RENCANA PEMBELAJARAN SEMESTER
PROGRAM STUDI SISTEM KOMPUTER – UNIVERSITAS GUNADARMA

Tanggal Penyusunan	22/09/2022		Tanggal revisi	22/09/2022
Fakultas	Direktorat Magister Teknologi dan Rekayasa			
Program Studi	Perangkat Lunak Sistem Informasi Kode Prodi: 57101			
Jenjang	Magister			
Kode dan Nama MK	MKB		Sistem Keamanana dan Kriptografi	
SKS dan Semester	SKS	2	Semester	
Prasyarat				
Status Mata Kuliah	[✓] Wajib [...] Pilihan			
Dosen Pengampu	Rodiah			
Capaian Pembelajaran Mata Kuliah	Ketrampilan Khusus		- Mampu memecahkan permasalahan berdasarkan dasar dan konsep dari keamanan pada sistem informasi sehingga mampu melakukan pengendalian keamananan dengan mengacu pada Prinsip-prinsip *The Five Trust Service* untuk keandalan system. - Mengetahui dan Memahami jenis serangan cyber (SQL Injection, DoS,Phishing, Man in The middle Attack, RansomWare) - Mengetahui beberapa algoritma modern dengan memahami penggunaan algoritma paling sederhana XOR. Penggunaan algoritma modern berdasarkan stream cipher dan block cipher - Memahami perbedaan kunci public dan kunci private - Mampu menjelaskan dan memahami penggunaan Fungsi Hash (Penggunaan Hash satu arah, Skema Fungsi hash dan konsep bit pengganjal dalam Fungsi Hash) - Memahami impelementasi Kriptografi dalam Blockchain dengan memahami Dasar dalam membangun Teknologi Blockchain sebagai trend teknologi pada Industri 4.0 - Memahami dan dapat menjelaskan tentang dasar dalam melakukan Manajemen Kunci Kriptografi mulai dari Pembangkitan Kunci, Penyebaran Kunci, Penggunaan Kunci, Perubahan Kunci dan Penghancuran Kunci (Key Destruction) - Mengetahui Konsep Keamanan Sistem Informasi dan Lingkup Security dengan memahami bentuk-bentuk ancaman dari sistem keamanan komputer dan implementasi metode pengamanan komputer berdasarkan sistem yang tepat tergantung pada jenis ancamannya - Mengetahui klasifikasi kejahatan komputer baik yang bersifat fisik, yang berhubungan dengan *personal*, keamanan dari data dan media serta teknik *communications* dan keamanan dalam operasi - Memahami konsep melakukan enkripsi, dekripsi dan proses pembangkitan kunci (*Key Generation*)Kriptanalisis dan Kriptologi serta memahami Tujuan implementasi Kriptografi dan Jenis Kriptografi - Mengetahui kategori kriptografi modern berdasarkan stream cipher dan block cipher, prinsip penyandian shannon dan mode operasi pada cipher block. - Memahami dan mampu menjelaskan kelemahan mode operasi pada Cipher Block - Memahami dan dapat menjelaskan cara pembangkitan kunci, proses enkripsi dan dekripsi pada algoritma Public Key (RSA, Diffie Hellman dan Knapsack) - Memahami beberapa algoritma yang mengimplentasikan Fungsi Hash (MD5 dan SHA) - Memahami konsep Digital Signature dengan Enkripsi pesan dan dapat menjelaskan prosedur verfikasi digital signature - Mengetahui Komponen Blockchain dan Cara Kerja Blockchain, cara mendeskripsikan Distibuted Ledger / Database dan dapat memahami cara melakukan Autentikasi dan Verifikasi dengan Kriptografi pada teknologi blockchain	

