

TRƯỜNG ĐẠI HỌC THĂNG LONG
MÔN THI: BẢO MẬT THÔNG TIN
Thời gian: **90 phút**
Đề 2

Câu 1: Cho hệ mật (X, K, Y) với:

X : Nguồn tin có phân phối:

X	x_1	x_2	x_3
P_X	1/4	1/4	1/2

K : Khóa có phân phối:

K	k_1	k_2	k_3
P_K	1/3	1/3	1/3

$Y = E_K(X)$ cho theo bảng:

	x_1	x_2	x_3
k_1	y_2	y_1	y_3
k_2	y_3	y_1	y_2
k_3	y_2	y_3	y_1

- Tính $H(X)$, $H(Y)$, $H(K)$.
- Tính $H(X|Y)$, $H(Y|X)$ và cho biết giữa X và Y trong kênh trên có độc lập không? Giải thích?.

Câu 2:

- Mã hóa $P = \text{"network security"}$ bằng phương pháp Vigenere với khóa $K = \text{Maxtin}$.
- Tính số khóa có thể của hệ mã trên, biết rằng chu kỳ d của khóa phải thỏa mãn điều kiện $2 \leq d$ và d là ước của độ dài của $P = 15$.

Câu 3: A chọn $p = 11, q = 13, e = 7$. B chọn $p = 17, q = 11, e = 13$

- Tính các khóa bí mật K_{RA} , K_{RB} của A, B tương ứng.
- Hãy giúp A mã hóa tin $P = 2$ theo cả 2 trường hợp mã chứng thực và mã bảo mật.

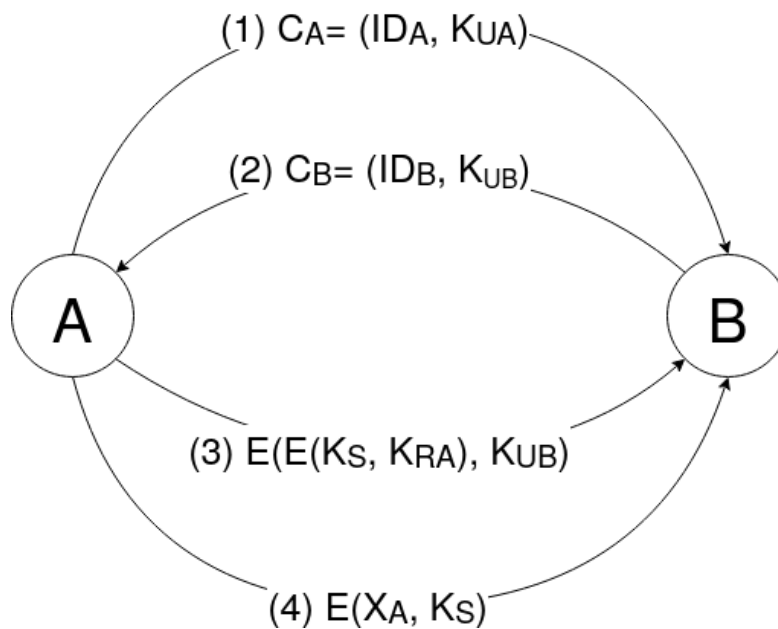
Câu 4: Cho hệ chữ ký RSA: với $p = 13, q = 17, e = 11$.

- a, Xác định chữ ký trên bản tin $P = 3$.
- b, Cho biết khóa công khai K_U và bí mật K_R của hệ trên.

Câu 5: A, B sử dụng phương pháp Diffie-Hellman để trao đổi khóa chung K_{AB} với lựa chọn $p = 11, \alpha = 2$.

- a, Chứng minh rằng α là phần tử nguyên thủy của $Z_p^* = Z_{11}^*$.
- b, Nếu khóa bí mật của A là $K_{RA} = 7$, hãy tìm khóa công khai K_{UA} .
- c, Nếu khóa công khai của B là $K_{UB} = 5$, hãy tìm khóa chung K_{AB} .

Câu 6: Cho giao thức mật mã được mô tả theo sơ đồ:



- a, Hãy cho biết giao thức trên là giao thức gì? Mục đích?
- b, Hãy giải thích các bước liên tiếp của giao thức? Mục đích?
- c, Để có thể xác thực được đối tượng (gửi, nhận) thì có cần bổ sung yêu cầu gì không? Giải thích?
- d, Giải thích vai trò của K_S .