Soal UTS EL5111

Waktu 150 menit

1. Pilih salah 1 dari soal berikut : (Jika anda mengerjakan dua soal, maka hanya jawaban pertama yang akan diperiksa)

   a) Sistem RSA menggunakan p=149, q= 107, e=3, c= 3646
   Soal : Hitung d , kemudian gunakan CRT untuk menghitung dP, dQ, qInv, m1, m2, h dan m !
   (Nilai maks 30)

d =	m1 =
dP =	m2 =
dQ =	h =
qInv=	m =

   b) Hitunglah pesan m dari system yang menggunakan RSA menggunakan CCA , jika diketahui p=47, q=37, e= 5, c= 1299 ! (Nilai maks 20)

   Jawaban :

   d = X= Y = M=

2. Diketahui kurva ECC E23(1,1) . Manakah yang lebih aman digunakan sebagai titik awal G, titik (13,7) atau (5,4) ? Berikan buktinya ! (Nilai maks 30)

3. Pilih salah 1 soal dari 2 soal berikut. Jika anda mengerjakan kedua soal, hanya jawaban pertama yang akan diperiksa.
   a) Attacker menyadap percakapan dua orang dan berhasil mendapatkan kunci public A =33, kunci public B= 8. Keduanya menggunakan algoritma enkripsi Diffie Helman q=37 serta α=2 , yang bentuk umumnya adalah $Y_A = \alpha^{Xa} \bmod q$ di mana x_a adalah kunci privat. Hitunglah shared key yang digunakan! (Nilai maks 30)
   b) Pertukaran kunci antara A dan B diattack oleh attacker C menggunakan *Man in the middle*. Ke A, C mengaku sebagai si B ; dan ke B, C mengaku sebagai si A. A dan B menggunakan DH. Berikan contoh angka-angka hingga muncul Shared key antara A dan C (K_{AC}) serta antara B dan C (K_{BC}) !
   Ketentuan : gunakan α = 2 dan q = 19
   Gambarkan juga diagram attacknya ! (Nilai maks 30)

4. Apa yang dimaksud dengan timing attack ? Berikan contoh singkat dengan menceritakan operasi algoritma tertentu yang dapat di-attack menggunakan attack ini ! (nilai maks 10)

5. Jelaskan secara singkat cara membangkitkan bilangan prima untuk RSA ! (nilai maks 10)