UAS II4031 Kriptografi dan Koding - Sem 2 - 2022/2023

Ujian Akhir Semester
Hari/Tanggal: Rabu 10 Mei 2023
Waktu: 90 menit
Sifat ujian: TUTUP BUKU

* Indicates required question

1. Email *

Identitas dan Pernyataan

Tuiskan NIM, Nama, dan pernyataan

2. Nama *

3. NIM *

4. Email *

5. Tulis ulang pernyataan berikut:
   "Saya menyatakan bahwa saya mengerjakan UAS ini dengan sejujur-jujurnya, tanpa bantuan orang lain dan tanpa menggunakan cara yang tidak dibenarkan. Apabila di kemudian hari diketahui saya mengerjakan UAS ini dengan cara yang tidak jujur, saya bersedia mendapatkan konsekuensinya, yaitu mendapatkan nilai E pada mata kuliah II4031 Semester 2 Tahun 2022/2023.

A. SOAL PILIHAN GANDA

Pilihlah satu jawaban YANG
PALING BENAR. Soal UAS pilihan berganda terdiri dari total 20
pertanyaan. Setiap soal bernilai 3. Anda boleh menggunakan kalkultor,
tetapi hanya
kakulator scientific di OS. Tidak diperkenankan menggunakan program
online yang ada di Intenet. Setiap peserta ujian hanya boleh melakukan
submission/response sebanyak 1x saja menggunakan akun @std.stei.itb.ac.id

6. Bob mengirim pesan kepada Alice, pesan tersebut akan ditandatangani dulu oleh Bob dengan menggunakan sebuah algoritma kriptografi kunci-publik. Untuk menandatangani pesan tersebut, Bob mengenkripsinya dengan menggunakan:

   Mark only one oval.

   - Kunci publik Alice
   - Kunci privat Alice
   - Kunci publik Bob
   - Kunci privat Bob
   - Kunci rahasia yang disepakati oleh Alice dan Bob

7. (lanjutan soal sebelumnya) Alice memverifikasi tandatangan digital dari Bob dengan menggunakan:

   Mark only one oval.

   - Kunci privat Bob
   - Kunci publik Bob
   - Kunci privat Alice
   - Kunci publik Alice
   - Kunci rahasia yang disepakati oleh Alice dan Bob

8. Di dalam GF(11), operasi 5 x 10 menghasilkan nilai:

   Mark only one oval.

   - 50
   - 61
   - 6
   - 5
   - 10
   - Tidak ada jawaban yang benar

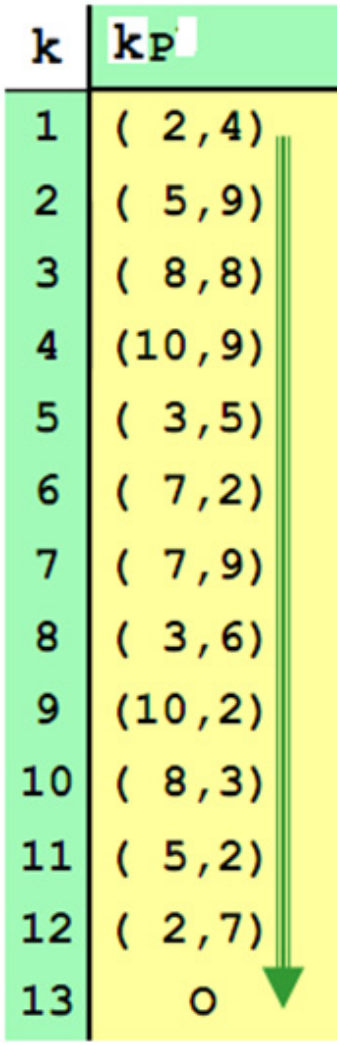
9. Elliptic Curve Discrete Logarithm Problem (ECDLP) berbunyi:

Mark only one oval.

- ( ) Diberikan P dan Q adalah dua buah titik di kurva eliptik , carilah integer k sedemikian sehingga Q = kP
- ( ) Diberikan Q sebuah titik di kurva eliptik dan integer k, carilah P sedemikian sehingga Q = kP
- ( ) Diberikan P sebuah titik di kurva eliptik dan integer k, carilah Q sedemikian sehingga Q = kP
- ( ) Diberikan P dan Q dua buah titik di kurva eliptik, carilah k sedemikian sehingga k = PQ
- ( ) Tidak ada jawaban yang benar

10. Diketahui P = (2, 4) adalah titik pada kurva eliptik. Diberikan tabel hasil perhitungan perkalian titik kP dengan berbagai nilai k seperti pada gambar berikut.