Capaian Pembelajaran Mata Kuliah	Menguasai teori berbagi jenis penerapan keamanan sistem (Steganografi, Watermarking dan Kriptografi) dan penerapannya Mengetahui -bentuk ancaman dan memahami jenis serangan cyber (SQL Injection, DoS,Phishing, Man in The middle Attack, RansomWare) Mengetahui dan Memahami Konsep dan Konsep dan Terminologi Kriptografi dan syarat-syarat dalam melakukan kriptografi dengan mengerti dan mampu menjelaskan tentang pemahaman enkripsi, dekripsi, cipher, ciphertext, dan dasar pembangkitan kunci pada kriptografi modern Mengetahui memahami kategori kriptografi modern berdasarkan stream cipher dan block cipher serta mampu menjelaskan kelemahan mode operasi pada Cipher Block Mengetahui perbedaan public key dan private key serta proses enkripsi dan dekripsi serta pembangkitan kunci pada beberapa algoritma public key (RSA, Diffie-Hellman dan Knapsack) Memahami penggunaan Fungsi Hash (Penggunaan Hash satu arah, Skema Fungsi hash dan konsep bit pengganjal dalam Fungsi Hash) Memahami dan dapat menjelaskan tentang dasar dalam melakukan Manajemen Kunci Kriptografi mulai dari Pembangkitan Kunci, Penyebaran Kunci, Penggunaan Kunci, Perubahan Kunci dan Penghancuran Kunci (Key Destruction) Memahami dan dapat menjelaskan tentang dasar dalam melakukan Manajemen Kunci Kriptografi mulai dari Pembangkitan Kunci, Penyebaran Kunci, Penggunaan Kunci, Perubahan Kunci dan Penghancuran Kunci (Key Destruction) Memahami mekanisme Konsesus, smart Contract dan membangun Distributed Ledger sebagai dasar dalam teknologi blockchain berdasarkan contoh Penerapan Blockchain berupa Skenario Implementasi Blockchain pada Transaksi Keuangan mulai dari Pembentukan Node, Pembentukan Public dan Private Key, Pembuatan Pasangan Kunci, Pembentukan Blockchain dan teknik Hashing Data Transaksi.			
Deskripsi Umum (Silabus)	Mata kuliah ini secara umum berisi materi mengenai dasar - dasar keamanan sistem informasi,prinsip Sistem Keamanan, jenis-jenis penerapan kemanan sistem, jenis serangan cyber, Konsep dan Terminologi Kriptografi, Konsep Keamanan Sistem Informasi, Lingkup Security, Bentuk-bentuk ancaman dari sistem keamanan komputer, klasifikasi kejahatan komputer , konsep melakukan enkripsi, dekripsi dan proses pembangkitan kunci (*Key Generation*),Kriptanalisis, Kriptologi, Algoritma Kriptografi Klasik, Algoritma Kriptografi Modern, Kriptografi Modern berdasarkan Stream Cipher dan Block Cipher, pembangkitan kunci, proses enkripsi dan dekripsi pada algoritma Public Key (RSA, Diffie Hellman dan Knapsack), penggunaan Fungsi Hash (Penggunaan Hash satu arah, Skema Fungsi hash dan konsep bit pengganjal dalam Fungsi Hash, Digital Signature, Algoritma yang mengimplementasikan Fungsi Hash (MD5 dan SHA), dasar manajemen kunci dalam kriptografi, mekanisme Konsesus, smart Contract dan membangun Distributed Ledger sebagai dasar dalam teknologi blockchain berdasarkan contoh Penerapan Blockchain berupa Skenario Implementasi Blockchain pada Transaksi Keuangan mulai dari Pembentukan Node, Pembentukan Public dan Private Key, Pembuatan Pasangan Kunci, Pembentukan Blockchain dan teknik Hashing Data Transaksi.			
Metode Pembelajaran	1. Ceramah/Kuliah Pakar	✓	4. Praktik Laboratorium	.....
	2. Problem Based Learning/FGD	✓	5. Self-Learning (V-Class)	✓
	3. Project Based Learning	.....	6. Lainnya: Discovery Learning	✓
Pengalaman Belajar/Tugas	a. Tayangan Presentasi	✓	c. Online exercise/kuiz (V-class)	✓
	b. Review textbook/Jurnal	✓	d. Laporan	✓
	e. Lainnya:			

