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

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

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 increasing use of devices and data connected to networks, the challenge of information and network security is becoming more important, especially to protect against threats from various types of attacks. Threats and attacks on the security of communication systems and networks are increasing, with significant impact and losses. One of the main tools for providing security services is cryptography techniques. This course will cover various cryptography techniques, ranging from principles, classical cryptography, symmetric cryptography, and public or asymmetric cryptography. In addition, the basics of number theory, finite fields, elliptic curve equations, and hash functions will also be studied. Students will also learn to implement the cryptography methods studied 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
(PLO-01) Be able to demonstrate attitudes and characters that reflect: being pious to God Almighty, having ethics and integrity, virtuous character, sensitive and concerned with social and environmental issues, respecting cultural differences and pluralism, upholding law enforcement, prioritizing the interests of the nation and the wider community, through creativity and innovation, excellence, strong leadership, synergy, and other potentia.ls 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
(PLO-04) Able to apply knowledge of sciences, mathematics, and information technology to acquire comprehensive understanding of engineering principles in 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
(PLO-08) Able to know and apply methods, skills according to the latest developments in the field of science and technology to solve electrical engineering problems by prioritizing universal values

Capaian Pembelajaran Mata Kuliah / Course Learning Outcomes

1. Mampu menjelaskan konsep dan prinsip keamanan informasi, teknik-teknik kriptografi klasik / *Able to explain the concepts and principles of information security, classical cryptography techniques.*
2. Mampu menghitung algoritma Euclidean, bilangan prima, aritmatika modular, Teorema Fermat dan Euler, Chinese Remainder Theorem, finite field, aritmatika polinomial, Galois field / *Able to calculate Euclidean algorithm, prime numbers, modular arithmetic, Fermat and Euler's theorem, Chinese Remainder Theorem, finite field, polynomial arithmetic, Galois field.*
3. Mampu menghitung kriptografi kunci publik, untuk tujuan kerahasiaan, pembangkitan kunci bersama, dan digital signature/ *Able to calculate public key cryptography, for confidentiality, key generation, and digital signatures.*
4. Mampu menjelaskan aplikasi kriptografi kunci pribadi dan kunci publik pada berbagai kebutuhan keamanan, antara lain: otentikasi, digital signature, keamanan jaringan / *Able to explain the applications of private key and public key cryptography in various security needs, including authentication, digital signatures, network security.*
5. Mampu mengimplementasikan berbagai algoritma kriptografi dengan menggunakan bahasa python dan Matlab / *Able to implement various cryptography algorithms using Python and Matlab programming language.*

Pokok Bahasan / Contents

1. Pengantar keamanan sistem komunikasi dan komputer / *Introduction to communication and computer system security*
2. Teknik-teknik Enkripsi Klasik / *Classic Encryption Techniques*
3. Block Cipher dan DES / *Block Ciphers and DES*
4. Teori Bilangan Bulat / *Integer Number Theory*
5. Finite Field / *Finite Fields*
6. Algoritma AES / *AES Algorithm*
7. Operasi Block Cipher / *Block Cipher Operations*
8. Kriptograpfi Kunci Publik dan RSA / *Public Key Cryptography and RSA*
9. Fungsi Hash / *Hash Functions*
10. Message Authentication Codes / *Message Authentication Codes*
11. Digital Signatures / *Digital Signatures*
12. Keamanan Jaringan Nirkabel / *Wireless Network Security*
13. Teknologi Blockchain / *Blockchain Technology*

Prasyarat / Pre-requisite

Aljabar Linier dan Variabel Kompleks, Dasar Pemrograman / *Linear Algebra and Complex Variables , Algorithms and Programming*

Pustaka / Reference

Utama / Primary :

1. William Stallings, "Network Security and Cryptography: Principles and Practice," 8th Edition, Pearson, 2023.
2. Shannon W. Bray, "Implementing Cryptography Using Python," Wiley, 2020.

Pendukung / Support :

1. Marius Iulian Mihailescu & Stefania Loredana Nita, "Cryptography and Cryptanalysis in Matlab: Creating and Programming Advanced Algorithms," Apress Media, 2021.
2. Kristian Gjøsteen, "Practical Mathematical Cryptography," CRC Press, 2022.