



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>Coding Theory and Cryptography</i>
Semester(s) in which the module is taught	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	<p><i>After completing this module, students be able to</i></p> <ul style="list-style-type: none"> • <i>Explain the basic concepts of coding theory</i> • <i>Differentiate the code types and their properties</i> • <i>Explain the concept of error correction code and its properties</i> • <i>Explain the application of the code in everyday life</i> • <i>Explain on how cryptographic schemes work</i> • <i>Give example on cryptography applications in everyday life.</i> 																												
Content	<p><i>Basic concept of code, linear code and its property, error correction code, application of coding theory in the daily life, relation with cryptography, classic encryption scheme, block cipher cryptography, Public Key Cryptography and Application of Cryptography.</i></p>																												
Examination forms	<p><i>Essay, Project, Presentation Slide</i></p>																												
Study and examination requirements	<p><i>The final score is the composition of mid-test scores, quizzes, and assignments with the following weight:</i></p> <table style="margin-left: 40px;"> <tr> <td><i>Assignment and Presentation</i></td> <td style="text-align: right;"><i>: 40 %</i></td> </tr> <tr> <td><i>Mid-test</i></td> <td style="text-align: right;"><i>: 30 %</i></td> </tr> <tr> <td><i>Project</i></td> <td style="text-align: right;"><i>: 30 %</i></td> </tr> <tr> <td><i>Total</i></td> <td style="text-align: right;"><i>: 100 %</i></td> </tr> </table> <table style="margin-left: 40px;"> <thead> <tr> <th style="text-align: center;">Mark</th> <th style="text-align: center;">Grade</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">85—100</td> <td style="text-align: center;">A</td> </tr> <tr> <td style="text-align: center;">80—<85</td> <td style="text-align: center;">A-</td> </tr> <tr> <td style="text-align: center;">75—<80</td> <td style="text-align: center;">B+</td> </tr> <tr> <td style="text-align: center;">70—<75</td> <td style="text-align: center;">B</td> </tr> <tr> <td style="text-align: center;">65—<70</td> <td style="text-align: center;">B-</td> </tr> <tr> <td style="text-align: center;">60—<65</td> <td style="text-align: center;">C+</td> </tr> <tr> <td style="text-align: center;">55—<60</td> <td style="text-align: center;">C</td> </tr> <tr> <td style="text-align: center;">40—<55</td> <td style="text-align: center;">D</td> </tr> <tr> <td style="text-align: center;"><40</td> <td style="text-align: center;">E</td> </tr> </tbody> </table>	<i>Assignment and Presentation</i>	<i>: 40 %</i>	<i>Mid-test</i>	<i>: 30 %</i>	<i>Project</i>	<i>: 30 %</i>	<i>Total</i>	<i>: 100 %</i>	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
<i>Assignment and Presentation</i>	<i>: 40 %</i>																												
<i>Mid-test</i>	<i>: 30 %</i>																												
<i>Project</i>	<i>: 30 %</i>																												
<i>Total</i>	<i>: 100 %</i>																												
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																												

Reading list	<p>[1] <i>W. Stalling, Cryptography and Network Security, 4th ed, Pearson2006</i></p> <p>[2] <i>C. Wuthrich, Coding and Cryptography,</i> https://www.maths.nottingham.ac.uk/plp/pmzcx/download/ccr.pdf</p> <p>[3] <i>Various articles</i></p>
--------------	--