UAS II4031 Kriptografi dan Koding

Ujian akhir II4031 Kriptografi dan Koding, Semester II tahun akademik 2021/2022.
Diperbolehkan menggunakan kalkulator. Waktu pelaksanaan ujian: 90 menit

* Required

1. NIM *

2. Nama *

3. 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 2021/2022. " *

Soal Pilihan Ganda

Pilihlah hanya satu jawaban yang benar. Soal pilihan ganda ini ada sebanyak 20 soal

4. Pernyataan yang benar tentang tanda-tangan digital 4 points

Mark only one oval.

- ( ) Pesan ditandatangani dengan kunci publik pengirim pesan, tanda tangan diverifikasi dengan kunci privat penerima pesan
- ( ) Pesan ditandatangani dengan kunci publik penerima pesan, tanda tangan diverifikasi dengan kunci privat penerima pesan
- ( ) Pesan ditandatangani dengan kunci privat pengirim pesan, tanda tangan diverifikasi dengan kunci publik penerima pesan
- (✓) Pesan ditandatangani dengan kunci privat pengirim pesan, tanda tangan diverifikasi dengan kunci publik pengirim pesan
- ( ) Pesan ditandatangani dengan kunci privat penerima pesan, tanda tangan diverifikasi dengan kunci publik penerima pesan
- ( ) Tidak ada jawaban yang benar

5. Message Authentication Code (MAC) tidak dapat berlaku sebagai tanda-tangan digital karena 4 points

Mark only one oval.

- ( ) Tidak dapat digunakan untuk otentikasi pengirim pesan
- ( ) Tidak dapat digunakan untuk memeriksa integritas pesan
- ( ) Tidak dapat digunakan untuk otentikasi penerima pesan
- (✓) Tidak dapat digunakan untuk menyangkal telah menerima pesan
- ( ) Tidak dapat digunakan untuk enkripsi pesan

6. Jika algoritma MAC berbasis block cipher dan cipher yang digunakan adalah AES, maka panjang MAC adalah 4 points

Mark only one oval.

- [ ] 64 bit
- [ ] 100 bit
- [x] 128 bit
- [ ] 160 bit
- [ ] 196 bit
- [ ] Tidak ada jawaban yang benar

7. Pernyataan yang SALAH tentang sertifikat digital 4 points

Mark only one oval.

- [x] Ditandatangani dengan menggunakan kunci publik CA
- [ ] Berisi kunci publik dan identitas pemilik kunci
- [ ] Tersedia secara publik
- [ ] Memiliki masa kadaluarsa
- [ ] Menggunakan kombinasi fungsi hash dan algoritma kriptografi kunci-publik

8. Misalkan H adalah fungsi hash. Untuk input a dan output y = H(a), sukar menemukan input kedua b sedemikian sehingga H(b) = y. Pernyataan tersebut adalah salah satu sifat fungsi hash yang dinamakan: 4 points

Mark only one oval.

- [ ] collision resistance
- [ ] preimage resistance
- [x] second preimage resistance
- [ ] prime preimage resistance
- [ ] Tidak ada jawaban yang benar

9. Pernyataan yang SALAH tentang fungsi hash MD5 4 points

Mark only one oval.

- [ ] Panjang message digest = 128 bit
- [ ] Membagi pesan menjadi blok-blok berukuran 512 bit
- [x] Memiliki 16 putaran
- [ ] Nilai hash pesan adalah hasil blok terakhir
- [ ] Memiliki 4 buah buffer, A, B, C, dan D yang masing-masing panjangnya 32 bit

10. Mekanisme "challenge and response" untuk mengotentikasi server adalah sebagai berikut 4 points

Mark only one oval.

