**THỰC HÀNH MÃ HÓA KHÓA CÔNG KHAI**

**THAM KHẢO BÀI TẬP**

**NHÓM K & (K + 5) LÀM BÀI K, K = 1, 2, 3, 4, 5**

1. **Trao đổi khóa Diffie-Hellman**
   **Input:** số nguyên tố q, a (căn nguyên thủy của q), xA = xB =
   **Ouput:** yA, yB, K

2. **Thuật toán RSA - Bài toán 1**
   Input: p, q, e
   **Output:**
   a) PU = {e, n} =
   b) PR = {d, n} =
   c) An mã: C =
   d) Ba giải mã C: M' =

3. **Thuật toán RSA - Bài toán 2:**
   Input: p, q, e
   **Output:**
   a) PU = {e, n} =
   b) PR = {d, n} =
   c) Ba mã: C =
   d) An giải mã C: M' =

4. **Mật mã ElGamal**
   Input: q là một số nguyên tố, a là căn nguyên thủy của q, xA, k, M
   **Output:**
   **a)** PU = {q, a, $Y_A$}
   a) Ba mã hóa M, bản mã là ($C_1$, $C_2$)
   b) An giải bản mã ($C_1$, $C_2$)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**
   Input: H(M), p , q , h, xA , k
   **Output:**
   a) Khóa công khai yA =
   b) Chữ ký số (r, s) =
   c) Ba xác minh chữ ký số?