UAS IF4020 Kriptografi - Sem 2 - 2022/2023

Ujian Akhir Semester
Hari/Tanggal: Senin 8 Mei 2023
Waktu: 100 menit
Sifat ujian: TUTUP BUKU

* Indicates required question

1. Email *

Identitas dan Pernyataan

2. Nama *

3. NIM *

4. Email (std) *

5. Tulis ulang pernyataan berikut: *

"Saya menyatakan bahwa:
1. 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 IF4020 Semester 2 Tahun 2022/2023.
2. Tidak menyebarkan soal ujian kepada mahasiswa lain yang mengambil mata kuliah serupa. Apabila di kemudian hari diketahui saya menyebarkan soal ujian kepada mahasiswa lain, maka saya bersedia mendapatkan nilai E pada mata kuliah IF4020 Semester 2 Tahun 2022/2023 "

A. SOAL PILIHAN GANDA

Pilihlah satu jawaban YANG
PALING BENAR. Soal UAS pilihan berganda terdiri dari total 24
pertanyaan. Setiap soal bernilai 3, kecuali soal terakhir (prediksi nilai) bernilai 2. 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

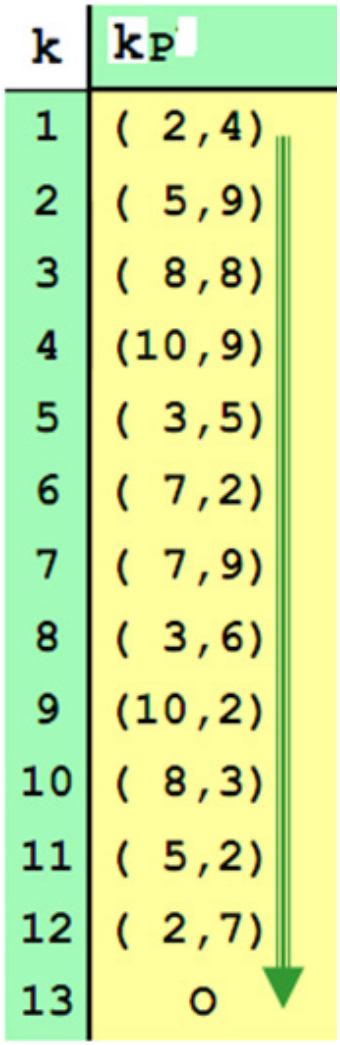
6. Misakan P adalah titik di kurva eliptik. Pernyataan yang SALAH tentang komputasi pada kurva eliptik adalah:

Mark only one oval.

- ◯ P - P = titik di infinity (O)
- ◯ Jika ordinat P sama dengan nol, maka P + P = 2P = titik di infinity
- ◯ P + titik di infinity = P
- ✓ P^n = P x P x ... P (sebanyak n kali)
- ◯ Tidak ada jawaban yang memenuhi

7. Diketahui B = (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 B sebagai basis. Misalkan Alice memilih kunci privat a = 3 dan Bob memilih kunci privat b = 5. 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.

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

8. 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

9. Fungsi hash yang dapat menghasilkan message digest berukuran sembarang adalah:

Mark only one oval.

- ( ) SHA-1
- ( ) MD5
- ( ) SHA-256
- ( ) SHA-512
- (✓) Keccak
- ( ) SHA-2

10. 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 terseebut 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
- [x] 160 bit
- [ ] 190 bit
- [ ] 256 bit
- [ ] Tidak ada jawaban yang benar

11. Alice mengirim pesan kepada Bob. Alice memiliki kunci privat a dan kunci publik A. Bob memiliki kunci privat b dan kunci publik B. Untuk menandatangani pesan tersebut, maka Alice mengenkripsi pesan dengan menggunakan

Mark only one oval.

- [x] a
- [ ] A
- [ ] b
- [ ] B
- [ ] a dan A
- [ ] b dan B
- [ ] a dan B
- [ ] b dan A

12. (Lanjutan soal di atas) Bob memverifikasi tanda-tangan digital Alice dengan mendekripsi tanda-tangan digital menggunakan:

Mark only one oval.

