INSTITUT TEKNOLOGI TELKOM SURABAYA
FAKULTAS TEKNOLOGI INFORMASI DAN INDUSTRI
PRODI S1 TEKNOLOGI INFORMASI

RENCANA PEMBELAJARAN SEMESTER

Mata Kuliah (MK)	Kode MK	Rumpun MK/Kelompok Keahlian (KK)	Bobot (SKS)	Semester	Tanggal Penyusunan
Kriptografi	ITA40J3	Mata Kuliah Pilihan	**3**	7	20 Juni 2019

Pengembang RPS	Koordinator RMK	Ketua Program Studi
Arliyanti Nurdin, S.T.,M.T.	Farah Zakiyah R., S.ST., M.T.	Farah Zakiyah R., S.ST., M.T.

Capaian Pembelajaran (CP)

CPL-PRODI (Kode P,KU,KK,P)

[P-01]	Menjelaskan konsep-konsep matematika untuk memecahkan berbagai masalah yang berkaitan dengan logika.
[P-02]	Menjelaskan konsep dan teori dasar logika dan struktur diskrit untuk mendukung permodelan dan penganalisaan masalah.
[KU-08]	Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada di bawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri.
[KK-01]	Menerapkan metode kriptografi.
[KK-02]	Membuat algoritma yang efisien untuk penyelesaian sebuah persoalan tertentu yang diimplementasikan dengan bahasa pemrograman.
[KK-06]	Memahami dan menerapkan berbagai paradigma pemrograman.
[KK-08]	Merancang, mengimplementasi, menguji, dan men-debug sebuah sandi blok sederhana.
[S-09]	Mampu menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri.

CP-MK (Kode M)

[M-1]	Mengenal beberapa jenis algoritma kriptografi klasik dan modern
[M-2]	Membuat beberapa jenis algoritma kriptografi sederhana terkait permasalahan sehari-hari

	SUB-CPMK (Kode L) L-1 Mahasiswa mampu memahami konsep kriptografi secara umum dan urgensinya dalam dunia teknologi informasi.
Deskripsi Singkat MK	Mata kuliah ini membahas sejarah kriptografi, perkembangan kriptografi modern, dan dasar-dasar teori yang digunakan dalam kriptografi. Materi kriptografi yang dibahas di antaranya adalah sistem kripto simetris klasik, sistem kripto simestri konvensional (DES dan AES), sistem kripto asimetris, protokol pertukaran kunci Diffie-Hellman, skema tanda tangan digital, dan skema distribusi rahasia. Setelah mengikuti perkuliahan, mahasiswa diharapkan memiliki pemahaman dasar teori dan keterampilan teknis dasar dalam kriptografi.
Materi Pembelajaran/ Pokok Bahasan	1. Pengenalan konsep kriptografi secara umum. 2. Konsep kriptografi konvensional. 3. Sistem kripto kunci public dan privat. 4. Metode tanda tangan digital beserta keunggulan dan kelemahannya. 5. Fungsi hash beserta keunggulan dan kelemahannya. 6. Sertifikat digital beserta keungulan dan kelemahannya. 7. Faktor persekutuan terbesar/ *greatest common divisor* (FPB/GCD). 8. Algoritma Euklid untuk kalkulasi GCD. 9. Sistem kongkurensi linear dan Teorema Sisa Tiongkok (*Chinese Remainder Theorem*, CRT). 10. Relatif prima dan fungsi phi Euler serta sifat-sifatnya. 11. Pengantar medan hingga (*finite field*) Z_p (bilangan bulat modulo p, dengan p prima). 12. Kongkurensi linear modulo p (p bilangan prima). 13. Sandi blok dan sandi stream. 14. *Data Encryption Standard* (DES). 15. *Advanced Encryption Standard* (AES). 16. IDEA 17. *Left feedback shift register* (LFSR). 18. Sandi *Vigenere*. 19. Sistem kripto SEAL. 20. Sistem kripto RC4. 21. Konsep sistem kripto kunci public

