NHÓM 1

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7523
   và a = 5 (là căn nguyên thủy của q).
   An chọn khóa riêng xA = 387
   Ba chọn khóa riêng xB = 247
   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 47 , q = 71 , e = 61 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách An tạo bản mã hóa thông điệp M = 59: C =
   d) Hãy cho biết cách người nhận giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 47 , q = 71 , e = 61 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) Cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách người gửi (Ba) mã hóa thông điệp M = 59 để gửi cho An: C =
   d) Cách An giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là
   q = 7433 là một số nguyên tố, a = 3 là căn nguyên thủy của q.
   An chọn khóa riêng là xA = 341
   Hãy cho biết
   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =
   b) Ba chọn số k = 872 để mã hóa bản tin M = 403 gửi cho An. Bản mã là (C_1, C_2) =
   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) = 7
   An và Ba thống nhất các giá trị: p = 47, q = 23, h = 34
   và An chọn xA = 2, k = 10
   Hãy cho biết
   a) Khóa công khai của An: yA =
   b) Chữ ký số của An cho bản tin M: (r, s) =
   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 2

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7879 và a = 3 (là căn nguyên thủy của q).

   An chọn khóa riêng xA = 524

   Ba chọn khóa riêng xB = 214

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 37 , q = 53 , e = 47 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 41: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 37 , q = 53 , e = 47 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 41 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 7919 là một số nguyên tố, a = 7 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 323

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 223 để mã hóa bản tin M = 364 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 31, q = 5, h = 23

   và An chọn xA = 3, k = 6

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 3

MÃ HÓA KHÓA CÔNG KHAI

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).

   An chọn khóa riêng xA = 395

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 43 , q = 47 , e = 67 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 59: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 43 , q = 47 , e = 67 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 59 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 6827 là một số nguyên tố, a = 5 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 307

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 919 để mã hóa bản tin M = 474 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 47, q = 23, h = 25

   và An chọn xA = 2, k = 3

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 4

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7207 và a = 3 (là căn nguyên thủy của q).

   An chọn khóa riêng xA = 422

   Ba chọn khóa riêng xB = 286

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 31 , q = 47 , e = 43 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 53: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 31 , q = 47 , e = 43 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 53 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 7349 là một số nguyên tố, a = 3 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 366

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 32 để mã hóa bản tin M = 333 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 59, q = 29, h = 10

   và An chọn xA = 2, k = 3

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 5

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7687
   và a = 6 (là căn nguyên thủy của q).
   An chọn khóa riêng xA = 437
   Ba chọn khóa riêng xB = 354
   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 17 , q = 23 , e = 19 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách An tạo bản mã hóa thông điệp M = 31: C =
   d) Hãy cho biết cách người nhận giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 17 , q = 23 , e = 19 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) Cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách người gửi (Ba) mã hóa thông điệp M = 31 để gửi cho An: C =
   d) Cách An giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là
   q = 6469 là một số nguyên tố, a = 18 là căn nguyên thủy của q.
   An chọn khóa riêng là xA = 409
   Hãy cho biết
   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =
   b) Ba chọn số k = 695 để mã hóa bản tin M = 491 gửi cho An. Bản mã là (C_1, C_2) =
   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =
   An và Ba thống nhất các giá trị: p = 67, q = 11, h = 9
   và An chọn xA = 2, k = 3
   Hãy cho biết
   a) Khóa công khai của An: yA =
   b) Chữ ký số của An cho bản tin M: (r, s) =
   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 6

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7669 và a = 6 (là căn nguyên thủy của q).

   An chọn khóa riêng xA = 338

   Ba chọn khóa riêng xB = 336

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 19 , q = 23 , e = 31 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 41: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 19 , q = 23 , e = 31 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 41 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 7243 là một số nguyên tố, a = 3 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 346