- [ ] a
- [x] A
- [ ] b
- [ ] B
- [ ] a dan B
- [ ] b dan A
- [ ] a dan A
- [ ] Option 8
- [ ] Option 9

13. Berikut daftar algoritma kriptografi:
    1. RSA
    2. ElGamal signature
    3. DSA
    4. Diffie-Hellman
    5. AES

    Algoritma apa yang dapat digunakan untuk menandatangani pesan?

Mark only one oval.

- [ ] 1, 2, 3, 4, 5
- [ ] 1, 2, 3, 4
- [x] 1, 2, 3
- [ ] 1, 2
- [ ] 2, 3

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

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

15. Tanda-tangan digital yang menggunakan kombinasi fungsi hash dan algoritma kriptografi kunci publik dapat digunakan untuk layanan kriptografi berikut:

Mark only one oval.

- Confidentiality, authentication, data integrity, non-repudiaton
- authentication dan data integrity
- data integrity dan non-repudiation
- [x] data integrity, authentication, non-repudiation
- non-repudiation
- authentication dan non-repudiation
- tidak ada jawaban yang benar

16. Sertifikat digital berisi informasi yang mengikat kunci publik dengan identitas pemilik kunci. Sesuai standar X.509, informasi apa saja yang tidak dimuat di dalam sertifikat digital?

Mark only one oval.

- [ ] Nomor seri sertifikat
- [ ] Tanggal mulai berlaku dan tanggal kadaluarsa
- [ ] Nama CA
- [ ] Algoritma tanda-tangan yang digunakan
- [x] Tanda-tangan digital pemilik kunci
- [ ] Versi X.509
- [ ] Tidak ada jawaban yang benar

17. Untuk memverifikasi tanda-tangan di dalam sertifikat digital, maka digunakan:

Mark only one oval.

- [ ] Kunci privat pemilik kunci publik
- [ ] Kunci publik pemilik kunci publik
- [ ] Kunci privat CA
- [x] Kunci publik CA
- [ ] Kunci publik pengguna sertifikat
- [ ] Kunci privat pengguna sertifikat
- [ ] Tidak adajawaban yang benar

18. Pembangkit bilangan acak yang digunakan oleh prosedur komputasi bersifat, KECUALI:

Mark only one oval.

- [ ] bilangan yang dibangkitkan adalah semi-acak
- [ ] deterministik
- [ ] memerlukan umpan (seed)
- [x] tidak memiliki periode
- [ ] tidak ada jawaban yang benar

19. Barisan bit biner acak akan dibangkitkan dengan Blum Blum Shub (BBS). Misalkan p = 11, q = 23, dan s = 3. Maka, 3 bit pertama baisan bit acak yang dibangkitkan adalah:

Mark only one oval.

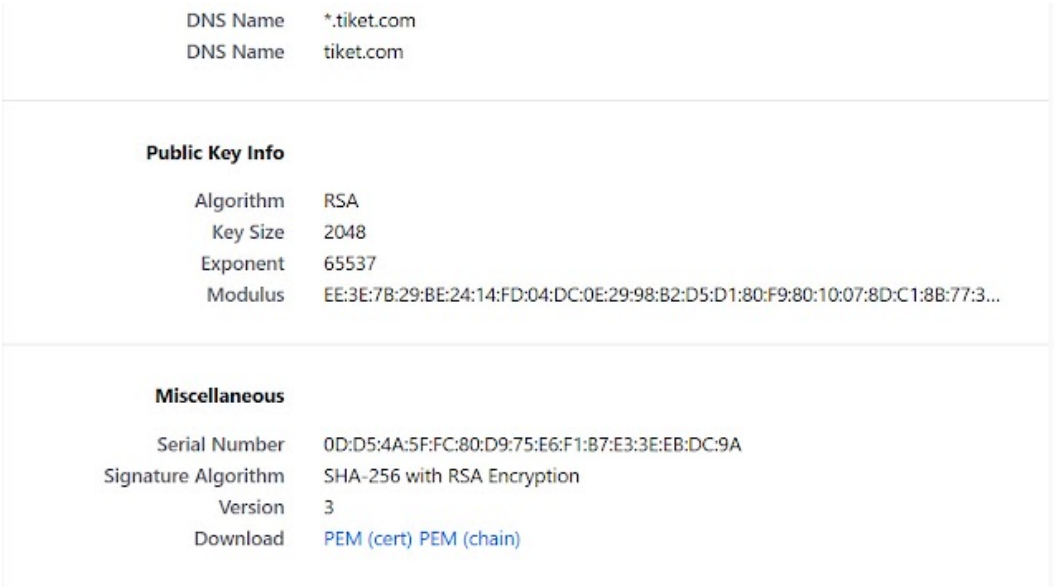
- [x] 100
- [ ] 101
- [ ] 110
- [ ] 010
- [ ] 001
- [ ] 011
- [ ] Tidak ada jawaban yang benar