Alice dan Bob akan melakukan perhitungan secret key dengan ECDH (Eliptic Curve Diffie-Hellman). Alice dan Bob menyepakati titik P sebagai basis. Misalkan Alice memilih kunci privat a = 4 dan Bob memilih kunci privat b = 7. Maka, kunci publik Alice dan kunci publik Bob masing-masing adalah:



k	kP
1	(2,4)
2	(5,9)
3	(8,8)
4	(10,9)
5	(3,5)
6	(7,2)
7	(7,9)
8	(3,6)
9	(10,2)
10	(8,3)
11	(5,2)
12	(2,7)
13	O

Mark only one oval.

- (5, 9) dan (7, 2)
- (10, 2) dan (2, 7)
- (10, 9) dan (7, 9)
- (2, 4) dan (3, 6)
- (8, 8) dan (7, 9)
- Tidak ada jawaban yang benar

11. Pernyataan yang benar tentang fungsi hash SHA-1:

Mark only one oval.

- ukuran blok = 512 bit, jumlah putaran = 4, message digest = 128 bit
- ukuran blok = 512 bit, jumlah putaran = 80, message digest = 160 bit
- ukuran blok = 256 bit, jumlah putaran = 80, message digest = 160 bit
- ukuran blok = 512 bit, jumlah putaran = 4, message digest = 256 bit
- ukuran blok = 512 bit, jumlah putaran = 60, message digest = 512 bit
- Tidak ada jawaban yang benar

12. Algoritma Keccak menghasilkan message digest berukuran:

Mark only one oval.

- 128 bit
- 160 bit
- 256 bit
- 512 bit
- 1024 bit
- sembarang ukuran

13. Sertifikat digital diterbitkan oleh CA. Sertifikat digital berisi informasi kunci publik dan identitas pemilik kunci. Sertifikat digital ditandatangani dengan menggunakan:

Mark only one oval.

- Kunci privat pemilik kunci publik.
- Kunci publik pemilik kunci publik
- Kunci privat CA
- Kunci publik CA
- Kunci publik pengguna sertifikat digital
- Tidak ada jawaban yang benar

14. Perubahan http menjadi https pada tampilan laman web di browser terjadi setelah menjalankan SSL pada subprotokol:

Mark only one oval.

- SSL handshaking
- SSL record
- SSL handshaking dan SSL record
- setelah SSL selesai dijalankan seluruhnya
- tidak ada jawaban yang benar

15. Proses yang dilakukan di dalam sub-protokol handshaking di dalam protokol SSL adalah, KECUALI

Mark only one oval.

- Menegosiasikan cipher yang digunakan
- Bertukar kunci sesi (key exchange)
- Meminta sertifikat digital
- Say "hello"
- Melakukan enkripsi pesan
- Tidak ada jawaban yang benar

16. Untuk sembarang output y , sukar menemukan input a sedemikian sehingga H(a) = y. Pernyataan ini adalah sifat fungsi hash H yang dinamakan:

Mark only one oval.

- collision resistance
- preimage resistance
- second preimage resistance
- collision detection
- second collision resistance
- tidak ada jawaban yang benar

17. MAC (Message Authentication Code) dapat dibangkitkan dengan menggunakan fungsi hash yang sudah ada (dinamakan HMAC). Pesan M digabung dengan kunci K lalu dihitung nilai hash gabungan tersebut dengan fungsi hash. Jika ukuran M = 100 bit dan K = 64 bit, lalu di-hash dengan SHA-1, maka MAC akan berukuran:

Mark only one oval.

- 164 bit
- 128 bit
- 160 bit
- 190 bit
- 256 bit
- Tidak ada jawaban yang benar

18. Mekanisme "challenge and response" untuk mengotentikasi server adalah dengan menggunakan kriptografi kunci publik. Client mengirim challenge berupa bit acak sepanjang 100 bit, lalu meminta server mengenkripsinya, dan mengirimkan hasil enkripsi (response) kembali kepada client. Jika hasil dekripsi response oleh client sama dengan bit acak (challenge) yang dikirim, maka client menyimpulkan bahwa server valid.

