Department of Mathematics
Institut Teknologi Sepuluh Nopember
email : matematika@its.ac.id – web : https://www.its.ac.id/matematika

Course	**Course Name**	**: Cryptography**
	Course Code	**: KM184830**
	Credit	**: 2**
	Semester	**: 8**

Description of Course	
Cryptography is a course that provides the basics of cryptography and digital signatures for data security. The topics include the fundamentals of mathematics, classical and modern cryptographic algorithms, criteria techniques and applications of cryptography. The teaching system includes tutorials, responses and scheduled workshops.	
Learning Outcome	
PLO 3	[C4] Students are able to analyze simple and practical problems in at least one field of analysis, algebra, modeling, system optimizations and computing sciences
PLO 4	[C5] Students are able to work on a simple and clearly defined scientific task and explain the results, both written and verbally either on the area of pure mathematics or applied mathematics or computing sciences
PLO 7	Students are able to demonstrate an attitude of responsibility and commitment to law enforcement, ethics, norms for community and environmental sustainability
Course Learning Outcome	
The students are able to develop the concepts and procedures of computer security techniques, particularly data and information security, individually and togetherly.	

Main Subject
1. INTRODUCTION OF CRYPTOGRAPHY: basic introduction of cryptography, security data, information theory, complexity and number 2. SOME ENCRYPTIONAL ALGORITHM: classical and modern encryption algorithms (DES and public key algorithms) 3. CRYPTOGRAPHIC TECHNIQUES: some cryptographic techniques, key management
Prerequisites
Discrete Mathematics
Reference
1. William.Stallings, Cryptography and Network Security, Principle and Practise. 2nd ed., Prentice Hall, 1999 2. Douglas R. Stinson, "Cryptography Theory and Practice", 3rd Edition, Chapman & Hall/CRC, 2006
Supporting Reference
1. Serge Vaudenay, "A Classical Introduction to Modern Cryptography', Springer, 2006 2. Rinaldi Munir "Kriptografi", Informatika Bandung