Chứng chỉ số

Bài 1.

Xét giao thức trao đổi khoá Diffie-Hellman với chứng chỉ số. Ta có hệ thống với ba người dùng Alice, Bob và Charley. Thuật toán Diffie-Hellman sử dụng $p = 61$ và $g = 18$. Ba khoá bí mật tương ứng là $a = 11, b = 22$, và $c = 33$. Ba định danh là $ID(A) = 1,\ ID(B) = 2$ và $ID(C) = 3$.

Để sinh chữ ký, người ta sử dụng hệ chữ ký số ElGamal với tham số $p' = 467, d' = 127$ và phần tử sinh $g' = 2$ và giá trị $\beta = {g'}^{d'}$. CA sử dụng khoá tạm thời $k_E = 213, 215$ và 217 cho Alice, Bob và Charley, tương ứng. (Trên thực tế, tốt hơn là CA nên sử dụng một bộ sinh số giả ngẫu nhiên cho k_E).

Để tính chứng chỉ số, CA tính $x_i = 4 \times b_i + ID(i)$ và dùng giá trị này như input cho thuật toán ký. (Đưa x_i ta có thể tính $ID(i) = x_i \mod 4$.)

1. Hãy tính ba chứng chỉ số $Cert_A, Cert_B$ và $Cert_C$.
2. Kiểm tra ba chứng chỉ trên.
3. Tính khoá phiên k_{AB}, k_{AC} và k_{BC}.