- [ ] Client mengirim string acak kepada server, server mengenkripsi string tersebut dengan kunci publik client lalu mengirimkan hasilnya ke client, client mendekripsi dengan kunci privatnya
- [ ] Client mengirim string acak kepada server, server mengenkripsi string tersebut dengan kunci publiknya lalu mengirimkan hasilnya ke client, client mendekripsi dengan kunci privatnya
- [x] Client mengirim string acak kepada server, server mengenkripsi string tersebut dengan kunci privatnya lalu mengirimkan hasilnya ke client, client mendekripsi dengan kunci publik server
- [ ] Client mengirim string acak kepada server, server mengenkripsi string tersebut dengan kunci publiknya lalu mengirimkan hasilnya ke client, client mendekripsi dengan kunci publik server
- [ ] Client mengirim string acak kepada server, server mengenkripsi string tersebut dengan kunci privatnya lalu mengirimkan hasilnya ke client, client mendekripsi dengan kunci privatnya
- [ ] Tidak ada jawaban yang benar

11. Perbedaan MD5 dengan SHA-1 4 points

Mark only one oval.

- ( ) A) Panjang nilai hash MD5 = 128 bit, panjang nilai hash SHA-1 = 180 bit
- ( ) B) MD5 memiliki 4 buah variabel buffer (ABCD), SHA-1 memiliki 5 buah variabel buffer (ABCDE)
- ( ) C) MD5 terdiri dari 4 putaran, SHA-1 terdiri dari 80 putaran
- ( ) D) MD5 memproses blok-blok pesan 512 bit, SHA-1 memproses blok-blok pesan 1024 bit
- ( ) E) Jawaban A, B, C benar
- (✓) F)Jawaban B dan C benar
- ( ) G) Jawaban A dan B benar

12. Secure Socket Layer (SSL) bertindak sebagai lapisan security (security layer) antara lapisan: 4 points

Mark only one oval.

- ( ) Transport layer (TCP) dan Network Layer (IP)
- (✓) Transport layer dan Application layer
- ( ) Application layer dan Network layer
- ( ) Data link layer dan Network layer
- ( ) Application layer dan Data link layer
- ( ) Tidak ada jawaban yang benar

13. Proses yang dilakukan di dalam sub-protokol handshaking di dalam protokol SSL adalah, KECUALI 4 points

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

14. Fungsi permutasi f di dalam algoritma Keccak bertujuan untuk: 4 points

Mark only one oval.

- ( ) Mengacak bit-bit di dalam blok-blok pesan Pi
- ( ) Mengacak r bit di dalam state S
- (✓) Mengacak semua bit di dalam state S
- ( ) Mengacak c bit di dalam state S
- ( ) Melakukan operasi XOR antara state S dengan blok pesan Pi
- ( ) Tidak ada jawaban yang benar

15. Komponen-komponen di dalam PKI adalah, KECUALI 4 points

Mark only one oval.

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

16. Algoritma pertukaran kunci Diffie-Hellman adalah salah satu algoritma kriptografi kunci publik. Algoritma ini digunakan untuk: 4 points

Mark only one oval.

- ( ) Mengenkripsi pesan antara pengirim dan penerima
- ( ) Menghitung kunci privat masing-masing pengirim dan penerima pesan
- ( ) Menandatangani pesan dari pengirim ke penerima
- (✓) Menghitung kunci simetri yang sama antara pengirim dan penerima pesan
- ( ) Mempertukarkan kunci publik masing-masing pengirim dan penerima pesan.
- ( ) Tidak ada jawaban yang benar

17. 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, titik yang terdapat pada kurva eliptik adalah 4 points

Mark only one oval.

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

18. Kelebihan ECC dibandingkan dengan algoritma kriptografi kunci publik lain seperti RSA, ElGamal, dll 4 points

Mark only one oval.