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 42 để mã hóa bản tin M = 428 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 47, q = 23, h = 9

   và An chọn xA = 5, k = 20

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 7

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 6781
   và a = 7 (là căn nguyên thủy của q).
   An chọn khóa riêng xA = 380
   Ba chọn khóa riêng xB = 478
   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 47 , q = 53 , e = 71 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách An tạo bản mã hóa thông điệp M = 67: C =
   d) Hãy cho biết cách người nhận giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 47 , q = 53 , e = 71 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) Cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách người gửi (Ba) mã hóa thông điệp M = 67 để gửi cho An: C =
   d) Cách An giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là
   q = 7057 là một số nguyên tố, a = 5 là căn nguyên thủy của q.
   An chọn khóa riêng là xA = 463
   Hãy cho biết
   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =
   b) Ba chọn số k = 973 để mã hóa bản tin M = 402 gửi cho An. Bản mã là (C_1, C_2) =
   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =
   An và Ba thống nhất các giá trị: p = 83, q = 41, h = 32
   và An chọn xA = 2, k = 2
   Hãy cho biết
   a) Khóa công khai của An: yA =
   b) Chữ ký số của An cho bản tin M: (r, s) =
   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 8

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 7159 và a = 3 (là căn nguyên thủy của q).

   An chọn khóa riêng xA = 371

   Ba chọn khóa riêng xB = 476

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 37 , q = 59 , e = 53 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 47: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 37 , q = 59 , e = 53 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 47 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 6571 là một số nguyên tố, a = 3 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 436

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 979 để mã hóa bản tin M = 459 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 59, q = 29, h = 3

   và An chọn xA = 19, k = 25

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 9

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 6199
   và a = 3 (là căn nguyên thủy của q).
   An chọn khóa riêng xA = 531
   Ba chọn khóa riêng xB = 540
   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 43 , q = 47 , e = 53 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách An tạo bản mã hóa thông điệp M = 67: C =
   d) Hãy cho biết cách người nhận giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 43 , q = 47 , e = 53 để tạo cặp khóa.
   Hãy cho biết
   a) Khóa công khai của An: PU = {e, n} =
   b) Cách An tạo ra khóa riêng: PR = {d, n} =
   c) Cách người gửi (Ba) mã hóa thông điệp M = 67 để gửi cho An: C =
   d) Cách An giải mã bản mã C:
   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là
   q = 7001 là một số nguyên tố, a = 6 là căn nguyên thủy của q.
   An chọn khóa riêng là xA = 382
   Hãy cho biết
   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =
   b) Ba chọn số k = 589 để mã hóa bản tin M = 442 gửi cho An. Bản mã là (C_1, C_2) =
   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =
   An và Ba thống nhất các giá trị: p = 89, q = 11, h = 38
   và An chọn xA = 5, k = 2
   Hãy cho biết
   a) Khóa công khai của An: yA =
   b) Chữ ký số của An cho bản tin M: (r, s) =
   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

NHÓM 10

MÃ HÓA KHÓA CÔNG KHAI

1. **Trao đổi khóa Diffie-Hellman**

   Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn số nguyên tố q = 6389 và a = 7 (là căn nguyên thủy của q).

   An chọn khóa riêng xA = 442

   Ba chọn khóa riêng xB = 342

   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 =

2. **Thuật toán RSA - Bài toán 1**

   Giả sử An chọn các giá trị p = 29 , q = 47 , e = 41 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách An tạo bản mã hóa thông điệp M = 43: C =

   d) Hãy cho biết cách người nhận giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

3. **Thuật toán RSA - Bài toán 2:**

   Giả sử An chọn các giá trị p = 29 , q = 47 , e = 41 để tạo cặp khóa.

   Hãy cho biết

   a) Khóa công khai của An: PU = {e, n} =

   b) Cách An tạo ra khóa riêng: PR = {d, n} =

   c) Cách người gửi (Ba) mã hóa thông điệp M = 43 để gửi cho An: C =

   d) Cách An giải mã bản mã C:

   e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

4. **Mật mã ElGamal**

   Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là q = 7283 là một số nguyên tố, a = 5 là căn nguyên thủy của q.

   An chọn khóa riêng là xA = 429

   Hãy cho biết

   a) Khóa công khai của An: PU = {q, a, Y_A} với yA =

   b) Ba chọn số k = 11 để mã hóa bản tin M = 372 gửi cho An. Bản mã là (C_1, C_2) =

   c) Cách An giải bản mã (C_1, C_2)?

5. **CHỮ KÝ ĐIỆN TỬ DSA**

   Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) =

   An và Ba thống nhất các giá trị: p = 67, q = 11, h = 43

   và An chọn xA = 6, k = 12

   Hãy cho biết

   a) Khóa công khai của An: yA =

   b) Chữ ký số của An cho bản tin M: (r, s) =

   c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?