Referensi / Sumber Belajar	(1) Rinaldi Munir, ***Kriptografi Edisi Kedua***, Informatika Bandung, 2019 (2) Vinod Pachghare, ***Cryptography and Information Security Third Edition*** PHI Learning September 2019 (3) Mauro Conti, Jianying Zhou, Emiliano Casalicchio, Angelo Spognardi, Applied Cryptography and Network Security Part, Lecture Notes in Computer Science,Springer, 1st ed. 2020 (4) Dan Boneh and Victor Shoup, **A Graduate Course in Applied Cryptography**, Ebook 900 Pages Available on : https://toc.cryptobook.us/book.pdf, 2020 (5) George Bull, **Cryptography An Introductory Crash Course on the Science and Art of Coding and Decoding of Messages, Ciphers, Cryptograms and Encryption** (Kindle Edition), 2016 (6) Heru Susanto, Fahmi Ibrahim, Rodiah, Didi Rosiyadi, Desi Setiana, Alifya Kayla Shafa Susanto, Nicolas Kusuma, Iwan Setiawan ,**Securing Financial Inclusiveness Adoption of Blockchain FinTech Compliance (pages 168-196)**, IGI Global Publisher od Timeley Knowledge Book Chapter, 2021

Minggu	Kemampuan Akhir yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Metode/Bentuk Pembelajaran	Waktu Belajar (Menit)	Kriteria Penilaian (Indikator)	Bobot Nilai (%)	Sumber belajar
1	- Mengetahui dan memahami dasar-dasar dan konsep dari keamanan pada sistem informasi - Mengetahui dan memahami Konsep dasar Keamanan Informasi dan Pemahaman Serangan , Tipe-Tipe pengendalian, dan Prinsip-prinsip The *Five Trust Service* untuk keandalan system - Mengetahui Konsep Keamanan Sistem Informasi dan Lingkup *Security*, bentuk-bentuk ancaman dari sistem keamanan komputer, jenis ancaman cyber dan implementasi metode pengamanan komputer berdasarkan sistem yang tepat tergantung pada jenis ancamannya - Mengetahui klasifikasi kejahatan komputer baik yang bersifat fisik, yang berhubungan dengan personal, eamanan dari data dan media serta teknik *communications* dan keamanan dalam operasi	**Memahami dasar - dasar kemananan Sistem Informasi** 1) Konsep Keamanan Sistem Informasi 2) Karakteristik Informasi 3) Mengetahui Prinsip Sistem Keamanan (Privacy / Confidentiality,Integrity, Authentication, Availability, Access Control dan Non-repudiation **Masalah pada Keamanan Sistem** 1) Konsep Keamanan Sistem Informasi 2) Lingkup Security (Keamananan) Sistem Komputer ▪ Pengamanan Secara Fisik ▪ Pengamanan Akses ▪ Pengamanan Data ▪ Pengamanan Komunikasi Jaringan 3) Jenis Serangan Cyber ▪ SQL Injection ▪ Web Phishing ▪ Denial of Service (DoS) ▪ Man in The Middle Attack ▪ RansomWare 4) Metode pengamanan komputer berdasarkan sistem ▪ Network Topology ▪ Security Information Management ▪ IDS / IPS ▪ Packet Fingerprinting **Klasifikasi Kejahatan Komputer** 1) Keamanan yang bersifat fisik (*physical security*) 2) Keamanan yang berhubungan dengan orang (personal) 3) Keamanan dari data dan media serta teknik komunikasi (*communications*) 4) Keamanan dalam sistem operasi	- Ceramah - Discovery Learning - Aktivitas Mandiri (Melakukan pendalaman prinsip sistem keamanan dan implementasiny a dalam kehidupan sehari-hari)	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan - Di bawah standar	10%	1,2,3

