Module Description of Cryptography

Module Name	:	Cryptography
Module Level	:	Bachelor
Code, if applicable	:	23H01131303
Subtitle, if applicable	:	-
Courses, if applicable	:	Cryptography
Semester(s) in which the module is taught	:	5 (Fifth Semester)
Module coordinator(s)	:	Prof. Dr. Amir Kamal Amir, M.Sc.
Lecturer(s)	:	Prof. Dr. Amir Kamal Amir, M.Sc. Dr. Andi Muhammad Anwar, S.Si., M.Si
Language	:	Bahasa (Indonesian language)
Relation to curriculum	:	Elective course in third year for Bachelor degree in Mathematics
Type of teaching/teaching method	:	Lecturing, Small Group Discussion, Cooperative Learning, Self-Directed Learning
Contact hours	:	150 minutes lectures per week, 180 minutes structured activities per week, and 180 minutes independent study per week
Workload	:	Total workload is 135 hours per semester which consists of 40 hours per semester for Learning and Teaching, 47.5 hours per semester for Self-Study, and 47.5 hours per semester for Structured Works
Credit points	:	3 (4.8 ECTS)
Requirements according to the examination regulations	:	Students are required to attend at least 80% of the total meetings which is recorded via the attendance menu at https://sikola-v2.unhas.ac.id/, complete all mandatory assignments, and obtain permission from the lecturer to participate in the written examination.
Recommended prerequisites	:	Students have completed and taken the exams for Calculus I, Calculus II, and Statistical Methods
Module objectives/intended learning outcomes	:	After the completion of this module, the student will be able to: CLO 1. describe cryptosystems and build cipher models from a given problem; CLO 2. explain several types of public key systems and apply them to solve several everyday problems; CLO 3. explaining and applying cryptanalysis to classical cryptography. The following is the mapping of the ILO and the CLO of this course:

	ILO 1	ILO 2	ILO 6
CLO 1	X	X	
CLO 2		X	X
CLO 3	X		X

<table>
<tr><td>Content</td><td>:</td><td>Cryptography is an elective course in the field of algebra that covers current topics in the application of mathematics, particularly in cryptography and data security. The material covered includes data communication security in computer networks, classical and modern cryptography (symmetric and public key), as well as basic algebraic concepts such as groups, rings, and fields. Additionally, the course covers cryptographic algorithms such as DES and AES, number theory in public-key cryptography, hashing functions, and digital signatures as part of cryptographic security systems.</td></tr>
<tr><td>Study and examination requirements</td><td>:</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 final grade.</td></tr>
<tr><td>Exams and assessment formats</td><td>:</td><td>Participants are marked based on their performance in theory: Quizzes (20%), Written Exam (30%), and Report (50%).

Reports measure analytical and writing skills. Quizzes are used to test continuous understanding of weekly content. The Written Exam assesses comprehension and synthesis of all materials discussed during the semester. Altogether, these components account for 100% of the final grade.
Students are marked based on their percentage of points obtained and based on the following grade scale:
<table>
<tr><th>Percentage of Achievement</th><th>Grade</th><th>Conversion Value</th></tr>
<tr><td>85 – 100</td><td>A</td><td>4.00</td></tr>
<tr><td>80 - <85</td><td>A-</td><td>3.75</td></tr>
<tr><td>75 - < 80</td><td>B+</td><td>3.5</td></tr>
<tr><td>70 - < 75</td><td>B</td><td>3.0</td></tr>
<tr><td>65 - < 70</td><td>B-</td><td>2.75</td></tr>
<tr><td>60 - < 65</td><td>C+</td><td>2.5</td></tr>
<tr><td>50 - < 60</td><td>C</td><td>2.00</td></tr>
<tr><td>40 - < 50</td><td>D</td><td>1.00</td></tr>
<tr><td>< 40</td><td>E</td><td>0.00</td></tr>
</table></td></tr>
<tr><td>Reading list</td><td>:</td><td>Hoffstein, J., Pipher, J., Silverman, H.J., 2014, An Introduction to Mathematical Cryptography (Undergraduate Text in Mathematics), Springer Science-Bussines Media, New York
Johannes A. Buchmann, 2001, Introduction to Cryptografi, Springer-Verlag, New York, Berlin, Heidelberg.Calculus, 7th edition, James Stewart, 2000.</td></tr>
<tr><td>Last revision date</td><td>:</td><td>July 28th, 2025</td></tr>
</table>