RENCANA PEMBELAJARAN SEMESTER

PROGRAM STUDI S2 SAINS DATA

FAKULTAS SAINS DAN MATEMATIKA
Universitas Kristen Satya Wacana

Form						
Semester	Ganjil 2026/2027					
Mata Kuliah	BD031 CRYPTO & SECURITY INTELLIGENCE					
Beban	3	SKS	T/A/P:	1/2/0	W/P:	Pilihan
Dosen Pengampu	1. Prof. Dr. Adi Setiawan, M.Sc. (Koordinator) 2. Dr. Bambang Susanto 3. Prof. Didit Budi Nugroho, S.Si., M.Si., D.Sc. 4. Dr. Irwan Sembiring (FTI)					

A. Program Learning Outcome / Capaian Pembelajaran Lulusan (CPL)	
CPL01	Mampu menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri.
CPL02	Menguasai konsep teoretis bidang pengetahuan dan keterampilan tertentu secara umum dan khusus untuk menyelesaikan masalah secara prosedural sesuai dengan lingkup pekerjaannya
CPL03	Mampu menganalisis kebutuhan perangkat lunak untuk menghasilkan spesifikasi yang tepat.
CPL04	Mampu merancang perangkat lunak yang sesuai dengan spesifikasi dan kebutuhan pengguna.
CPL05	Mampu mengimplementasikan perangkat lunak berdasarkan spesifikasi yang telah dirancang.
CPL06	Mampu berkomunikasi secara efektif, baik lisan maupun tulisan, dalam konteks profesional.
CPL07	Mampu bekerjasama dalam tim serta menunjukkan kemampuan kepemimpinan dalam konteks kerja kelompok.
CPL08	Mampu mengintegrasikan prinsip etika dan tanggung jawab sosial dalam pengambilan keputusan profesional.

B. Course Learning Outcome / Capaian Pembelajaran Mata Kuliah (CPMK)	
CPMKBD03111	(CPL01) Mampu menunjukkan sikap bertanggung jawab dalam memahami prinsip dasar kriptografi dan keamanan data serta penerapannya secara mandiri dalam kegiatan pembelajaran dan tugas akademik.
CPMKBD03122	(CPL02) Menguasai konsep teoretis kriptografi dan keamanan data untuk penerapan intelligence secara sistematis.
CPMKBD03133	(CPL03) Mampu menganalisis kebutuhan keamanan data dan sistem informasi untuk merumuskan spesifikasi solusi crypto dan security intelligence yang tepat sesuai konteks permasalahan.

CPMKBD03144	(CPL04) Mampu merancang sistem crypto dan security intelligence yang sesuai dengan spesifikasi kebutuhan keamanan, kerahasiaan, dan integritas data pengguna.

C. Prerequisite/Corequisite Courses /Prasyarat Mata Kuliah	
Code	Course Name

D. Description/Deskripsi

This course introduces cryptographic concepts and their application in cyber security, covering: computer and network security concepts, mathematical foundations for cryptography (number theory, group/ring/field/Galois field theory), classical and modern encryption techniques (block ciphers, DES, AES), asymmetric ciphers and RSA, cryptographic hash functions and data integrity algorithms, and network and internet security.

Mata kuliah ini membahas konsep kriptografi dan penerapannya dalam keamanan siber, meliputi: konsep keamanan komputer dan jaringan, dasar matematika untuk kriptografi (teori bilangan, teori grup/ring/field/Galois field), teknik enkripsi klasik dan modern (block cipher, DES, AES), cipher asimetris dan RSA, algoritma fungsi hash kriptografis dan integritas data, serta keamanan jaringan dan internet.

E. Learning Stage/Tahap Pembelajaran

Week	Final Ability	Material	Methods	Duration	Indicators	Assesment
1	*Have extensive knowledge of computer and network security concepts.* Memiliki pengetahuan luas tentang konsep keamanan komputer dan jaringan.	Computer & Network Security Concepts	Presentation Discussion Demonstration Practicum	150'	Provides information about computer and network security concepts; Discussion	Discussion
2	*Master the mathematical foundations of cryptography: Number Theory.* Menguasai dasar matematika kriptografi: Teori Bilangan.	Number Theory for Cryptography	Presentation Discussion Demonstration Practicum	150'	Obtain information about Number Theory and its use in cryptography; Discussion and Practicum	Discussion
3	*Master the mathematical foundations of cryptography: Group Theory and Ring Theory.* Menguasai dasar matematika kriptografi: Teori Grup dan Teori Ring.	Group Theory & Ring Theory for Cryptography	Presentation Discussion Demonstration Practicum	150'	Obtain information about Group Theory and Ring Theory and their use in cryptography; Discussion and Practicum	Discussion

