BG Ch7 Bài 2. Một số sơ đồ thỏa thuận khóa

1. Sơ đồ thỏa thuận khóa Diffie – Helman trong hệ mật ElGamal
   Giả sử hai đối tác A và B đã thống nhất với nhau sử dụng Hệ mật ElGamal với số nguyên tố p và phần tử nguyên thủy α nào đó.
   Khi đó, các bước thỏa thuận khóa thực hiện như sau:

Bước 1. Đối tác A chọn bí mật số ngẫu nhiên a thuộc Z_p^* và tính $\alpha^a \text{mod} p = \beta_A$, rồi gửi nó cho B.

Đối tác B cũng làm tương tự, chọn bí mật số ngẫu nhiên b thuộc Z_p^* và tính $\alpha^b \text{mod} p = \beta_B$, rồi gửi nó cho A.

Bước 2. Hai bên nhận được số β của đối tác, dùng nó để tạo ra khóa chung

$K_{AB} = (\beta_A)^b \text{mod} p$

$= (\beta_B)^a \text{mod} p$

Bước 3. Hai bên A và B sử dụng khóa bí mật chung để liên hệ.

Ví dụ:

Câu 5. Thỏa thuận khóa

Alice và Bob thống nhất dùng giao thức thỏa thuận khóa Diffie – Hellman.

a) Nếu họ dùng hệ mật ElGamal với p = 10007, chọn phần tử nguyên thủy α = 5, Alice chọn khóa a = 2603, Bob chọn b = 1503.

Hãy xác định khóa chung của họ.

Giải

Tính $\beta_A = 5^{2603} \bmod 10007$

$= 245$

Tính $\beta_B = 5^{1503} \bmod 10007$

$= 6028$

Tính $K_{AB} = 8714 = MXE$

b) Chuyển khóa chung của họ sang chữ cái tiếng Anh để làm khóa của hệ mật Vigener. Hãy sử dụng khóa đó để mã hóa bản tin x =

THANGTHANHNIEN và giải mã bản mã nhận được.

THA	NGT	HAN	HNI	ENZ
MXE	MXE	MXE	MXE	MXE

x = HAIDUONGANH HUNG

2. Thỏa thuận khóa Diffie – Hellman trong sơ đồ hệ mật EC – ElGamal

Bước tạo khóa: Hai bên A và B thống nhất với nhau 1 đường cong Elliptic và điểm cơ sở P có cấp là n.

Khi đó, các bước thỏa thuận khóa thực hiện như sau:

Bước 1. Đối tác A chọn bí mật số ngẫu nhiên d_a thỏa mãn $1 \leq d_a \leq n - 1$ và tính $d_a * P = B_A$, rồi gửi nó cho B.

Đối tác B cũng làm tương tự, chọn bí mật số ngẫu nhiên d_b thỏa mãn

$1 \leq d_b \leq n - 1$ và tính $d_b * P = B_B$, rồi gửi nó cho A.

Bước 2. Hai bên nhận được số B của đối tác, dùng nó để tạo ra khóa chung

$K_{AB} = d_a * B_B$

$= d_b * B_A$

Bước 3. Hai bên A và B sử dụng hoành độ của K_{AB} làm khóa bí mật chung để liên hệ.

Bài tập:

Lấy Số bí mật d=Ngày sinh + 6 và thực hiện thuật toán trao đổi khóa Diffie – Hellman trên Hệ mật ElGamal với p= 43.

Ví dụ 2.

Đường cong $E_{43}(13, 15)$ có 43 điểm

Mỗi sv lấy d=Ngày sinh + 5

Chị Đào Minh Hoàn: d=33

Chị Hoàng Ngọc Huyền: d=25

Hai chị thống nhất chọn P=(0, 12) làm điểm cơ sở.

Cấp của P là 43.

$B_{Hoàn} = 33P = (35, 1)$

$B_{Huyền} = 25P = (36, 22)$

Tính khóa chung

$K_{AB} = 25\ B_{Hoàn} = (28, 10)$

$= 33B_{Huyền} = (28, 10)$

$28 = BC$

Bài tập về nhà

Thực hiện thuật toán trao đổi khóa trên hệ mật EC – ElGamal với đường cong Elliptic tương ứng với p là số nguyên tố gồm 5 chữ số và p gồm 20 bit mà các bạn đã xây dựng.

Bài tập nộp trước ngày Thứ 6 16/11/2022.