TRƯỜNG ĐẠI HỌC THĂNG LONG

Đề ôn tập môn:
BẢO MẬT THÔNG TIN

Nguyễn Tú Anh
Ngày 10 tháng 3 năm 2020

Đề 1

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	1/2	1/4

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	1	3	2
k_2	3	2	1
k_3	2	3	1

a, Tính $H(X)$, $H(Y)$, $H(K)$.

b, 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:

a, Mã hóa P= "network security" bằng phương pháp Vigenere với khóa K= Shannon

b, Tính số khóa có thể của hệ mã trên, biết rằng chu kỳ d của khóa phải thỏa mãn điều kiện $2 \le d$ và d là ước của độ dài của P= 15.

Câu 3: A chọn $p = 13, q = 11, e = 7$. B chọn $p = 11, q = 17, e = 9$

a, Tính các khóa bí mật K_{RA}, K_{RB} của A, B tương ứng.

b, Hãy giúp A mã hóa tin P= 3 theo cả 2 trường hợp mã chứng thực và mã bảo mật.

Câu 4: Cho hệ chữ ký RSA: với $p = 13, q = 17, e = 7$.

a, Xác định chữ ký trên bản tin P= 2.

b, Cho biết khóa công khai K_U và bí mật K_R của hệ trên.

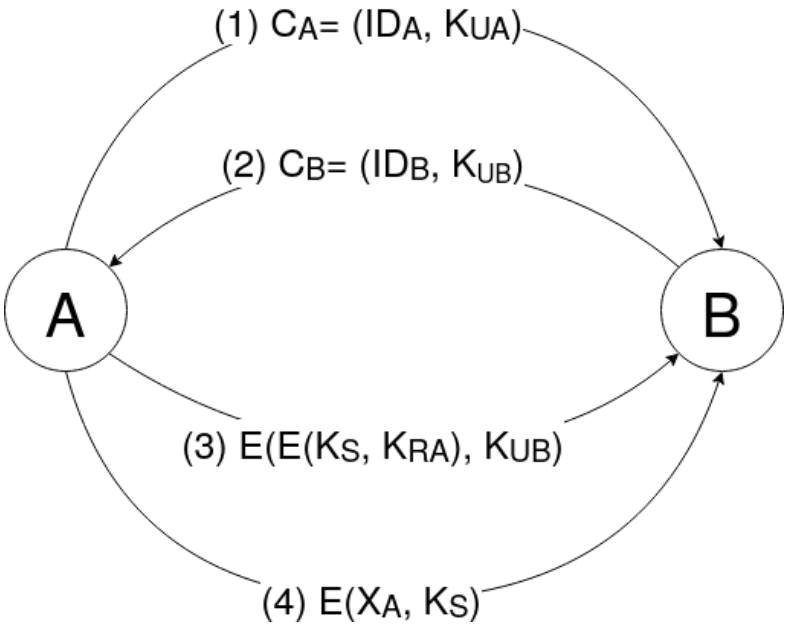
Câu 5: A, B sử dụng phương pháp Diffie-Hellman để trao đổi khóa chung K_{AB} với lựa chọn $p = 11$, $\alpha = 2$.

a, Chứng minh rằng α là phần tử nguyên thủy của $Z_p^* = Z_{11}^*$.

b, Nếu khóa công khai của A là $K_{UA} = 5$, hãy tìm khóa bí mật K_{RA}.

c, Nếu khóa công khai của B là $K_{UB} = 3$, hãy tìm khóa chung K_{AB}.

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



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 địch?

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.

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	2	1	3
k_2	3	1	2
k_3	2	3	1

a, Tính $H(X)$, $H(Y)$, $H(K)$.

b, 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:

a, Mã hóa P= "network security" bằng phương pháp Vigenere với khóa K= Maxtin.

b, Tính số khóa có thể của hệ mã trên, biết rằng chu kỳ d của khóa phải thỏa mãn điều kiện $2 \le d$ và d là ước của độ dài của P= 15.

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

a, Tính các khóa bí mật K_{RA}, K_{RB} của A, B tương ứng.

b, 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.

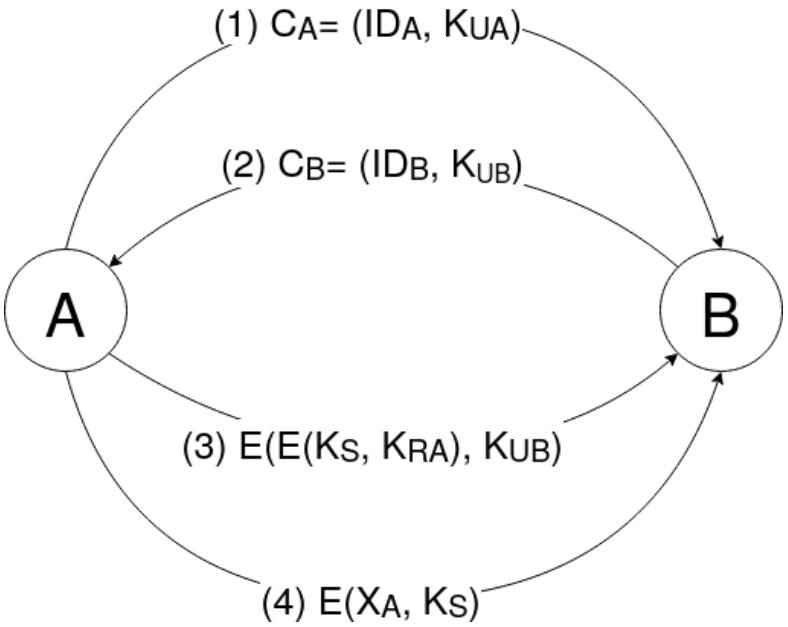
Câu 5: A, B sử dụng phương pháp Diffie-Hellman để trao đổi khóa chung K_{AB} với lựa chọn $p = 13$, $\alpha = 2$.

a, Chứng minh rằng α là phần tử nguyên thủy của $Z_p^* = Z_{11}^*$.

b, Nếu khóa công khai của A là $K_{UA} = 7$, hãy tìm khóa bí mật K_{RA}.

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 biêt giao thức trên là giao thức gì? Mục đích?

b, Hãy giải thích các bước liên tiếp của giao thức? Mục địch?

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.