	22. Teorema kecil Fermat dan aplikasinya. 23. Sistemkripto Rivest-Shamir-Adleman (RSA). 24. Protokol pertukaran kunci Diffie-Hellman. 25. Sistemkripto El Gamal. 26. Konsep dan cara kerja skema tanda tangan digital. 27. konsep dasar dan metode pendistribusian dan pengendalian kunci. 28. *Message Authentication Code* (MAC). 29. Unconditionally secure authentication code. 30. Sistem KERBEROS. *31. Pretty Good Privacy* 32. *Universal electronic payment system*.
Pustaka	**Utama** 1. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone. *Handbook of Applied Cryptography* CRC Press. 1996. 2. Douglas R. Stinson. *Cryptography: Theory and Practice, 3rd Edition.* Chapman & Hall/ CRC. 2005 3. Niels Ferguson, Bruce Schneider, Tadayashi Kohno. *Cryptograpgy Engineering: Design Principles and Practical Applications.* Wiley. 2010. 4. J. Hoffstein, J. C. Pipher, J. H. Silverman. *An Introduction to Mathematical Cryptography, 2nd Edition.* Springer. 2014 **Pendukung**
Media Pembelajaran	**Perangkat Keras**: Komputer/ Laptop **Perangkat Lunak**
Team Teaching	
Assessment	
Matakuliah Prasyarat	Dasar Algoritma dan Pemrograman, Algoritma dan Struktur Data, Logika Matematika, Matematika Diskrit

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
1	Mahasiswa mampu memahami konsep kriptografi secara umum dan urgensinya dalam dunia teknologi informasi.	1. Memahami konsep kriptografi secara umum dan kaitannya dengan mata kuliah dasar yang telah diambil. 2. Mengetahui sejarah kriptografi, beserta beberapa contoh sistem kripto yang digunakan. 3. Memahami prinsip dasar dan contoh kriptografi konvensional.	1. Pengenalan konsep kriptografi secara umum. 2. Sejarah kriptografi. 3. Definisi kriptografi. 4. Konsep kriptografi konvensional.	**Bentuk:** Kuliah **Metode:** Ceramah, diskusi, tanyajawab	Kuis 1: Mendefinisikan kriptografi dengan bahasa ilmiah sendiri. Kuis 2: Menjelaskan prinsip dasar kriptografi.	**TM: 1 x(3x50")** **BT : 1x(3x60")]** **BM : 1x(3x60")]**	**Tes :** Tulis Pedoman Penskoran **Non Tes:** Kuis : Post-Test	1. Ketepatan menjelaskan konsep kriptografi secara umum. 2. Ketepatan menjelaskan secara singkat sejarah kriptografi, beserta beberapa contoh sistem kripto yang digunakan. 3. Kebenaran dalam mendefinisikan kriptografi dengan bahasa ilmiah sendiri. 4. Ketepatan	5	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								dalam menjelaskan prinsip dasar dan contoh kriptografi konvensional.		
2	Mahasiswa mampu memahami konsep dasar sistem kripto kunci public dan privat, tanda tangan digital, fungsi hash, dan sertifikat digital.	1. Memahami secara umum sistem kripto kunci public (*public key cryptogsystem*) dan memberikan contohnya. 2. Memahami secara umum sistem kripto kunci privat/ rahasia (*Private/ secret key crypto system)* dan memberikan contohnya. 3. Memahami secara umum metode tanda tangan digital (*digital signature scheme*) dan memberikan contohnya. 4. Mampu menjelaskan secara umum fungsi hash	1. Sistem kripto kunci public berikut keunggulan dan kelemahannya. 2. Sistem kripto kunci privat/ rahasia berikut keunggulan dan kelemahannya. 3. Metode tanda tangan digital beserta keunggulan dan kelemahannya. 4. Fungsi hash beserta keunggulan dan kelemahannya. 5. Sertifikat digital beserta keungulan dan kelemahannya.	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning, simulasi komputasi, tanyajawab,		**TM: 1 x(3x50")** **BT : 1x(3x60")]** **BM : 1x(3x60")]**	**Tes:** Tulis Pedoman penskoran	1. Ketepatan dalam menjelaskan secara umum sistem kripto kunci publik dan sistem kripto kunci privat/ rahasia. 2. Ketepatan dalam membedakan sistem kripto kunci publik dan kunci rahasia, serta memberikan keunggulan dan	5	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
		dan memberikan contohnya. 5. Mampu menjelaskan secara umum sertifikat digital dan memberikan contohnya.						kelemahannya. 3. Ketepatan dalam menjelaskan secara umum metode tanda tangan digital, fungsi hash, dan sertifkat digital. 4. Ketepatan dalam kalkulasi fungsi hash sederhana.		