Pernyataan manakah yang benar?

Mark only one oval.

- Server mengenkirpsi challenge dengan kunci publik server, client mendekripsi response dengan kunci privat client
- Server mengenkirpsi challenge dengan kunci publik client, client mendekripsi response dengan kunci privat client
- Server mengenkirpsi challenge dengan kunci privat server, client mendekripsi response dengan kunci publik client
- Server mengenkirpsi challenge dengan kunci privat server, client mendekripsi response dengan kunci publik server
- Tidak ada jawaban yang benar

19. Mengapa algoritma kriptografi kunci simetri tidak dapat digunakan untuk tanda-tangan digital?

Mark only one oval.

- A) Tidak dapat mengotentikasi pengirim dan penerima pesan
- B) Tidak dapat mengatasi serangan phising
- C) Tidak dapat melakukan mekanisme anti penyangkalan (non-repudiation)
- A, B, dan C benar
- A dan C benar

20. Komponen-komponen di dalam PKI adalah, KECUALI

Mark only one oval.

- Sertifikat digital
- Repositori
- Certification Authority (CA)
- Kebijakan (policy)
- Registration Authority (RA)
- Kunci publik

21. Karakteristik blockchain adalah, KECUALI

Mark only one oval.

- desentralisasi
- transparan
- tidak membutuhkan pihak ketiga
- immutable
- tidak ada jawaban yang memenuhi

22. Setiap blok di dalam blockchain memiliki pointer berupa nilai hash dari:

Mark only one oval.

- blok berikutnya
- blok sebelumnya
- blok yang bersangkutan
- semua blok yang ada
- tidak ada jawaban yang benar

23. Di dalam blockchain terdapat node yang memiliki otoritas untuk menyetujui apakah seseorang dapat bergabung ke dalam blockchain, mengontrol akses ke jaringan blockchain , dan mengatur akses baca dan tulis ke ledger. Blockchain seperti ini tergolong ke dalam:

Mark only one oval.

- A) Public blockchain
- B) Permissionless blockchain
- C) Private blockchain
- D) Permissioned blockchain
- E) Hybrid blockchain
- A dan B benar
- C dan D benar

24. MAC (Message Authentication Code) dapat dihasilkan dengan menggunakan block cipher yang dioperasikan dengan suatu mode operasi tertentu. Pesan dibagi menjadi n buah blok, setiap blok ukurannya sama.. Misalkan block cipher yang digunakan adalah salah satu dari DES dan AES. Pernyataan mana yang benar?

Mark only one oval.

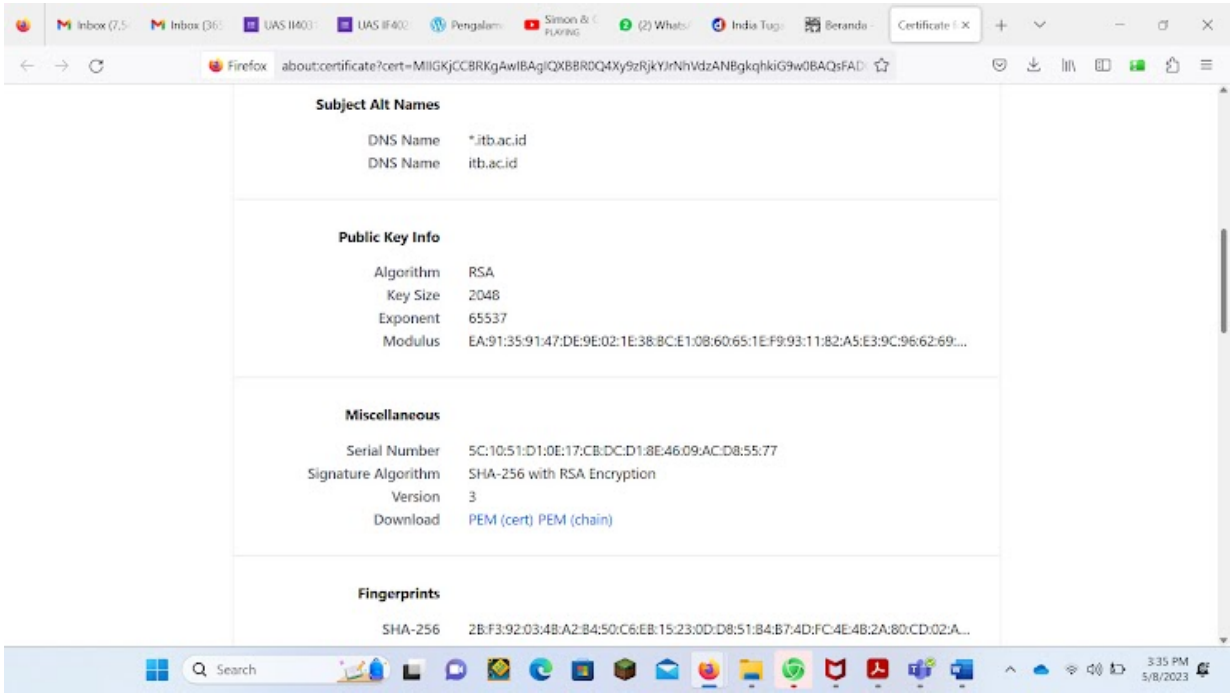
- DES, mode ECB, panjang MAC = 64 bit
- DES, mode CBC, panjang MAC = 128 bit
- AES, mode ECB, panjang MAC = 128 bit
- AES, mode CBC, panjang MAC = 128 bit
- Tidak ada jawaban yang benar