20. 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" antara client dan server
- [x] Melakukan enkripsi pesan
- [ ] Tidak ada jawaban yang benar

21. Gambar di bawah ini memperlihatkan tangkapan layar sertifikat digital web server tiket.com. Dari gambar tersebut dapat diperoleh informasi sebagai berikut, KECUALI



DNS Name	*.tiket.com
DNS Name	tiket.com
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	EE:3E:7B:29:BE:24:14:FD:04:DC:0E:29:98:B2:D5:D1:80:F9:80:10:07:8D:C1:8B:77:3...
Miscellaneous	
Serial Number	0D:D5:4A:5F:FC:80:D9:75:E6:F1:B7:E3:3E:EB:DC:9A
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Mark only one oval.

- ( ) Algoritma yang digunakan untuk tanda-tangan digital adalah SHA-256 dan RSA
- ( ) Tiket.com menggunaan algoritma RSA untuk enkripsi dan dekripsi
- (✓) Kunci publik tiket.com adalah e = EE:3E:7B:29:BE:24:14:FD:04:DC:0E:29:98:B2:D5:D1:80:F9:80:10:07:8D:C1:8B:77:31:07:18:0A
- ( ) Versi X.509 yang digunakan adalah versi 3
- ( ) Nomor seri sertifikat digital adalah 0D:D5:4A:5F:FC:80:D9:75:E6:F1:B7:E3:3E:EB:DC:9A
- ( ) Panjang modulus adalah 2048 bit
- ( ) Tidak ada jawaban yang benar

22. Mengalikan dua buah cipherteks hasilnya apabila didekripsi sama dengan perkalian dua buah plainteksnya, merupakan karakteristik algoritma enkripsi homomorfik:

Mark only one oval.

- ( ) RSA
- ( ) Elgamal
- ( ) Paillier
- (✓) RSA dan Elgamal
- ( ) RSA dan Paillier
- ( ) Elgamal dan Paillier
- ( ) Tidak ada jawaban yang benar

23. Algoritma Paillier merupakan algoritma enkripsi homomorfik yang bersifat aditif, artinya

Mark only one oval.

- (✓) Jika dua buah cipherteks dikalikan maka hasil dekripsinya sama dengan penjumlahan kedua plainteksnya
- ( ) Jika dua buah cipherteks dijumlahkan maka hasil dekripsinya sama dengan penjumlahan kedua plainteksnya
- ( ) Jika dua buah cipherteks dikalikan maka hasil dekripsinya sama dengan perkalian kedua plainteksnya
- ( ) Jika dua buah cipherteks dijumlahkan maka hasil dekripsinya sama dengan perkalian kedua plainteksnya
- ( ) Tidak ada jawaban yang benar

24. Setiap blok di dalam blockchain terangkai dengan blok tetangganya, karena setiap blok 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

25. Untuk memutuskan apakah sebuah peer dapat menambahkan sebuah blok di dalam jaringan blockchain , maka diperlukan metode persetujuan untuk menyepakati peer mana yang dapat menambahkan blok. Metode persetujuan ini dinamakan:

Mark only one oval.