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
3	Mahasiswa mampu melakukan kalkulasi aritmatika sederhana dalam ring bilangan bulat modulo n.	1. Menghitung FPB/ GCD dari dua bilangan bulat dengan algoritma Euklid (*Euclidean algorithm*). 2. Menggunkaan teorema-teorema terkait GCD untuk mempermudah kalkulasi GCD. 3. Mengklasifikasikan kelas-kelas kongruensi bilangan bulat. 4. Melakukan kalkulasi aritmatika sederhana dalam ring bilangan bulat modulo n. 5. Menentukan invers perkalian (*multiplicative inverse*) dari suatu bilangan dalam ring bilangan bulat modulo n (jika ada).	1. Faktor persekutuan terbesar/ *greatest common divisor* (FPB/GCD). 2. Pengantar ring bilangan bulat modulo n, Z_n. 3. Keterbagian dan kongruensi bilangan bulat. 4. Algoritma Euklid untuk kalkulasi GCD. 5. Algoritma *extended* Euklid untuk kalkulasi invers perkalian pada ring bilangan bulat modulo n.	**Bentuk:** Kuliah **Metode:** Ceramah, diskusi, latihan	**Tugas :** Menerapkan algoritma euklid pada studi kasus.	**TM: 1 x(3x50")** **BT : 1x(3x60")]** **BM : 1x(3x60")]**	**Tes**: Tulis Pedoman Penskoran **Non Tes :** Tugas Rubrik penilaian	1. Kebenaran dalam menghitung FPB dari dua bilangan bulat dengan algortima euklid. 2. Ketepatan dalam menggunakan teorema GCD. 3. Ketepatan dalam mengklasifikasikan kelas-kelas kongruensi bilangan bulat. 4. Ketetapan dalam kalkulasi aritmatika		Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								dalam ring bilangan bulat modulo n. 5. Ketepatan dalam menghitung invers perkalian dari suatu bilangan dalm ring bilangan bulat modulo n.		
4	Mampu menyelesaikan sistem kongkurensi linear.	1. Menyelesaikan sistem kongkurensi linear (dengan subtitusi balik/ *backward substitution* atau TST/CRT). 2. Menjelaskan fungsi phi Euler dan proses kalkulasinya. 3. Menyelesaikan	1. Sistem kongkurensi linear dan Teorema Sisa Tiongkok (*Chinese Remainder Theorem*, CRT). 2. Relatif prima dan fungsi phi Euler serta sifat-sifatnya. 3. Pengantar medan	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)	**Kuis :** Menyelesaikan studi kasus sistem kongkurensi linear.	**TM: 1 x(3x50")** **BT : 1x(3x60")]** **BM : 1x(3x60")]**	**Tes**: Tulis Pedoman Penskoran **Non Tes :** Kuis (akhir pertemuan) Rubrik penilaian	1. Ketepatan dalam menyelesaikan sistem kongkurensi linear dan Teorema Sisa Tiongkok. 2. Ketepatan dalam menjelaskan fungsi phi	5	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
		kongkurensi linear di Z_p(kongkurensi linear modulo p, p bilangan prima). 4. Menghitung pangkat bilangan dalam Z_p dengan bantuan TFK/ FLT.	hingga (*finite field*) Z_p (bilangan bulat modulo p, dengan p prima). 4. Kongkurensi linear modulo p (p bilangan prima). 5. Pangkat bilangan dalam Z_p (*power of a number in modulo prime*) dan Teorema Kecil Fermat (*Fermat's Little Theorem*, FLT)					Euler dan proses kalkulasinya. 3. Ketepanatn dalam menyelesaikan kongkurensi linear di Z_p(kongkurensi linear modulo p, p bilangan prima). 4. Ketepatan dalam menghitung pangkat bilangan dalam Z_p dengan bantuan TFK/ FLT.		
5	Mahasiswa mampu menghitung kongkurensi binomial dan	1. Memahami dan definisi akar primitive (*primitive roots*) di Z_p. 2. Memahami definisi	1. Akar primitif di Z_p. 2. Residu kuadratik, kongruensi binomial, dan	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning	**Tugas :** Menyelesaikan studi kasus logaritma	**TM: 1 x(3x50")** **BT : 1x(3x60**	**Tes:** Tulis Pedoman Penskoran **Non Tes :**	1. Ketepatan mendefinisikan akar primitive (*primitive*	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