25. (Lanjutan dari soal sebelumnya) Nilai MAC diambil dari hasil enkripsi blok pesan yang ke berapa?

Mark only one oval.

- Blok pertama
- Blok kedua
- Blok terakhir
- Dua blok terakhir
- Gabungan semua blok

26. Tangkapan layar sertifikat digital website ITB (www.itb.ac.id). Dari ganbar tangkapan layar tersebut dapat diperoleh informasi sebagai berikut, KECUALI:



Mark only one oval.

- Algoritma pembangkitan tanda-tangan digital adalah RSA, fungsi hash yang digunakan SHA-256
- Algoritma kriptografi kunci publik yang digunakan adalah RSA, kunci publik e = 65537
- Tanda-tangan digital adalah 63:69:3B:DB:DD:BD:2D:F0:3B:4D:B3:1F:F6:26:94:4A:25:53:5E:5E
- Ukuran n (modulus) adalah 2048 bit
- Nomor seri sertifikat adalah 5C:10:51:D1:0E:17:CB:DC:D1:8E:46:09:AC:D8:55:77

27. Dengan menggunakan protokol SSL maka transmisi data antara client dan server menjadi aman, karena:

Mark only one oval.

- Data yang dikirim selalu dienkripsi dengan algoritma kriptografi kunci-publik
- Jika data diubah selama transmisi maka dapat dideteksi perubahannya
- Data yang dikirim selalu dikompresi terlebih dahulu
- Data yang dikirim selalu diberi tanda tangan digital
- Tidak ada jawaban yang benar

28. Perediksi nilai akhir anda untuk kuliah II4031 Kriptografidan Koding ini adalah:

Mark only one oval.

- A
- AB
- B
- BC
- C
- D
- E

B. SOAL ESSAY

Jawablah soal ini pada kertas lembar jawaban

29. 1. (NILAI = 10 + 10)
(a) Gambarkan dalam satu gambar diagram proses pembangkitan MAC secara umum di sisi pengirim dan proses verifikasi MAC di sisi penerima pesan untuk memeriksa integritas pesan. Penerima dan pengirim pesan menggunakan kunci K yang sama

(b) HMAC adalah salah satu cara pembangkitan MAC dengan menggunakan fungsi hash. Gambarkan dalam satu gambar diagram proses pembangkitan MAC di sisi pengirim dengan menggunakan fungsi hash H dan kunci rahasia K, dan di sisi penerima pesan untuk memeriksa integritas pesan menggunakan kunci K yang sama

30. 2. (NILAI = 10)
Misalkan sebuah kurva eliptik memiliki persamaan y^2 = x^3 + x + 6 (mod 11) dengan x dan y didefinisikan di dalam GF(11). Untuk x = 5, tentukan titik yang terdapat pada kurva eliptik tersebut

31. 3. (NILAI = 10)
Misalkan Alice membantah telah mengirim pesan kepada Bob. Jelaskan bagaimana cara Bob menggunakan tanda-tangan digital unuk melakukan anti penyangkalan (non-repudiation).