- ( ) smart contract
- (✓) consensus
- ( ) immutable
- ( ) decentralized
- ( ) ethereum
- ( ) Tidak ada jawaban yang benar

26. Komponen-komponen di dalam PKI adalah, KECUALI

Mark only one oval.

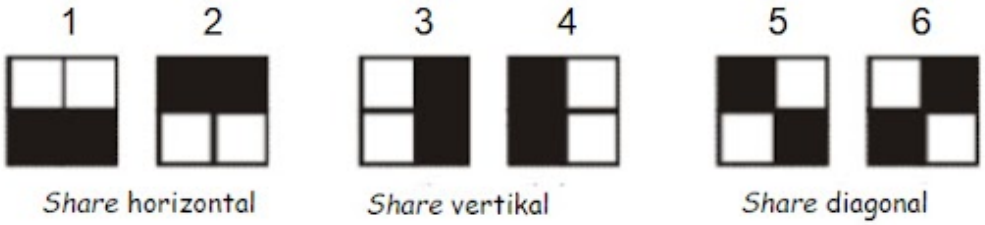
- [ ] Sertifikat digital
- [ ] Repositori
- [ ] Certification Authority (CA)
- [ ] Kebijakan (policy)
- [ ] Registration Authority (RA)
- [x] Kunci publik
- [ ] Tidak ada jawaban yang benar

27. Sebuah secret S dibagi menjadi 5 buah share dan dibagikan kepada 5 orang, yaitu Amir, Budi, Cana, Dimas, dan Endang. Skema secret sharing scheme yang digunakan adalah (3, 5). Untuk merekonstruksi kembali secret S, maka gabungan pemilik share yang dapat menghasilkan S adalah

Mark only one oval.

- [ ] A) Cana, Endang
- [ ] B) Amir, Dimas
- [ ] C) Amir, Budi, Cana
- [ ] D) Amir, Budi, Cana, Dimas
- [ ] E) Amir, Budi, Cana, Dimas, Endang
- [ ] Semua jawaban benar
- [x] Jawaban C, D, dan E benar
- [ ] Semua jawaban salah

28. Di dalam sebuah skema kriptografi visual, satu pixel dibagi menjadi 4 buah sub pixel seperti pada gambar berikut. Sebuah pixel pada original image dibagi menjadi empat buah sub-pixel pada share 1 dan share 2. Kombinasi share 1 dan share 2 mana yang tidak menghasilkan pixel berwarna "putih"?



Mark only one oval.

- [ ] 2 dan 5
- [ ] 3 dan 6
- [ ] 1 dan 3
- [x] 5 dan 6
- [ ] 1 dan 4
- [ ] Tidak ada jawaban yang benar

29. Prediksi nilai anda untuk mata kuliah ini adalah:

Mark only one oval.

- [x] A
- [x] AB
- [x] B
- [x] BC
- [x] C
- [x] D
- [x] E

B. SOAL ESSAY

Jawablah soal essay ini pada kertas jawaban, jangan pada google form ini

30. 1. (NILAI = 15) Alice menandatangani pesan M dengan menggunakan kombinasi fungsi hash dan algoritma kunci publik. Fungsi hash yang digunakan adalah H, algoritma kriptografi kunci publik yang digunakan adalah E, algoritma dekripsinya adalah D. Kunci privat Alice adalah a, kunci publiknya A. Kunci privat Bob adalah b, dan kunci publiknya adalah B. Gambarkan satu diagram yang memperlihatkan pembangkitan tanda-tangan digital S pada sisi Alice dan verifikasi tanda tangan digital pada sisi Bob menggunakan variabel-variabel tersebut.

31. 2. (NILAI = 14) Tuliskan sebuah protokol (langkah-langkah 1, 2, 3...) untuk mengotentikasi sebuah server oleh client dengan mekanisme "challenge and response" menggunakan kriptografi kunci publik.