	logaritma diskrit dari bilangan di Z_n	residu kuadratik (*quadratic residue*), kongkurensi binomial, dan symbol Legendre di Z_p. 3. Menghitung kongkurensi binomial dari bilangan di Z_p. 4. Memahami definisi dan mampu menghitung logaritma diskrit di Z_p.	symbol Legendre di Z_p. 3. Logaritma diskrit di Z_p.	(latihan/ simulasi)	diskrit.	**")]** **BM : 1x(3x60")]**	Tugas Rubrik penilaian	*roots*) di Z_p. 2. Ketepatan mendefinisikan residu kuadratik (*quadratic residue*), kongkurensi binomial, dan symbol Legendre di Z_p. 3. Ketapatan dalam menghitung kongkurensi binomial dari bilangan di Z_p. 4. Ketepatan dalam menghitung logaritma diskrit di Z_p.		
6	Mahasiswa mampu menjelaskan prinsip kerja	1. Memahami prinsip kerja sandi blok dan sandi stream.	**1.** Sandi blok dan sandi stream. **2.** *Data Encryption*	**Bentuk:** Kuliah **Metode:** Ceramah,	**Tugas :** Memberikan contoh aplikasi	**TM: 1 x(3x50")** **BT :**	**Tes:** Tulis Pedoman penskoran	1. Ketepatan dalam menjelaskan	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
	sandi blok (*block cipher*) dan sandi stream (*stream cipher*). Mahasiswa mampu menjelaskan cara kerja sistem kripto *Data Encryption Standard* (DES).	2. Memahami kelebihan dan kekurangan sandi blok dan sandi stream. 3. Memahami cara kerja sistem kripto *Data Encryption Standard* (DES). 4. Mampu memberikan contoh aplikasi DES.	*Standard* (DES).	diskusi, latihan.	DES	**1x(3x60")]** **BM : 1x(3x60")]**	**Non tes :** Tugas Rubrik penilaian	prinsip kerja sandi blok dan sandi stream. 2. Ketepatan dalam menjelaskan cara kerja sistem kripto *Data Encryption Standard* (DES).		
7	Mahasiswa mampu menjelaskan cara kerja sistem kripto *iterated* DES, DESX, dan AES (*Advanced Encryption Standard*) serta perbedaan DES dan AES. Mahasiswa mampu menjelaskan cara kerja IDEA.	1. Memahami cara kerja sistem kripto *iterated* DES, DESX, dan AES (*Advanced Encryption Standard*). 2. Memahami perbedaan DES dan AES. 3. Memahami cara kerja IDEA.	1. DES dan beberapa varian dari DES : *iterated* DES dan DESX. 2. *Advanced Encryption Standard* (AES). 3. IDEA	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)	Kuis : Menjelaskan cara kerja DES, AES, dan IDEA.	**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Non tes:** Kuis	1. Ketepatan dalam ,menjelaskan cara kerja sistem kripto *iterated* DES, DESX, dan AES (*Advanced Encryption Standard*). 2. Ketepatan dalam mendeskripsikan	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								perbedaan DES dan AES. 3. Ketepatan dalam menjelaskan cara kerja IDEA.		
UTS										
9	Mahasiswa mampu menjelaskan prinsip kerja *left feedback shift register* (LFSR), sandi Vigenere Mahasiswa mampu menjelaskan sistem kripto SEAL dan RC4 serta memberikan beberapa aplikasinya.	1. Memahami prinsip kerja *left feedback shift register* (LFSR), sandi Vigenere. 2. Memahami sistem kripto SEAL dan RC4 serta memberikan beberapa aplikasinya.	1. *Left feedback shift register* (LFSR). 2. Sandi Vigenere. 3. Sistem kripto SEAL. 4. Sistem kripto RC4.	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketapatan dalam menjelaskan prinsip kerja *left feedback shift register* (LFSR), sandi Vigenere. 2. Ketepatan dalam mengaplikasikan sistem kripto SEAL dan RC4 dalam keamanan informasi.	10	Utama : [3], penunjang :[1,2,4]
10	Mahasiswa mampu menjelaskan	1. Memahami perbedaan sistem kripto asimetris dan	1. Konsep sistem kripto kunci public	**Bentuk:** Kuliah **Metode:**		**[TM: 1 x(3x50")**	**Tes**: Tulis Pedoman	1. Ketepatan dalam menjelaskan	10	Utama : [3], penunjang

