Module Description

Module name	Cryptography
Module level, if applicable	Bachelor of Informatics
Code, if applicable	21D12141803
Subtitle, if applicable	-
Course, if applicable	
Semester(s) in which the module is taught	6th or 7th
Person responsible for the module	Dr. Eng. Ady Wahyudi Paundu
Lecturer	1. Dr. Eng Ady Wahyudi Paundu 2. Dr. Adnan
Language	Indonesian Language [Bahasa Indonesia]
Relation to Curriculum	This course is an elective course and offered in the 6th or 7th semester.
Type of teaching, contact hours	Teaching methods: [case study], [collaborative learning]. Teaching forms: [lecture], [tutorial], [practicum]. CH : 8.00 - 16.00
Workload	For this course, students are required to meet a minimum of 136.00 hours in one semester, which consist of: - 40.00 hours for lecture, - 48.00 hours for structured assignments, - 48.00 hours for private study
Credit points	3 credit points (equivalent with 5.1 ECTS)
Requirements	Students have participated in at least 80% of the learning activities

according to the examination regulations	(Academic Regulations, Chapter VII)
Recommended prerequisites	-
Module objectives/intended learning outcomes	**Intended Learning Outcomes (ILO):** **ILO 1 :** Have the knowledge of fundamental in Computing Science that includes basic theory and concepts of computer science, Mathematics and Statistics, Programming Algorithm, Software Engineering, Information Management and Digital Resilience, also the advance topics of either Artificial Intelligence, Data Science, Computer Network, Cloud Computing or Internet of Things. **ILO 3 :** Apply the knowledge of computing and other related disciplines to analyse and identify solutions for any computing-based problem. **Course Learning Objective (CLO):** After attending the Cryptography course, students have a basic knowledge of Cryptology, either in Cryptography or in Cryptanalysis and basic skills to implement their knowledge to solve problems in their professional course. **Sub CLO :** ILO1=>CLO1: Students are able to understand basic cryptography and cryptanalysis concepts, including the history from the earlier traditional cipher, modular arithmetic. ILO3=>CLO2: Students have the knowledge of how symmetric cipher works, and able to design a simple symmetric cipher ILO3=>CLO3: Students have the knowledge of how asymmetric cipher works, and able to design a simple asymmetric cipher
Content	Students will learn about : 1) Taxonomy of Cryptology 2) Traditional Cipher

<table>
<tr><td></td><td>
3) Modular Arithmetic
4) Stream Cipher: Linear Feedback Shift Registers
5) Data Encryption Standard
6) Advanced Encryption Standard
7) Basics of Galois Field
8) Euclidian Algorithms
9) Euler Phi Function
10) Fermat Little theorem
11) Euler's Theorem
12) RSA Cryptosystem
13) Diffie-Hellman Key Exchange
14) El Gamal Encryption
15) Elliptic Curve Cryptosystems
16) Digital Signature
17) Hash Functions
18) Message Authentication Codes
</td></tr>
<tr><td>Forms of Assessment</td><td>
Assessment techniques: [observation], [participation], [written test].

Assessment forms: [final term exam], [assignment].

<table>
<tr><td>CLO 1</td><td colspan="2">CLO 2</td><td colspan="2">CLO 3</td></tr>
<tr><td>Exam 1</td><td>Exam 2</td><td>Assign 1</td><td>Exam 3</td><td>Assign 2</td></tr>
<tr><td>20</td><td>20</td><td>20</td><td>20</td><td>20</td></tr>
</table>
</td></tr>
<tr><td>Study and examination requirements and forms of examination</td><td>
Study and examination requirements:
- Students must attend 15 minutes before the class starts.
- Students must switch off all electronic devices.
- Students must inform the lecturer if they will not attend the class due to sickness, etc.
- Students must submit all class assignments before the deadline.
- Students must attend the exam to get the final grade.
Form of examination:
Written exam and assignments
</td></tr>
<tr><td>Media employed</td><td>Video conference, slide presentation, Learning Management System (LMS)</td></tr>
<tr><td>Reading list</td><td>Main :</td></tr>
</table>

	1. Christof Paar and Jan Pelzl. 2010. Understanding Cryptography: A Textbook for Students and Practitioners. Springer-Verlag. ISBN: 978-3-642-04100-6 **Support :**