d} 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 K_{RU} và K_{RA}, 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.

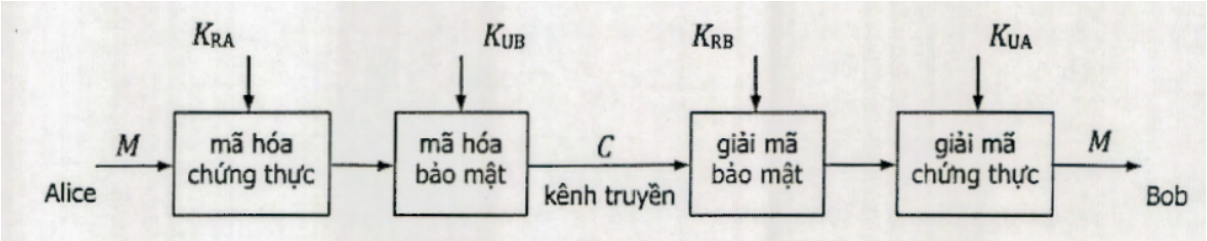
Câu 8: Cho p = 11, q= 13, e = 11. Tính khóa riêng (d, N) trong phương pháp RSA

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:

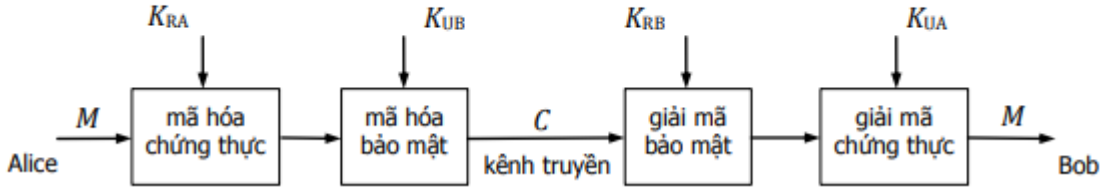
a. Tính khóa riêng KRA của Alice và KRB của Bob

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.



$$C = E(E(M, K_{RA}), K_{UB})$$

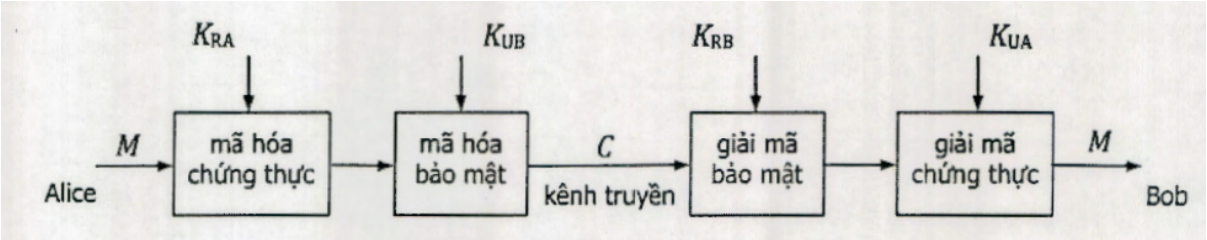
$$M = D(D(C, K_{RB}), K_{UA})$$



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, $X_A = 5$, $X_B = 12$ hãy tính Y_A, Y_B và khóa chung K_{AB}.

Câu 13: cho q = 11, anpha = 2, $X_A = 9$, $X_B = 3$ hãy tính $Y_{A,}$ Y_B và khóa chung $K_{AB.}$

Câu 14: cho q = 17, anpha = 10, $X_A = 7$, $X_B = 5$ hãy tính $Y_{A,}$ Y_B và khóa chung $K_{AB.}$

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:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Hằng số vòng:

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

AA	24	00	09
1E	BE	6D	AC
26	C2	51	4E
62	76	15	89
W_{32}	**W_{33}**	**W_{34}**	**W_{35}**

i (decimal)	temp	After RotWord	After SubWord	Rcon (8)	After XOR with Rcon	w[i 4]	w[i] = temp Xor w[i 4]
36	09AC 4E89	AC4E8 909	912F A701	80000 000	112F A701	AA1E 2662	BB318163

BB	9F	39	30
31	8F	E2	4E
81	43	12	5C
63	15	00	89
W_{36}	**W_{37}**	**W_{38}**	**W_{39}**

THUẬT TOÁN SHA1, 512….