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
	prinsip kerja sistem kripto asimetris.	simetris. 2. Memahami Teorema Kecil Fermat dan aplikasinya dalam pangkat bilangan bulat di Zn. 3. Memahami prinsip kerja sistemkripto Rivest-Shamir-Adleman (RSA). 4. Memahami kebenaran fungsi enkripsi dan dekripsi untuk RSA secara formal.	2. Teorema kecil Fermat dan aplikasinya. 3. Sistemkripto Rivest-Shamir-Adleman (RSA).	Ceramah, problem-based learning (latihan/ simulasi)		**]** **[BT+BM:(1+1) x(3x60")]**	Penskoran	perbedaan sistem kripto asimetris dan simetris. 2. Ketepatan dalam mengaplikasikan teorema Kecil Fermat dalam pangkat bilangan bulat di Zn. 3. Ketapatan dalam menjelaskan prinsip kerja sistemkripto Rivest-Shamir-Adleman (RSA).		:[1,2,4]
	Mahasiswa mampu menjelaskan prinsip kerja protocol pertukaran kunci Diffie-Hellman dan sistemkripto	1. Memahami prinsip kerja protocol pertukaran kunci Diffie-Hellman dan contoh penerapannya. 2. Memahami prinsip kerja sistemkripto El	1. Protokol pertukaran kunci Diffie-Hellman. 2. Sistemkripto El Gamal.	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")**	**Tes**: Tulis Pedoman Penskoran	1. Ketapatan dalam menjelaskan prinsip kerja protocol pertukaran kunci Diffie-		Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
	El Gamal serta contoh penerapannya.	Gamal dan contoh penerapannya.				]		Hellman dan contoh penerapannya. 2. Ketepatan dalam menjelaskan prinsip kerja sistemkripto El Gamal dan contoh penerapannya.		
11	Mahasiswa mampu menerapkan skema tanda tangan digital dan melakukan verifikasi tanda tangan digital dengan sistem batch.	1. Memahami konsep dan cara kerja skema tanda tangan digital. 2. Memahami prinsip dan cara kerja skema tanda tangan digital RSA, dan penerapannya. 3. Memahami prinsip dan cara kerja skema tanda tangan digital Ong – Schnorr – Shamir dan penerapannya. 4. Memahami verifikasi tanda tangan digital dengan sistem *batch*.	1. Konsep dan cara kerja skema tanda tangan digital. 2. Skema tanda tangan digital RSA. 3. Skema tanda tangan Ong-Schnorr – Shamir. 4. Metode verifikasi skema tanda tangan digital dengan sistem *batch.*	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketapatan dalam menjelaskan konsep dan cara kerja skema tanda tangan digital. 2. Ketepatan menjelaskan prinsip dan cara kerja skema tanda tangan digital RSA, dan penerapannya. 3. Ketapatan menjelaskan	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								prinsip dan cara kerja skema tanda tangan digital Ong – Schnorr – Shamir dan penerapannya. 4. Ketepatan menjelaskan verifikasi tanda tangan digital dengan sistem *batch*.		