4	*Master the mathematical foundations of cryptography: Field Theory and Galois Theory.* Menguasai dasar matematika kriptografi: Teori Field dan Teori Galois.	Field Theory & Galois Theory for Cryptography	Presentation Discussion Demonstration Practicum	150'	Obtain information about Field Theory and Galois Theory and their use in cryptography; Discussion and Practicum	Task: Submit a practicum report.
5	*Master practical work related to the mathematical foundations used in cryptography.* Menguasai praktikum terkait dasar matematika yang digunakan dalam kriptografi.	Practicum/Case Study related to Meeting 1-4	Presentation Discussion Demonstration Practicum	150'	Carrying out practicum and tutorials related to Meeting 1 to Meeting 4	Practical Assignment /Report - CPMK2 (10%)
6	*Master Classical Encryption Techniques and Block Cipher/the Data Encryption Standard (DES).* Menguasai Teknik Enkripsi Klasik dan Block Cipher/Data Encryption Standard (DES).	Classical Encryption Techniques; Block Cipher & DES	Presentation Discussion Demonstration Practicum	150'	Obtain information about classical encryption techniques and DES; Discussion and Practicum	Discussion
7	*Master the Advanced Encryption Standard (AES).* Menguasai Advanced Encryption Standard (AES).	Advanced Encryption Standard (AES)	Presentation Discussion Demonstration Practicum	150'	Obtain information about AES; Discussion and Practicum	Discussion
8	*Master Public-Key Cryptography and RSA, other public-key cryptosystems, and Cryptographic Hash Functions.* Menguasai Kriptografi Kunci-Publik dan RSA, sistem kriptografi kunci-publik lainnya, dan Fungsi Hash Kriptografis.	Public-Key Cryptography & RSA; Cryptographic Hash Functions	Presentation Discussion Demonstration Practicum	150'	Obtain information about public-key cryptography, RSA, and hash functions; Discussion and Practicum	Task: Submit a practicum report.
9	*Master practical work related to the algorithms used in cryptography: DES, AES, and RSA.* Menguasai praktikum terkait algoritma yang digunakan dalam kriptografi: DES, AES, dan RSA.	Practicum/Case Study related to Meeting 6-8	Presentation Discussion Demonstration Practicum	150'	Carrying out practicum and tutorials related to Meeting 6 to Meeting 8	Practical Assignment /Report - CPMK2 (10%)
10	*Have extensive knowledge of network security fundamentals and protocols.* Memiliki pengetahuan luas tentang dasar-dasar dan protokol keamanan jaringan.	Network Security Fundamentals & Protocols	Presentation Discussion Demonstration Practicum	150'	Obtain information about network security fundamentals and protocols; Discussion and Practicum	Discussion

11	*Master requirement analysis for secure internet-based systems.* Menguasai analisis kebutuhan untuk sistem berbasis internet yang aman.	Internet Security: Requirement Analysis for Secure Systems	Presentation Discussion Demonstration Practicum	150'	Obtain information about internet security requirement analysis; Discussion and Practicum	Practical Assignment /Report - CPMK3 (15%)
12	*Master cryptographic data integrity algorithms and digital signatures.* Menguasai algoritma integritas data kriptografis dan tanda tangan digital.	Cryptographic Data Integrity Algorithms & Digital Signatures	Presentation Discussion Demonstration Practicum	150'	Obtain information about data integrity algorithms and digital signatures; Discussion and Practicum	Discussion
13	*Master the design of secure network and internet systems.* Menguasai perancangan sistem keamanan jaringan dan internet.	Network & Internet Security: Design of Secure Systems	Presentation Discussion Demonstration Practicum	150'	Obtain information about the design of secure network and internet systems; Discussion and Practicum	Discussion
14	*Master practical work related to network and internet security.* Menguasai praktikum terkait keamanan jaringan dan internet.	Practicum/Case Study related to Meeting 10-13	Presentation Discussion Demonstration Practicum	150'	Carrying out practicum and tutorials related to Meeting 10 to Meeting 13	Practical Assignment /Report - CPMK4 (15%)
15	*Able to design and build an applied crypto and security intelligence system.* Mampu merancang dan membangun sistem crypto and security intelligence secara terapan.	PROJECT WORK	Project Work	150'	Design and build a crypto and security intelligence project	Final Project Work - CPMK4 (35%)
16	*Able to present and defend the crypto and security intelligence project.* Mampu mempresentasikan dan mempertanggungjawabkan proyek crypto and security intelligence.	PROJECT PRESENTATION	Presentation Discussion	150'	Presenting the crypto and security intelligence project	Project Presentation - CPMK1 (15%)

Note/Catatan untuk Tabel E.

Abbreviation	Description
CPL	Capaian Pembelajaran Lulusan / Program Learning Outcome
CPMK	Capaian Pembelajaran Mata Kuliah / Course Learning Outcome
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest-Shamir-Adleman (public-key cryptosystem)

F. Learning Media and Tools
R/RStudio/Python Program Package, Computer, Flearn (Online Learning Media), WAG and Google Meet/Zoom.

G. Student Learning Experience/Portfolio
Students gain experience in performing encryption and decryption, developing more efficient cryptographic algorithms, and addressing problems in network and internet security. Mahasiswa memperoleh pengalaman dalam melakukan enkripsi dan dekripsi, mengembangkan algoritma kriptografi yang lebih efisien, serta mengatasi permasalahan keamanan jaringan dan internet.

H. References
1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed., Global Edition). Pearson.
2. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.
3. Karim, A., & Simarmata, J. (Eds.). (2022). Kriptografi: Teknik Keamanan Data. Yayasan Kita Menulis.
4. Munir, R. (2019). Kriptografi (Edisi 2). Penerbit Informatika Bandung.
5. Paar, C., & Pelzl, J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

I. Authorization

Pengembang	Tanggal	Koordinator	Kaprodi
Prof. Dr. Adi Setiawan, M.Sc.	8 Agustus 2026		Prof. Hanna Arini Parhusip, M.Sc.nat