Soal UAS EL 5111 Kriptografi dan Aplikasinya

Waktu 150 menit

Bagian 1 (bobot per soal 30%)

1. Pilih salah satu dari soal berikut (hanya jawaban pertama yang akan diperiksa jika anda mengerjakan 2 soal)
   a. Kartu ID menggunakan ECDSA untuk tanda tangan digital, dengan kurva $E_{23}(1,1)$. Titik awal yang digunakan adalah G(3,10) dengan e= H(m) = 16 , kunci privat d = 17, bilangan acak k = 23. Diketahui kunci public Q=dG. Berapa nilai n (orde kurva), r dan s ? Dapatkah tandatangan diverifikasi sebagai valid ?

      Proses tandatangan digital

      n = … r = …….. s =…….

      Verifikasi tandatangan

      w = …. u_1.G = …… u_2.Q=…….

      X = u_1G + u_2Q = …

      Tandatangan : (valid/tidak) → Coret yang salah

   b. Kartu ID menggunakan ECDSA untuk tanda tangan digital, dengan kurva $E_{23}(1,1)$. Titik awal yang digunakan adalah G(1,16) dengan e= H(m) = 14 , kunci privat d = 25, bilangan acak k = 19. Diketahui kunci public Q=dG. Berapa nilai n (orde kurva), r dan s ? Dapatkah tandatangan diverifikasi sebagai valid ?

      Proses tandatangan digital

      n = … r = …….. s =…….

      Verifikasi tandatangan

      w = …. u1.G = …… u2.Q=…….

      X = u_1G + u_2Q = …

      Tandatangan : (valid/tidak) → Coret yang salah

2. Sebuah dokumen m ditandatangani dengan fungsi hash dan RSA, dimana digital signature $s = h^d \bmod n$ dimana d adalah kunci privat RSA sedangkan n adalah modulus RSA. Fungsi hash berada di dalam secure hardware yang jika dibuka, isinya akan lenyap. Attacker dapat menggunakan fungsi hash tsb tanpa perlu mengetahui algoritmanya. Output dari fungsi hash adalah h. Parameter RSA yang diketahui oleh attacker adalah m= 6, e=7, n=30301. Bagaimana cara attacker memalsukan dokumen tsb ? Jelaskan disertai perhitungan yang lengkap !

Bagian kedua (bobot per soal 12,5%)

Pilih 4 dari 6 soal berikut ! Hanya 4 jawaban pertama yang akan diperiksa jika anda mengerjakan lebih dari 4 soal !

1. Tuliskan persamaan ECDH, dan buktikan bagaimana pertukaran kunci bisa dilakukan dengan ECDH !
2. Gambarkan struktur HMAC beserta penjelasan singkat!
3. Gambarkan struktur DAC (Data Authentication Code) Algorithm beserta penjelasan singkat!
4. Gambarkan CMAC beserta penjelasan singkat!
5. Gambarkan blok diagram otentikasi CCM beserta penjelasan singkat!
6. Apa perbedaan antara *Collision resistant* dan *Second preimage resistant* ? Mana yang membutuhkan lebih sedikit data ? Mengapa bisa demikian ?