12	Mahasiswa mampu menjelaskan metode pendistribusian dan pengelolaan kunci rahasia dan kunci publik	1. Memahami konsep dasar pendistribusian kunci. 2. Memahami metode pendistribusian kunci rahasia dan kunci public. 3. Memahami metode penentuan usia kunci. 4. Memahami peran layanan pihak ketiga yang dapat dipercaya. 5. Memahami bentuk	1. Latar belakang dan konsep dasar pendistribusian kunci. 2. Metode mendistribusikan kunci rahasia. 3. Metode mendistribusikan kunci public. 4. Usia kunci. 5. Metode pengendalian pemakaian kunci. 6. Layanan pihak ketiga yang dapat	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketapatan dalam menjelaskan konsep dasar pendisribusian kunci. 2. Ketepatan menjelaskan metode pendistribusian kunci rahasia dan kunci publik. 3. Ketepatan dalam menentukan	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
		pengelolaan kunci yang sesuai untuk suatu sistemkripto.	dipercaya.					usia kunci dari suatu sistemkripto. 4. Ketepatan dalam menjelaskan pengendalian pemakaian kunci dalam suatu sistemkripto. 5. Ketepatan menjelaskan peran layanan pihak ketiga yang dapat dipercaya dalam suatu sistemkripto.		
13	Mahasiswa mampu memahami fungsi hash, message authentication code, dan *unconditionally secure authentication code* dari sebuah sistem.	Memahami fungsi hash, message authentication code, dan *unconditionally secure authentication code* dari sebuah sistem.	1. Fungsi hash 2. *Message Authentication Code (MAC).* 3. *Unconditionally secure authentication code.*	**Bentuk:** Kuliah **Metode:** Ceramah, problem-based learning (latihan/ simulasi)		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketapatan dalam menjelaskan definisi fungsi hash dan contohnya. 2. Ketapatan dalam melakukan kalkulasi beberapa fungsi hash	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								sederhana. 3. Ketepatan menjelaskan menjelaskan MAC dari sebuah sistem dan contohnya. 4. Ketepatan dalam menjelaskan *unconditionally secure authentication code* pada sebuah sistem dan contohnya.		
14	Mahasiswa mampu menjelaskan sistem KERBEROS secara sederhana, konsep *good privacy* dalam keamanan informasi.	1. Memahami sistem KERBEROS secara sederhana. 2. Memahami konsep *pretty good privacy* dalam keamanan informasi. 3. Memahami pengertian *universal electronic payment system* dan contoh penerapannya.	1. Sistem KERBEROS. 2. *Pretty Good Privacy* 3. *Universal electronic payment system.*	**Bentuk:** Kuliah **Metode:** Ceramah, diskusi		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketepatan dalam mendefinisikan sistem KERBEROS secara sederhana. 2. Ketepatan dalam menjelaskan konsep *pretty good privacy* dalam keamanan	10	Utama : [3], penunjang :[1,2,4]

