



UNIVERSITAS INDONESIA
 Faculty of Mathematics and Natural Sciences
 Department of Mathematics
 Building D, Kampus UI Depok 16424, Telp: 021 - 7863439,
 Email: sekretariat.math@sci.ui.ac.id, website: <https://www.math.ui.ac.id/>

MODULE HANDBOOK

Module designation	<i>Cryptography</i>
Semester(s) in which the module is taught	6, 7
Person responsible for the module	<i>Dr. Kiki Ariyanti Sugeng</i>
Language	<i>Indonesia</i>
Relation to curriculum	<i>Elective</i>
Teaching methods	<i>Flipped Class and Problem-based learning using E-learning</i>
Workload (incl. contact hours, self-study hours)	<i>Total workload: 170 minutes/credit point Contact hours: 50 minutes synchronous and 120 minutes asynchronous (independent study / reading, doing homework, discussion with peers)</i>
Credit points	<i>3 SKS (4.77 ECTS)</i>
Required and recommended prerequisites for joining the module	<i>Linear Algebra Discrete Mathematics Algebra</i>
Module objectives/intended learning outcomes	<i>After completing this module, students be able to</i> <ul style="list-style-type: none"> • <i>Explaining the basic concept of cryptographic systems.</i> • <i>Using basic mathematical concepts in classification and modern cryptography.</i> • <i>Explaining how block cipher and public key Cryptography works</i> • <i>Explaining post-quantum cryptography</i> • <i>Show examples on what the cryptography applications in everyday life and how it works</i>
Content	<i>Classic Cryptography, Block Cipher Cryptography, Public Key Cryptography and RSA, Post Quantum Cryptography, Application of Cryptography.</i>
Examination forms	<i>Essay, Project, Presentation</i>

<p>Study and examination requirements</p>	<p><i>The final score is the composition of mid-test scores, quizzes, and assignments with the following weight:</i></p> <p><i>Assignment and Presentation : 40 %</i> <i>Mid-test : 30 %</i> <i>Project : 30 %</i> <i>Total : 100 %</i></p> <table data-bbox="845 448 1212 884"> <thead> <tr> <th>Mark</th> <th>Grade</th> </tr> </thead> <tbody> <tr> <td>85—100</td> <td>A</td> </tr> <tr> <td>80—<85</td> <td>A-</td> </tr> <tr> <td>75—<80</td> <td>B+</td> </tr> <tr> <td>70—<75</td> <td>B</td> </tr> <tr> <td>65—<70</td> <td>B-</td> </tr> <tr> <td>60—<65</td> <td>C+</td> </tr> <tr> <td>55—<60</td> <td>C</td> </tr> <tr> <td>40—<55</td> <td>D</td> </tr> <tr> <td><40</td> <td>E</td> </tr> </tbody> </table>	Mark	Grade	85—100	A	80—<85	A-	75—<80	B+	70—<75	B	65—<70	B-	60—<65	C+	55—<60	C	40—<55	D	<40	E
Mark	Grade																				
85—100	A																				
80—<85	A-																				
75—<80	B+																				
70—<75	B																				
65—<70	B-																				
60—<65	C+																				
55—<60	C																				
40—<55	D																				
<40	E																				
<p>Reading list</p>	<p><i>[1] W. Stallng, Cryptography and Network Security, 4th ed, Pearson2006</i> <i>[2] Various articles</i></p>																				