UNDERGRADUATE PROGRAM IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER SCIENCE AND ELECTRONICS
FACULTY OF MATHEMATICS AND NATURAL SCIENCES
UNIVERSITAS GADJAH MADA

<table>
<tr><td>Module name</td><td>System and Cyber Security</td></tr>
<tr><td>Module level</td><td>Undergraduate</td></tr>
<tr><td>Code</td><td>MII-3602</td></tr>
<tr><td>Courses (if applicable)</td><td>System and Cyber Security</td></tr>
<tr><td>Semester</td><td>Fall (Odd)</td></tr>
<tr><td>Contact person</td><td></td></tr>
<tr><td>Lecturer</td><td></td></tr>
<tr><td>Language</td><td>Bahasa Indonesia</td></tr>
<tr><td>Relation to curriculum</td><td>1. Undergraduate degree program, compulsory, 5th or 7th semester.
2. International undergraduate program, compulsory, 5th or 7th semester.</td></tr>
<tr><td>Type of teaching, contact hours</td><td>1. Undergraduate degree program: lectures, < 60 students,
2. International undergraduate program: lectures, < 30 students.</td></tr>
<tr><td>Workload</td><td>1. Lectures: 3 x 50 = 150 minutes (2,5 hours) per week.
2. Exercises and Assignments: 3 x 60 = 180 minutes (3 hours) per week.
3. Private study: 3 x 60 = 180 minutes (3 hours) per week.</td></tr>
<tr><td>Credit points</td><td>3 credit points (sks)</td></tr>
<tr><td>Requirements according to the Examination regulations</td><td>A student must have attended at least 75% of the lectures to sit in the exams.</td></tr>
<tr><td>Recommended prerequisites</td><td>Cryptography and Network Security</td></tr>
<tr><td>Learning outcomes (course outcomes) and their corresponding PLOs</td><td>After completing this module, a student is expected to:
CO1 comprehend the foundational and theoretical knowledge of system and cyber security, which are cyber systems and cyber laws
CO2 comprehend the applied knowledge of system and cyber security, which are specification, scanning, firewall and defense, types of attack, security measures, and ethical hacking
CO3 be able to apply knowledge and state-of-the-art in the field of system and cyber security to anticipate and solve problems related to system and cyber security
CO4 be able to develop advanced skill and keep up with technologies in the field of system and cyber security

<table>
<tr><th colspan="2">PLO</th><th>CO1</th><th>CO2</th><th>CO3</th><th>CO4</th></tr>
<tr><td rowspan="3">Program Learning</td><td>PLO1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PLO2</td><td>√</td><td></td><td></td><td></td></tr>
<tr><td>PLO3</td><td></td><td>√</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td rowspan="2">Outcome (PLO)</td><td>PLO4</td><td></td><td></td><td>√</td><td></td></tr>
<tr><td>PLO5</td><td></td><td></td><td></td><td>√</td></tr>
</table>
</td></tr>
<tr><td>Contents</td><td>(a) Cyber systems: scope, requirements, threats, latest reports
(b) Cyber laws: cyber crimes dan threats global, security standard and compliances
(c) Specification: naming, addressing, subnetting, networking protocols & devices, application layer, transport layer, Internet layer, and link layer
(d) Scanning networks to find malicious networks — network scanning types, port scanning & its tools, and network architecture
(e) Security measures for mobile and web applications
(f) Firewall and defense
(g) Malware, denial-of-service (DoS) attacks, man-in-the-middle (MITM) attack, social engineering attacks, spoofing, phishing, SQL injection
(h) Security measure Cloud and IoT
(i) Ethical hacking</td></tr>
<tr><td>Study and examination requirements and forms of examination</td><td>The evaluation is done in 3 forms, namely:
1. Examination, either midterm or final exam,
2. Two assignments, including individual or group assignments to be completed within a certain timeframe, and
3. Two quizzes, held on LMS (eLOK), once before midterm exam and once after midterm exam, with a short answer or multiple choice form

Assessment is done using benchmark assessment, to measure the level of student’s comprehension and competency related to the target and class rank</td></tr>
<tr><td>Media employed</td><td>LCD, blackboard, and websites, learning management systems (eLOK)</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></tr>
<tr><td>Quiz</td><td>20%</td><td>√</td><td></td><td></td><td>√</td></tr>
<tr><td>Individual Task</td><td>10%</td><td></td><td>√</td><td></td><td></td></tr>
<tr><td>Group Task</td><td>10%</td><td></td><td></td><td>√</td><td></td></tr>
<tr><td>Midterm Exam</td><td>30%</td><td>√</td><td>√</td><td></td><td></td></tr>
<tr><td>Final Exam</td><td>30%</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></tr>
</table>
</td></tr>
<tr><td>Reading List</td><td>Cyber Security: Managing System, Conducting Testing and Investigating Intrusions, Thomas J Mowbray, October 2013, Wiley</td></tr>
</table>