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
								informasi. 3. Ketapatan dalam mendeskripsikan *universal electronic payment system* dan contoh penerapannya.		
15	Mahasiswa mampu melakukan analisis sistemkripto sederhana.	1. Mampu melakukan analisis sistemkripto sederhana. 2. Mampu meberikan contoh sistemkripto sederhana.	1. Analisis sistemkripto sederhana. 2. Presentasi tugas besar.	**Bentuk:** Kuliah **Metode:** Presentasi dan diskusi terkait tugas besar.		**[TM: 1 x(3x50")]** **[BT+BM:(1+1) x(3x60")]**	**Tes**: Tulis Pedoman Penskoran	1. Ketepatan dalam melakukan analisis kinerja sistemkripto sederhana. 2. Ketepatan dalam mengidentifikasi maslaah komputasi yang melandasi kemananan suatu sistemkripto sederhana.	10	Utama : [3], penunjang :[1,2,4]
UAS										
Catatan:										

Pertemuan Ke	Kemampuan Akhir yang direncanakan	Indikator	Materi Pokok	Bentuk dan Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Estimasi Waktu	Penilaian			Referensi
							Bentuk & Kriteria	Indikator Penilaian	Bobot (%)	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)

(1). TM: Tatap Muka; TS: Penugasan Terstruktur; BM: Belajar Mandiri.
(2). 1 sks = (50’ TM + 60’ PT + 60’ BM)/ Minggu
(3). CPL-Prodi: Capaian Pembelajaran Lulusan Program Studi; CP-MK: Capaian Pembelajaran Mata-Kuliah
(4). Simbol-simbol elemen KKNI pada CPL-Prodi: S = Sikap; KU = Ketrampilan Umum; KK = Ketrampilan Khusus; P = Pengetahuan

INSTITUT TEKNOLOGI TELKOM SURABAYA
FAKULTAS TEKNOLOGI INDUSTRI DAN INFORMASI
PRODI STUDI REKAYASA PERANGKAT LUNAK

RENCANA TUGAS MAHASISWA

Mata Kuliah (MK)	Kode MK	Rumpun MK/Kelompok Keahlian (KK)	Bobot (SKS)	Semester	Tahun Akademik
Algoritma dan Pemrograman	**FA11T01**	Algoritma dan Pemrograman	**3**	1	2018/2019

Dosen Pengampu

Arliyanti Nurdin, S.T., M.T.

TUGAS KE-	JUDUL TUGAS
13	Tugas Besar

SUB-CAPAIAN PEMBELAJARAN MATA-KULIAH

Mampu menjelaskan langkah-langkah logis penyelesaian suatu masalah dan menuliskannnya ke dalam bentuk notasi standar.
Mampu menerjemahkan alur penyelesaian masalah yang dihasilkan ke dalam bentuk bahasa pemrograman

TUJUAN PENUGASAN

Menerapkan semua konsep algoritma yang telah dipelajari untuk menyelesaikan kasus tugas besar secara komprehensif dan mempresentasikannya.

DESKRIPSI TUGAS	METODE PENGERJAAN TUGAS
1. Objek Garapan: • Proposal kasus yang akan diselesaikan dan rancangan penyelesaiannya. • Algoritma / program yang dibangun untuk menyelesaikan kasus sesuai dengan proposal yang sudah diajukan. • Laporan dan presentasi algoritma/program yang dibuat sesuai dengan proposal yang sudah diajukan. 2. Batasan: • Proposal berisi deskripsi kasus yang akan diselesaikan, deskripsi program yang akan dibuat, list fungsionalitas program, batasan dan asumsi, definisi	1. Tugas besar dikerjakan secara berkelompok 3-4 orang. 2. Topik tugas besar berasal dari dosen, sedangkan judul boleh berasal dari dosen/ mahasiswa. 3. Format proposal dan laporan diberikan oleh dosen. 4. Program dibuat mengacu pada rancangan penyelesaian kasus yang diajukan oleh mahasiswa.

<table>
<tr><td>kamus yang akan digunakan untuk membangun program, dan rencana pembagian kerja dalam kelompok.
• Algoritma/program untuk menyelesaikan kasus tugas besar dibangun dengan menggunakan bahasa Pemrograman C++.
• Program dan laporan dipresentasikan pada minggu 15</td><td></td></tr>
<tr><th>BENTUK DAN FORMAT LUARAN TUGAS</th><th>INDIKATOR, KRITERIA DAN BOBOT PENILAIAN</th></tr>
<tr><td>1. Proposal
2. Algoritma/Program
3. Laporan</td><td>1. Penilaian Individu (50%)
- Kemampuan presentasi (20%)
- Pemahaman materi (80%)

2. Penilaian Kelompok (50%)
- Kelengkapan dan ketepatan fungsionalitas (50%)
- Ketepatan skema algoritma (30%)
- Tata tulis algoritma/program (20%)</td></tr>
<tr><th>JADWAL PELAKSANAAN TUGAS</th><th>CATATAN /LAIN-LAIN</th></tr>
<tr><td>Proposal dikumpulkan pada minggu ke-13
Laporan dan Presentasi pada minggu ke-15</td><td></td></tr>
<tr><th colspan="2">DAFTAR RUJUKAN</th></tr>
<tr><td colspan="2">Shalahuddin, M., Rosa A.S. 2010. Modul Pembelajaran Algoritma dan Pemrograman. Bandung: Penerbit Modula.
Munir, Rinaldi. 20. Algoritma & Pemrograman dalam Bahasa Pascal dan C; Edisi Revisi. Bandung: Penerbit Informatika</td></tr>
</table>