UNIVERSITAS GADJAH MADA
Faculty of Mathematics and Natural Sciences
Department of Computer Science and Electronics
Sekip Utara Bulaksumur Yogyakarta 55281 Telp: +62 274 546194 Email: dep-ike.mipa@ugm.ac.id Website: http://dcse.fmipa.ugm.ac.id

Bachelor in Computer Science
Telp : +62 274 546194
Email : prodi-s1-ilkom.mipa@ugm.ac.id
Website : http://dcse.ugm.ac.id/

MODULE HANDBOOK

Module name	**Cryptography and Network Security**
Module level, if applicable	Undergraduate
Code, if applicable	MII-2604
Courses, if applicable	NA
Semester(s) in which the module is taught	Fall (Odd)
Person responsible for the module	Drs. Bambang Nurcahyo Prastowo, M.Sc
Lecturer(s)	Drs. Bambang Nurcahyo Prastowo, M.Sc
Language	Bahasa Indonesia & English
Relation to curriculum	1. Undergraduate degree program, compulsory, 4th semester. 2. International undergraduate program, compulsory, 4th semester.
Teaching methods	1. Undergraduate degree program: lectures, < 60 students, 2. International undergraduate program: lectures, < 30 students.
Workload (incl. contact hours, self-study hours)	1. Lectures: 3 x 50 = 100 minutes per week. 2. Exercises and Assignments: 3 x 50 = 100 minutes per week. 3. Private study: 1 x 50 = 50 minutes per week.
Credit points	3 credit points (sks).
Requirements according to the examination regulations	A student must have attended at least 75% of the lectures to sit in the exams.
Required and recommended prerequisites for joining the module	NA
Learning outcomes and their corresponding PLOs	After completing this module, a student is expected to: CO1. Able to identify and explain the concept of information and communication security CO.2 Able to explain and identify cryptography CO3. Able to identify tools and approaches (algorithms) used in cryptography and network security CO4. Be able to explain how to work and optimize performance on cryptography and network security CO5. Able to present and present the implementation of cryptography and network security

PLO	CO1	CO2	CO3	CO4	CO5

<table>
<tr><td></td><td>
<table>
<tr><td rowspan="5">Program Learning Outcome (PLO)</td><td>PLO1</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>PLO2</td><td>√</td><td>√</td><td></td><td></td><td></td></tr>
<tr><td>PLO3</td><td></td><td>√</td><td>√</td><td></td><td></td></tr>
<tr><td>PLO4</td><td></td><td></td><td>√</td><td>√</td><td></td></tr>
<tr><td>PLO5</td><td></td><td></td><td></td><td>√</td><td>√</td></tr>
</table>
</td></tr>
<tr><td>Content</td><td>This course provides knowledge, understanding related to information and communication security. The material also discusses cryptography. Tools, approaches / algorithms and supports used in cryptography and network security. Learn how to work and performance optimization in cryptography and network security, and implement the use of cryptography and network security
1. The concept of information and communication security. an introduction to cryptography
2. Classic cryptography, one-time-pad.
3. Symmetric encryption, block cipher, Faistel's Algorithm, AES
4. Pseudorandom number generator, stream cipher.
5. Block cipher modes of operations
6. Asymmetric algorithm. RSA, Diffie Hellman, Ellective curve
7. Cryptographic hash functions, SHA-2, SHA-3, use of hash functions on the block chain.
8. Message authentication codes and digital signatures
9. Lattice-based cryptography
10. Key management and distribution.
11. Attacks against data and privacy, fabrication, wiretapping, forgery, viruses, spyware, worms
12. System and network security, attacks on systems and networks, Spam, phishing, botnets, denial of service, firewall, bastian host, DMZ.
13. The basic principles of web security, web application security, content security, session management.</td></tr>
<tr><td>Study and examination requirements and examination forms</td><td>The evaluation is done in 2 forms, namely:
1. Trial, either midterm or semester test,
2. Two tasks, including individual or
3. Two group assignments to be completed within a certain timeframe, and

Assessment is done using benchmark assessment, with the aim of measuring the level of student understanding related to the target and class rank.</td></tr>
<tr><td>Media employed</td><td>e-learning Platform (ELOK), LCD, blackboard, and websites.</td></tr>
<tr><td>Assessments and evaluation</td><td>
<table>
<tr><th>Type</th><th>Percentage</th><th>CO1</th><th>CO2</th><th>CO3</th><th>CO4</th><th>CO5</th></tr>
<tr><td>Task 1</td><td>10</td><td>√</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Group Task 1</td><td>10</td><td></td><td>√</td><td></td><td></td><td></td></tr>
<tr><td>MidSem Test</td><td>30</td><td></td><td>√</td><td>√</td><td></td><td></td></tr>
<tr><td>Task 2</td><td>5</td><td></td><td></td><td></td><td>√</td><td></td></tr>
<tr><td>Group Task 2</td><td>10</td><td></td><td></td><td>√</td><td>√</td><td></td></tr>
<tr><td>Final Test</td><td>30</td><td></td><td></td><td></td><td>√</td><td>√</td></tr>
<tr><td>Total</td><td>100</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Reading list	1. Stallings, W., 2020, Cryptography and Network Security: Principles and Practices, 8th edition, Pearson Education Inc., New Jersey. 2. Speciner, M., Perlman, R., Kaufman, C., 2002, Network Security Private Communications in a Public World, 2nd edition, Pearson.

Created date : June 25, 2021

Revision date : July 1, 2022