INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS)
FAKULTAS TEKNOLOGI ELEKTRO DAN INFORMATIKA CERDAS
DEPARTEMEN TEKNIK ELEKTRO
Program Studi Sarjana (S1) Teknik Telekomunikasi

INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS)
FACULTY OF INTELLIGENT ELECTRICAL & INFORMATICS TECHNOLOGY
DEPARTMENT OF ELECTRICAL ENGINEERING
Bachelor Degree Program in Telecommunication Engineering

1	**Nama Mata Kuliah / *Course Name***	:	Sekuriti dan Kriptografi / *Security and Cryptography*
2	**Kode Mata Kuliah / *Course Code***	:	EL234707
3	**Kredit / *Credits***	:	3 SKS
4	**Semester / *Semester***	:	Pilihan

Deskripsi Mata Kuliah / *Course Description*

Dengan semakin pesatnya perkembangan jaringan komunikasi dan internet dan semakin luasnya penggunaan perangkat serta data yang terhubung ke jaringan, tantangan terhadap keamanan informasi dan jaringan semakin penting, terutama untuk melindungi dari ancaman dari berbagai macam serangan. Ancaman dan serangan terhadap keamanan sistem dan jaringan komunikasi semakin meningkat, dengan dampak dan kerugian yang sangat besar. Salah satu alat utama untuk memberikan layanan keamanan adalah teknik kriptografi. Pada kuliah ini akan dipelajari berbagai teknik kriptografi, mulai dari prinsip, kriptografi klasik, kriptografi simetrik dan kriptografi publik atau asimetrik. Selain itu juga dipelajari dasar-dasar teori bilangan, finite field, persamaan kurva elliptic, dan fungsi hash. Mahasiswa juga akan mempelajari penerapan metode-metode kriptografi yang dipelajari dengan mengimplementasikannya pada pemrograman python./ *With the rapid development of communication networks and the Internet and the widespread use of devices and data connected to the network, challenges to information and network security are increasingly important, especially to protect against threats from various kinds of attacks. Threats and attacks on the security of communication systems and networks are increasing, with huge impacts and losses. One of the main tools to provide security services is cryptographic techniques. In this lecture, we will learn various cryptographic techniques, ranging from principles, classical cryptography, symmetric cryptography and public or asymmetric cryptography. Students will also learn the basics of number theory, finite field, elliptic curve equation, and hash function. Students will also learn the application of the cryptography methods learned by implementing them in python programming.*

Capaian Pembelajaran Lulusan (CPL) Yang Dibebankan Mata Kuliah / *Program Learning Outcomes Charged to The Course*

1. (CPL-01) Mampu menunjukkan sikap dan karakter yang mencerminkan: ketakwaan kepada Tuhan Yang Maha Esa, etika dan integritas, berbudi pekerti luhur, peka dan peduli terhadap masalah sosial dan lingkungan, menghargai perbedaan budaya dan kemajemukan, menjunjung tinggi penegakan hukum, mendahulukan kepentingan bangsa dan masyarakat luas, melalui kreatifitas dan inovasi, ekselensi, kepemimpinan yang kuat, sinergi, dan potensi lain yang dimiliki untuk mencapai hasil yang maksimal. / *Able to demonstrate attitudes and characters that reflect: devotion to God Almighty, ethics and integrity, noble character, sensitive and concerned about social and environmental problems, respect for cultural differences and pluralism, uphold law enforcement, prioritize the interests of the nation and the wider community, through creativity and innovation, excellence, strong leadership, synergy, and other potentials to achieve maximum results.*
2. (CPL-04) Mampu menerapkan ilmu pengetahuan alam dan matematika serta teknologi dan rekayasa informasi untuk memperoleh pemahaman komprehensif pada bidang Teknik Telekomunikasi. / *Able to apply natural and mathematical sciences as well as technology and information engineering to obtain a comprehensive understanding of the field of Telecommunication Engineering.*
3. (CPL-08) Mampu mengetahui dan mengaplikasi metode dan keahlian sesuai perkembangan terkini di bidang ilmu pengetahuan dan teknologi untuk menyelesaikan permasalahan di bidang Teknik Telekomunikasi dengan mengedepankan nilai-nilai universal. / *Able to know and apply methods and expertise according to the latest developments in the field of science and technology to solve problems in the field of Telecommunication Engineering by prioritizing universal values.*

Capaian Pembelajaran Mata Kuliah / *Course Learning Outcomes*

1. Mampu menjelaskan konsep dan prinsip keamanan informasi, teknik-teknik kriptografi klasik
2. Mampu menghitung algoritma Euclidean, bilangan prima, aritmatika modular, Teorema Fermat dan Euler, Chinese Remainder Theorem, finite field, aritmatika polinomial, Galois field
3. Mampu menghitung kriptografi kunci publik, untuk tujuan kerahasiaan, pembangkitan kunci bersama, dan digital signature
4. Mampu menjelaskan aplikasi kriptografi kunci pribadi dan kunci publik pada berbagai kebutuhan keamanan, antara lain: otentikasi, digital signature, keamanan jaringan
5. Mampu mengimplementasikan berbagai algoritma kriptografi dengan menggunakan bahasa python dan Matlab

1. Able to explain the concepts and principles of information security, classical cryptography techniques
2. Able to calculate Euclidean algorithm, prime numbers, modular arithmetic, Fermat and Euler's Theorem, Chinese Remainder Theorem, finite field, polynomial arithmetic, Galois field
3. Able to calculate public key cryptography, for the purpose of confidentiality, shared key generation, and digital signature
4. Able to explain the application of private key and public key cryptography to various security needs, including: authentication, digital signature, and network security.

Able to implement various cryptographic algorithms using python and Matlab languages

Pokok Bahasan / *Contents*

1. Pengantar keamanan sistem komunikasi dan komputer
2. Teknik-teknik Enkripsi Klasik
3. Block Cipher dan DES
4. Teori Bilangan Bulat
5. Finite Field
6. Algoritma AES
7. Operasi Block Cipher
8. Kriptograpfi Kunci Publik dan RSA
9. Fungsi Hash
10. Message Authentication Codes
11. Digital Signatures
12. Keamanan Jaringan Nirkabel
13. Teknologi Blockchain

1. *Introduction to communication and computer system security*
2. *Classic Encryption Techniques*
3. *Block Cipher and DES*
4. *Integer Theory*
5. *Finite Field*
6. *AES Algorithm*

7. *Block Cipher Operation*
8. *Public Key Cryptography and RSA*
9. *Hash Function*
10. *Message Authentication Codes*
11. *Digital Signatures*
12. *Wireless Network Security*
13. *Blockchain Technology*

Prasyarat / *Pre-requisite*

Aljabar Linier dan Variabel Kompleks / *Linear Algebra and Complex Variables*, Probabilitas dan Statistik */ Probability and Statistics*

Pustaka / *Reference*

1. William Stallings, "Network Security and Cryptography: Principles and Practice," 8th Edition, Pearson, 2023.
2. Shannon W. Bray, "Implementing Cryptography Using Python," Wiley, 2020.
3. Marius Iulian Mihailescu & Stefania Loredana Nita, "Cryptography and Cryptanalysis in Matlab: Creating and Programming Advanced Algorithms," Apress Media, 2021.
4. Kristian Gjøsteen, "Practical Mathematical Cryptography," CRC Press, 2022.