Minggu	Kemampuan Akhir yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Metode/Bentuk Pembelajaran	Waktu Belajar (Menit)	Kriteria Penilaian (Indikator)	Bobot Nilai (%)	Sumber belajar
2	- Mengetahui dan Memahami Konsep dan Konsep dan Terminologi Kriptografi dan syarat-syarat dalam melakukan kriptografi dengan memahami konsep melakukan enkripsi, dekripsi dan proses pembangkitan kunci (*Key Generation*)Kriptanalisis dan Kriptologi - Mengetahui dan memahami Tujuan implementasi Kriptografi dan Jenis Kriptografi	**1). Pengantar Kriptografi** Definisi dan Terminologi ▪ Pesan, Plaintext dan Ciphertext ▪ Pengirim dan Penerma ▪ Enkripsi dan Dekripsi ▪ Cipher dan Kunci ▪ Sistem Kriptografi ▪ Penyadap ▪ Kriptanalisis dan Kriptologi **2) Tujuan Kriptografi** **3) Sejarah Kriptografi** **4) Jenis Kriptografi** ▪ Algoritma Kriptografi Klasik ▪ Algoritma Kriptografi Modern	- Ceramah - Discovery Learning - Aktivitas Mandiri (Melakukan pendalaman Konsep dan Konsep dan Terminologi Kriptografi dan konsep melakukan enkripsi)	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan - Di bawah standar	10%	1,2,3,4,5
3,4	- Mengetahui beberapa algoritma klasik berbasis alfabet dan angka - Memahami teknik dalam melakukan analisis frekuensi - Memahami penggunaan Affine Cipher, Vigenere Cipher dan Variasi dalam Vigenere Cipher, Playfair Cipher dan algoritma One Time Pad	**1) Algoritma Kriptografi Klasik** ▪ Cipher Subtitusi dan Jenis-jenis cipher subtitusi a) Cipher Alfabet Tunggal b) Cipher Alfabet Majemuk c) Cipher Subtitusi Homofonik d) Cipher Subtitusi Poligram ▪ Cipher Transposisi **2) Teknik Analisis Frekuensi** ▪ Kelemahan Cipher Subtitusi ▪ Cara melakukan teknik analisis frekuensi ▪ Metode Exhaustive Key Search **3) Affine Cipher** **4) Vigenere Cipher** ▪ Metode Kasiski untuk menentukan panjang kunci ▪ Variasi dalam Vigenere Cipher **5) Playfair Cipher** **6) One Time Pad**	- Ceramah - Discovery Learning - Aktivitas Mandiri (Melakukan pendalaman algoritma klasik berbasis alfabet dan angka dan teknik dalam melakukan analisis frekuensi	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan - Di bawah standar	10%	1,2,3,4,5
5,6	- Mengetahui beberapa algoritma modern dengan memahami penggunaan	**1) Algoritma Kriptografi Modern** ▪ Rangkaian bit dan operasinya ▪ Algoritma Enkripsi dengan XOR	- Ceramah - Discovery Learning - Aktivitas Mandiri (Melakukan	2,332x170 menit	Kuis Dimensi : Pemahaman	10%	1,2,3,4,5

Minggu	Kemampuan Akhir yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Metode/Bentuk Pembelajaran	Waktu Belajar (Menit)	Kriteria Penilaian (Indikator)	Bobot Nilai (%)	Sumber belajar
	algoritma paling sederhana XOR - Mengetahui dan dapat menjelaskan kategori kriptografi modern berdasarkan stream cipher dan block cipher. - Mengetahui prinsip penyandian shannon dan mode operasi pada cipher block. - Memahami dan mampu menjelaskan kelemahan mode operasi pada Cipher Block	Sederhana **2) Kategori Cipher kunci Simetri** ▪ Cipher Aliran ▪ Pembangkit Aliran Kunci ▪ Jenis-jenis Cipher Aliran **3) Serangan terhadap Cipher Aliran** ▪ Known Plain Attack ▪ Ciphertext Only Attack ▪ Flip Bit Attack **4) Cipher Block** ▪ Prinsip Penyandian Shannon ▪ Mode Operasi Cipher Block (ECB dan CBC) ▪ Kelemahan Mode CBC	algoritma kriptografi modern dengan kategori stream cipher dan block cipher)		Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan - Di bawah standar		
7	- Memahami perbedaan kunci public dan kunci private - Memahami dan dapat menjelaskan cara pembangkitan kunci, proses enkripsi dan dekripsi pada algoritma Public Key (RSA, Diffie Hellman dan Knapsack)	**Kriptografi Kunci Publik (Public Key)** ▪ Konsep Kriptografi Kunci Publik ▪ Perbandingan Kriptografi Kunci Simetri dan Asimetri ▪ Aplikasi Kriptografi Public Key 1) Algoritma RSA - Besaran pada Algoritma RSA - Pembangkitan Kunci RSA - Enkripsi dan Dekripsi dengan RSA 2) Algoritma Pertukaran Kunci Diffie-Hellman - Parameter Umum dalam Diffie Hellman 3) Algoritma Knapsack - Knapsack Problem - Superincreasing Knapsack - Implementasi Knapsack	- Ceramah - Discovery Learning - Aktivitas Mandiri (Melakukan algoritma kriptografi modern dengan kategori public key dan memahami beberapa algoritma public key (RSA, Diffie-Hellman dan Knapsack)	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Di bawah standar	10%	1,2,3,4,5
UJIAN TENGAH SEMESTER							
8,9	- Mampu menjelaskan dan memahami penggunaan Fungsi Hash (Penggunaan Hash satu arah, Skema Fungsi hash dan konsep bit pengganjal dalam Fungsi Hash) - Memahami beberapa algoritma yang mengimplentasikan Fungsi	**Fungsi HASH Kriptografi** **1) Definisi Dan Konsep Hash Value** **2) Konsep Message Digest** **3) Fungsi Hash Satu Arah** ▪ Sifat Fungsi Hash Satu Arah ▪ Skema Fungsi Hash ▪ Konsep Padding Bit **4) Implementasi Hash pada beberapa Algoritma** ▪ Algoritma MD5	- Ceramah - Discovery Learning - Aktivitas Mandiri (Memahami dan dapat menjelaskan penggunaan Fungsi dalam Kriptografi, konsep tanda tangan digital dan prosedur verifikasi keabsahan tanda	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi	10%	2,3,4,5