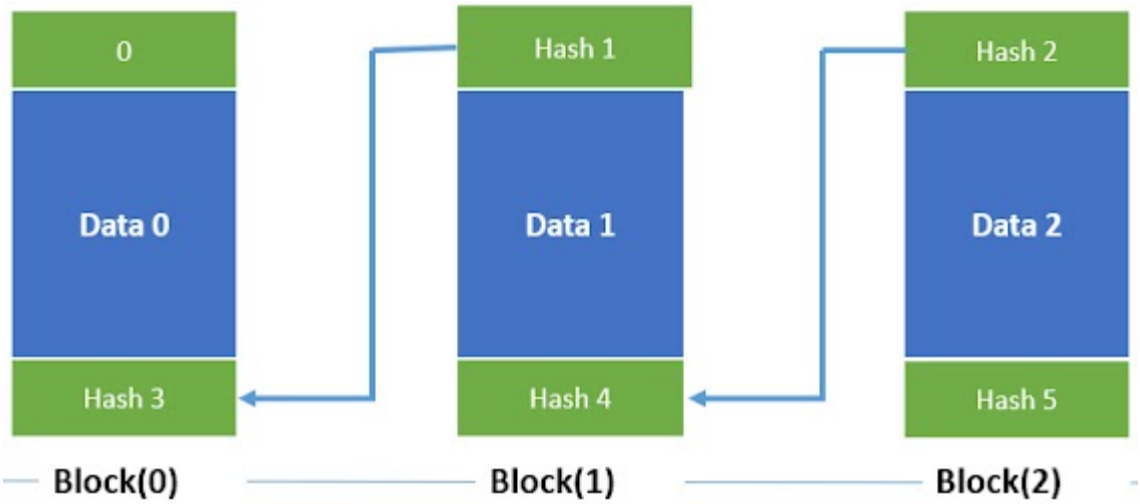
- ( ) A) Komputasi lebh sederhana, cocok untuk perangkat nirkabel
- ( ) B) Panjang kunci lebih pendek, namun tingkat keamanan setara dengan RSA yang kuncinya lebih panjang
- ( ) C) Panjang kunci lebih pendek, menghemat storage dan bandwidth
- (✓) Semua jawaban di atas benar
- ( ) Hanya jawaban A dan C benar
- ( ) Hanya jawaban A dan B benar
- ( ) Hanya jawaban B dan C benar

19. Karakteristik blockchain adalah, KECUALI 4 points

Mark only one oval.

- ( ) Transparansi
- (✓) Terpusat
- ( ) Immutable
- ( ) Independent dan personal
- ( ) Tidak memerlukan pihak ketiga dalam transaksi
- ( ) Tidak ada jawaban yang benar

20. Prhatikan gambar blockchain berikut ini. Nilai hash block(0) = 6ABC1056871F97, nilai hash block(1) = DFC54029876A41, nilai hash block(2) = A851C4BB4501, nilai hash block(3) = 501FD7EA018B. Maka field Hash 1, Hash 2, Hash 3, Hash 4, dan Hash 5 pada gambar akan berisi nilai: 4 points



Mark only one oval.

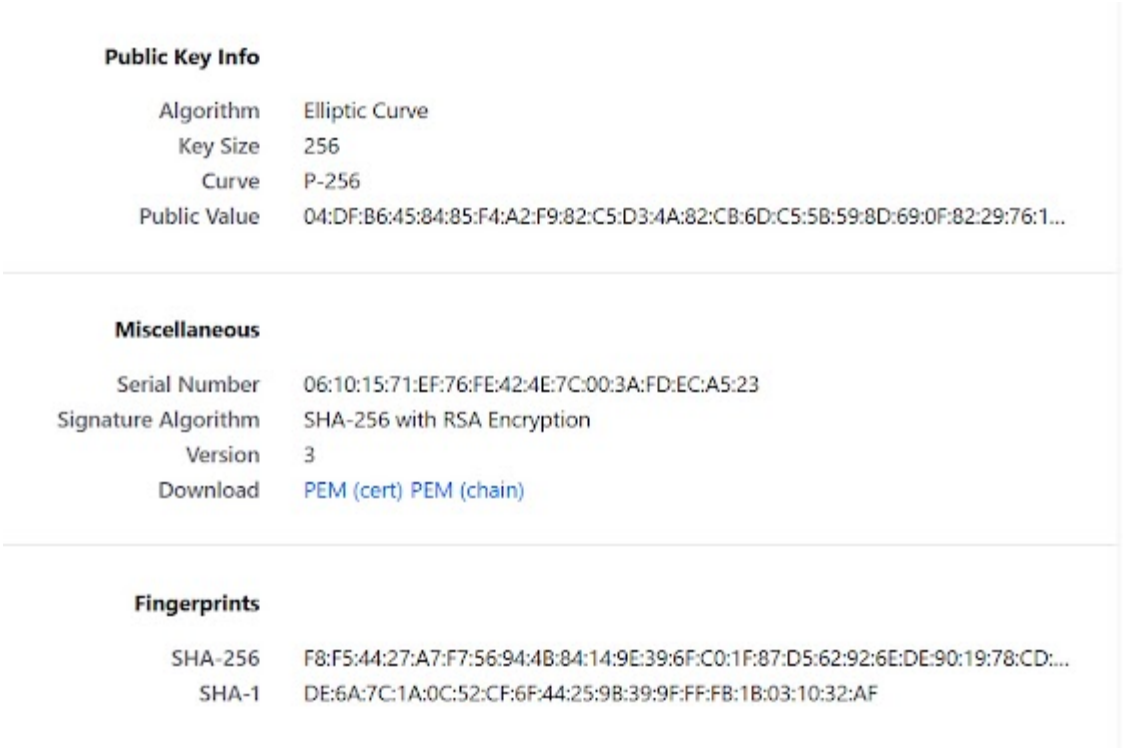
- ( ) Hash 1 = DFC54029876A41
- ( ) Hash 2 = A851C4BB4501
- ( ) Hash 3 = DFC54029876A41
- ( ) Hash 4 = A851C4BB4501
- ( ) Hash 5 = DFC54029876A41
- (✓) Tidak ada jawaban yang benar

