Subject Description Form

Subject Code	AMA3100
Subject Title	Number, Combinatorics and Statistics
Credit Value	3
Level	3
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	1. Introduce to students the necessary mathematical background for the understanding of modern information security measures 2. Equip students with knowledge of basic number theory, combinatorics and statistical methods 3. Introduce the applications of these theories in the area of information security
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand number theory as the background of modern cryptography 2. Understand statistical methods and their applications to the area of information security 3. Understand combinatorial mathematics Category B: Attributes for all-Roundedness 4. Recognise the need for continuing development
Contribution of the Subject to the Attainment of the Programme Outcomes	**Programme Outcomes:** Category A: Professional/academic knowledge and skills • Programme Outcome 1: This subject contributes to the knowledge of mathematics necessary to the discipline of information security. • Programme Outcome 2: This subject equips the students with the necessary tools for the modelling of information security requirements and processes. Category B: Attributes for all-Roundedness • Programme Outcome 8: This subject empowers the students with the mathematical background to communicate effectively with the academia.
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Number Theory This part aims to cover elementary number theory. Topics include modular exponentiation, Euclidean algorithms, modular arithmetic, multiplicative inverses, system of linear congruences, discrete logarithms, and error correcting codes. 2. Combinatorics This part covers combinatorial probability, Knapsack problem, and pigeonhole principle, and binomial coefficients. Optional overview of advanced topics such as linear programming and game theory, network and graph theory. 3. Statistics This part covers methods of collecting and summarising data. Statistical inference methods concerning population means, proportions and variances are given. Common statistical tests and procedures, including correlation, regression analysis, Chi-square test will be covered. 4. RSA encryption

<table>
<tr><td></td><td>Applications of the above mathematical concepts to the area of information security will be discussed (e.g. RSA and ElGamal encryption based on number theory, virus signature detection using statistical test).</td></tr>
<tr><td>Teaching/Learning Methodology</td><td>During the lectures, students will come across the common concepts and theories. Those concepts and theories would be explained with reference to sample applications.

In the tutorials, students will be given scenarios related to the area of information security where these mathematical concepts are relevant.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Subject Learning Outcomes</td><td>
<table>
<tr><th rowspan="2">Specific Assessment Methods/Tasks</th><th rowspan="2">% Weighting</th><th colspan="4">Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)</th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td>1. Continuous Assessment</td><td>50%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2. Examination</td><td>50%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Total</td><td>100%</td><td colspan="4"></td></tr>
</table>

Types of assessments include assignments, test and examination.

Assignments are designed to reinforce the concepts and theories learned in the lecture and tutorial, by solving bigger problems. Test and examination are used to assess independent problem solving and critical thinking skills.</td></tr>
<tr><td>Student Study Effort Expected</td><td>
<table>
<tr><td>Class contact:</td><td></td></tr>
<tr><td>• Lecture</td><td>26 Hours</td></tr>
<tr><td>• Tutorial / Lab</td><td>13 Hours</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>• Assignments, project, self-study, text and exam preparation</td><td>66 Hours</td></tr>
<tr><td>Total student study effort:</td><td>105 Hours</td></tr>
</table>
</td></tr>
<tr><td>Reading List and References</td><td>Reference Books:

1. John Stillwell, Elements of Number Theory., United States: Springer Undergraduate Texts in Mathematics, 2002.
2. J. H. van Lint, R. M. Wilson, A Course in Combinatorics, Cambridge: Cambridge University Press, 2001.
3. Douglas C. Montgomery, George C. Runger, Norma F. Hubele, Engineering Statistics. United States: Wiley, 2010.
4. Johannes A. Buchmann, Introduction to Cryptography. United States: Springer Undergraduate Texts in Mathematics, 2004.
5. Douglas Stinson, Cryptography: Theory and Practice. United States: CRC Press, 2006
6. W. Cary Huffman, Vera Pless, Fundamentals of Error Correcting Codes. Cambridge: Cambridge University Press, 2003
7. Hans Kellerer, Ulrich Pferschy, David Pisinger, Knapsack Problems. Berlin: Springer, 2004</td></tr>
</table>