Minggu	Kemampuan Akhir yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Metode/Bentuk Pembelajaran	Waktu Belajar (Menit)	Kriteria Penilaian (Indikator)	Bobot Nilai (%)	Sumber belajar
	Hash (MD5 dan SHA) - Memahami konsep Digital Signature dengan Enkripsi pesan dan dapat menjelaskan prosedur untuk melakukan verfikasi keabsahan tanda tangan digital	▪ Algoritma SHA **Konsep Digital Signature** ▪ Penandatanganan dengan Enkripsi Pesan ▪ Konsep Tanda Tangan Digital ▪ Prosedur Verifikasi keabsahan Tanda Tangan Digital	tangan digital)		Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas Kurang memuaskan Di bawah standar		
10,11	- Memahami dan dapat menjelaskan tentang dasar dalam melakukan Manajemen Kunci Kriptografi mulai dari Pembangkitan Kunci, Penyebaran Kunci, Penggunaan Kunci, Perubahan Kunci dan Penghancuran Kunci (Key Destruction)	**Dasar Manajemen Kunci Kriptografi** **1) Pembangkitan Kunci (Key Generation)** ▪ Linier Congruential Generator (LCG) ▪ Pembangkit bilangan acak yang aman untuk kriptografi ▪ Blum Blum Shut ▪ CSPRNG berbasis RSA **2) Penyebaran Kunci** **3) Penggunaan Kunci** **4) Perubahan Kunci** **5) Penghancuran Kunci (Key Destruction)**	- Ceramah - Discovery Learning - Aktivitas Mandiri (Mengetahui dan dapat menjelaskan dasar manajemen kunci dalam kriptografi)	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Di bawah standar	10%	2,3,4,5
12,13,14, 15	- Memahami impelementasi Kriptografi dalam Blockchain dengan memahami Dasar dalam membangun Teknologi Blockchain - Mengetahui Komponen Blockchain dan Cara Kerja Blockchain, cara mendeskripsikan Distibuted Ledger / Database - Mengetahui cara melakukan Autentikasi dan Verifikasi dengan Kriptografi pada teknologi blockchain - Memahami mekanisme	**Kriptografi dalam Blockchain** **1) Konsep Dasar Teknologi Blockchain** **2) Pemanfaatan Blockchain dalam Industri 4.0** **3) Komponen Blockchain** **4) Cara Kerja Blockchain** **5) Komponen Utama Blockchain** ▪ Distibuted Ledger / Database ▪ Autentikasi dan Verifikasi dengan Kriptogrfi ▪ Mekanisme Konsesus ▪ Smart Contract **6) Contoh Penerapan Blockchain** ▪ Skenario Implementasi Blockchain pada Transaksi Keuangan ▪ Pembentukan Node	- Ceramah - Discovery Learning - Aktivitas Mandiri (Mampu memahami penggunaan kriptografi dalam penerapan Teknologi Blockchain sebagai Trend Teknologi di Industri 4.0)	2,332x170 menit	Kuis Dimensi : Pemahaman Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Laporan dan Komunikasi Dimensi : Kelengkapan laporan dan Kebenaran laporan Penilaian kompetensinya : - Sangat memuaskan - Memuaskan - Batas - Kurang memuaskan Di	20%	4,5,6

