1. Trao đổi khóa Diffie-Hellman Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 6947 và a = 5 (là căn nguyên thủy của q).
2. An chọn khóa riêng xA = 395
3. Ba chọn khóa riêng xB = 338

Hãy cho biết

a) Cách An tính ra khóa công khai yA và khóa phiên K? yA = K =

b) Cách Ba tính ra khóa công khai yB và khóa phiên K? yB = K =

-

q=6947

a=5

-an tao khoa

+Chon khoa rieng(Xa<q) Xa=17

+tinh khoa cong khai Ya=a^Xa mod **q Ya=5^17 mod 6947=1722**

-ba tao khoa

+ chon khoa rieng Xb=19

+tinh khoa cng khai Yb=b^Xb mod q **Yb=5^19 mod 6947=6105**

-an tinh khóa bi mat chung

K=Yb^Xa mod q =6105^17 mod 6947=

-ba tinh khoa bi mat chung

K=Ya^Xb mod q= 1722^19mod 6947=