21. Tanda tangan digital yang dihitung dengan fungsi hash dan algoritma kriptografi kunci publik akan berbeda-beda nilainya, bergantung pada 4 points

Mark only one oval.

- [ ] A) Kunci privat yang digunakan
- [ ] B) Kunci publik yang digunakan
- [ ] C) Isi pesan
- [ ] D) jawaban A, B, dan C benar
- [ ] E) jawaban A dan B benar
- [x] F) jawaban A dan C benar

22. Gambar berikut adalah sebagian informasi di dalam sertifikat digital situs traveloka.com. Berdasarkan informasi tersebut dapat disimpulkan bahwa: 4 points



Public Key Info

Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:DF:B6:45:84:85:F4:A2:F9:82:C5:D3:4A:82:CB:6D:C5:5B:59:8D:69:0F:82:29:76:1...

Miscellaneous

Serial Number	06:10:15:71:EF:76:FE:42:4E:7C:00:3A:FD:EC:A5:23
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	F8:F5:44:27:A7:F7:56:94:4B:84:14:9E:39:6F:C0:1F:87:D5:62:92:6E:DE:90:19:78:CD:...
SHA-1	DE:6A:7C:1A:0C:52:CF:6F:44:25:9B:39:9F:FF:FB:1B:03:10:32:AF

Mark only one oval.

- ( ) Fungsi hash yang digunakan untuk tanda-tangan digital adalah SHA-1
- ( ) Algoritma kunci publik yang digunakan untuk tanda tangan digital adalah Elliptic Curve
- ( ) Kunci publik algoritma RSA adalah 04:DF:B6:45:84:85:F4:A2:F9:82:C5:D3:4A:82:CB:6D:C5:5B:59:8D:69:0F:82:29:76:1F:46:
- ( ) Panjang kunci publik algoritma RSA adalah 256 bit
- (✓) Nilai hash sertifikat digital adalah DE:6A:7C:1A:0C:52:CF:6F:44:25:9B:39:9F:FF:FB:1B:03:10:32:AF
- ( ) Version 3 adalah versi serial number

23. Algoritma kriptografi kunci publik apa saja yang dapat digunakan untuk menandatangani pesan? 4 points

Mark only one oval.

- [ ] Diffie-Hellman
- [ ] AES
- [ ] DES
- [x] RSA
- [ ] MD5

Soal Essay

24. Misalkan Alice dan Bob akan bertukar kunci sesi dengan algoritma Diffie-Hellman. Alice dan Bob menyepakati bilangan prima n = 23 dan g = 11. Alice memilih kunci privatnya x = 6 dan Bob memilih kunci privatnya y = 5. Hitung kunci K yang diperoleh oleh Alice dan Bob. 10 points

25. Jelaskan cara sistem mengotentikasi password pengguna dengan menggunakan public key dan private key pengguna yang login ke sistem. Public key pengguna disimpan oleh sistem, sedangkan private key pengguna hanya diketahui oleh pengguna. (Petunjuk:mekanisme challenge and response) 10 points

26. Tentukan perkiraan nilai anda untuk mata kuliah ini * 2 points

Mark only one oval.

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