Minggu	Kemampuan Akhir yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Metode/Bentuk Pembelajaran	Waktu Belajar (Menit)	Kriteria Penilaian (Indikator)	Bobot Nilai (%)	Sumber belajar
	Konsesus, smart Contract - Memahami teknologi blockchain berdasarkan contoh Penerapan Blockchain berupa Skenario Implementasi Blockchain pada Transaksi Keuangan mulai dari Pembentukan Node, Pembentukan Public dan Private Key, Pembuatan Pasangan Kunci, Pembentukan Blockchain dan teknik Hashing Data Transaksi.	▪ Pembentukan Public dan Private Key ▪ Pembuatan Pasangan Kunci ▪ Pembentukan Blockchain ▪ Hashing Data Transaksi			bawah standar		

FORMAT RANCANGAN TUGAS 1

Nama Mata Kuliah : Sistem Keamanan dan Kriptografi **SKS : 2**
Program Studi : Magister Manajemen Sistem Informasi **Pertemuan ke: 2**
Fakultas : Direktorat Magister Teknologi dan Rekayasa

A. TUJUAN TUGAS :

Mahasiswa mampu memahami dan menelaah Kasus pada Desain sistem biometrik

B. URAIAN TUGAS :

a. Obyek Garapan
Contoh kasus-kasus keamanan pada sistem informasi, Jenis Serangan (SQL Injection/Phishing/DoS/Man In The Middle Attack, Ransomware) , Tipe-Tipe pengendalian berdasarkan prinsip The Five Trust Service dan cara penanganan berkaitan dengan kriptografi

b. Metode atau Cara pengerjaan
- Carilah referensi berupa jurnal / artikel ilmiah, dan artikel populer di web atau di textbook kriptografi
- Rangkumlah referensi tersebut
- Rangkuman dibuat dalam bentuk paper minimal 10 halaman

c. Deskripsi Luaran tugas yang dihasilkan :
Paper minimal 10 halaman dengan spasi 1.5 dan font Times New Roman ukuran 12

C. KRITERIA PENILAIAN (5 %)

Kelengkapan isi rangkuman
Kebenaran isi rangkuman
Daya tarik komunikasi tulisan

FORMAT RANCANGAN TUGAS 2

Nama Mata Kuliah : Sistem Keamanan dan Kriptografi **SKS : 2**
Program Studi : Magister Manajemen Sistem Informasi **Pertemuan ke: 5**
Fakultas : Direktorat Magister Teknologi dan Rekayasa

B. TUJUAN TUGAS :

Mahasiswa mampu menjelaskan salah satu algoritma kriptografi modern (block cipher/stream cipher)

B. URAIAN TUGAS :

a. Obyek Garapan
   Mencari satu jurnal internasional yang menjelaskan satu implementasi algoritma kriptografi modern (boleh menggunakan algoritma berbasis block cipher/stream cipher) proses enkripsi, dekripsi, cipher, ciphertext, dan dasar pembangkitan kuncinya

b. Metode atau Cara pengerjaan
   - Carilah referensi kasus berupa jurnal / artikel ilmiah atau artikel how-to di internet
   - Rangkumlah referensi tersebut

c. Deskripsi Luaran tugas yang dihasilkan :
   Deskripsi Review Jurnal 3-4 halaman dengan spasi 1.5 dan font Times New Roman ukuran 12

C. KRITERIA PENILAIAN (8 %)

Kelengkapan isi rangkuman
Kebenaran isi rangkuman
Daya tarik komunikasi/presentasi

