

Subject Description Form

Subject Code	AMA3100
Subject Title	Number, Combinatorics and Statistics
Credit Value	3
Level	3
Pre-requisite	Basic algebra, calculus, statistics
Co-requisite/ Exclusion	Nil
Objectives	<ol style="list-style-type: none"> 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	<p>Upon completion of the subject, students will be able to:</p> <p><u>Category A: Professional/academic knowledge and skills</u></p> <ol style="list-style-type: none"> 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 <p><u>Category B: Attributes for all-Roundedness</u></p> <ol style="list-style-type: none"> 4. Recognise the need for continuing development
Subject Synopsis/ Indicative Syllabus	<p>Syllabus:</p> <ol style="list-style-type: none"> 1. <u>Number Theory</u> 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. <u>Combinatorics</u> 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. <u>Statistics</u> 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. <u>RSA encryption</u> Applications of the above mathematical concepts to the area of information security will be discussed (e.g. RSA encryption based on number theory, virus signature detection using statistical test).
Teaching/Learning Methodology	<p>During the lectures, students will come across the common concepts and theories. Those concepts and theories would be explained with reference to sample applications.</p> <p>In the tutorials, students will be given scenarios related to the area of information security where these mathematical concepts are relevant.</p>

Assessment Methods in Alignment with Intended Subject Learning Outcomes	Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)			
			1	2	3	4
	1. Continuous Assessment	50%	✓	✓	✓	✓
	2. Examination	50%	✓	✓	✓	✓
	Total	100%				
	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.					
	Students are required to pass both the continuous assessment and the final examination components in order to pass the subject.					
Student Study Effort Expected	Class contact:					
	• Lecture					26 Hours
	• Tutorial / Lab					13 Hours
	Other student study effort:					
	• Assignments, project, self-study, text and exam preparation					66 Hours
	Total student study effort:					105 Hours
Reading List and References	Reference Books:					
	1. John Stillwell, <i>Elements of Number Theory.</i> , United States: Springer Undergraduate Texts in Mathematics, 2002.					
	2. J. H. van Lint, R. M. Wilson, <i>A Course in Combinatorics</i> , Cambridge: Cambridge University Press, 2001.					
	3. Douglas C. Montgomery, George C. Runger, Norma F. Hubele, <i>Engineering Statistics</i> . United States: Wiley, 2010.					
	4. Johannes A. Buchmann, <i>Introduction to Cryptography</i> . United States: Springer Undergraduate Texts in Mathematics, 2004.					
Last Updated	June 2016					
Prepared by	AMA and COMP Departments					