FORMAT RANCANGAN TUGAS 3

Nama Mata Kuliah : Sistem Keamanan dan Kriptografi **SKS : 2**
Program Studi : Magister Manajemen Sistem Informasi **Pertemuan ke: 8**
Fakultas : Direktorat Magister Teknologi dan Rekayasa

C. TUJUAN TUGAS :

Mahasiswa mampu mengimplementasikan penggunaan algoritma kriptografi (public/private key) dalam Teknologi Blockchain

B. URAIAN TUGAS :

a. Obyek Garapan
   Implementasi salah satu algoritma kriptografi dalam pembentukan private/public key pada Teknologi Blockchain
b. Metode atau Cara pengerjaan
   - Carilah referensi kasus berupa jurnal / artikel ilmiah atau artikel how-to di internet
   - Rangkumlah referensi tersebut
   - Rangkuman dibuat dalam bentuk paper minimal 10 halaman
c. Deskripsi Luaran tugas yang dihasilkan :
   Paper minimal 10 halaman dengan spasi 1.5 dan font Times New Roman ukuran 12

C. KRITERIA PENILAIAN (8 %)

Kelengkapan isi rangkuman
Kebenaran isi rangkuman
Daya tarik komunikasi/presentasi

GRADING SCHEME COMPETENCE

KRITERIA 1 : Kelengkapan isi rangkuman

DIMENSI	Sangat Memuaskan	Memuaskan	Batas	Kurang Memuaskan	Di bawah standard	SKOR
Kelengkapan konsep	Lengkap dan terpadu	Lengkap	Masih kurang beberapa aspek yang be lum terungkap	Hanya menunjukkan sebagian konsep saja	Tidak ada konsep	2

KRITERIA 2 : Kebenaran isi rangkuman

DIMENSI	Sangat Memuaskan	Memuaskan	Batas	Kurang Memuaskan	Di bawah standard	SKOR
Kebenaran konsep	Diungkapkan dengan tepat, terdapat aspek penting, analisis dan membantu memahami konsep	Diungkap dengan tepat tetapi deskriptif	Sebagian besar konsep sudah terungkap, namun masih ada yang terlewatkan	Kurang dapat mengungkapkan aspek penting, melebihi halaman, tidak ada proses merangkum hanya mencontoh	Tidak ada konsep yang disajikan	2

KRITERIA 3 : Daya tarik komunikasi/presentasi

KRITERIA 3a : Komunikasi tertulis

DIMENSI	Sangat Memuaskan	Memuaskan	Batas	Kurang Memuaskan	Di bawah standard	SKOR
Bahasa Paper	Bahasa menggugah pembaca untuk mencari tahu konsep lebih dalam	Bahasa menambah informasi pembaca	Bahasa deskriptif, tidak terlalu menambah pengetahuan	Informasi dan data yang disampaikan tidak menarik dan membingungkan	Tidak ada hasil	1
Kerapian Paper	Paper dibuat dengan sangat menarik dan menggugah semangat membaca	Paper cukup menarik, walau tidak terlalu mengundang	Dijilid biasa	Dijilid namun kurang rapi	Tidak ada hasil	1

KRITERIA 3b : Komunikasi lisan

DIMENSI	Sangat Memuaskan	Memuaskan	Batas	Kurang Memuaskan	Di bawah standard	SKOR

Isi	Memberi inspirasi pendengar untuk mencari lebih dalam	Menambah wawasan	Pembaca masih harus menambah lagi informasi dari beberapa sumber	Informasi yang disampaikan tidak menambah wawasan bagi pendengarnya	Informasi yang disampaikan menyesatkan atau salah	2
Organisasi	Sangat runtut dan integratif sehingga pendengar dapat mengkompilasi isi dengan baik	Cukup runtut dan memberi data pendukung fakta yang disampaikan	Tidak didukung data, namun menyampaikan informasi yang benar	Informasi yang disampaikan tidak ada dasarnya	Tidak mau presentasi	1
Gaya Presentasi	Menggugah semangat pendengar	Membuat pendengar paham, hanya sesekali saja memandang catatan	Lebih banyak membaca catatan	Selalu membaca catatan (tergantung pada catatan)	Tidak berbunyi	1