Subject Code	COMP6521
Subject Title	Cryptography and Blockchain
Credit Value	3
Level	6
Normal Duration	1 semester
Pre-requisite/ Co-requisite/ Exclusion	Nil
Role and Purposes	To equip students with some basic understanding of cryptography that leads to an understanding of blockchain and cybersecurity. Core cryptographic tools like encryption, authentication, digital signature and key agreement protocols are used behind daily on-line transactions nowadays. Such tools will be covered in the first part of the course. In the second part, students will learn the blockchain mechanism and its various business applications. At the final part of the course, students will be exposed to the threats to the Internet infrastructure. This subject will contribute to the achievement of the DFintech program outcomes by • allowing students to acquire the ability to conduct original applied research in tech-related business areas. (Outcome 3)
Subject Learning Outcomes	Upon completion of the subject, students will be able to: a. acquire a foundational understanding of the three cryptographic primitives: encryptions (including secret-key encryption and public-key encryption), one-way hash functions and digital signatures; b. understand the basics of the blockchain technology and its various business applications, including cryptocurrencies; c. understand the major security issues in implementing major security functions: secrecy, identity authentication, message authentication, nonrepudiation and availability; d. understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; e. understand the major threats to the Internet-wide security today, such as various security attacks.
Subject Synopsis/ Indicative Syllabus	Topic 1. Cryptographic functions and services • Symmetric encryptions, hash functions, message authentication codes, public-key encryption, digital signatures and authentication protocols. Topic 2. Overview of cybersecurity

<table>
<tr><td></td><td>
Types of attacks, threat models and the role of cryptography in network security.
Topic 3. Internet security
Link layer security, network layer security, transport layer security and application layer security.
Topic 4. Understanding blockchain
Discover the technology, the operation of blockchain and the scope of the blockchain industry.
Topic 5. Cryptocurrencies and new payment mechanisms
Explore how blockchain is powering new payment rail and cryptocurrencies, and new mechanisms for trading, settlement and clearing.
Investigate key strategic challenges and opportunities in these areas.
Topic 6. Blockchain-based applications and business models
Discover how blockchain is enabling new forms of management and organization through decentralized applications, smart contracts, and new frameworks for identity and data sharing.
Learn how blockchain is fundamentally changing ways of doing business, and the impact this has on industries, consumers and society.
</td></tr>
<tr><td>Teaching/Learning Methodology</td><td>The course will be offered in a mode that combines seminars (including guest lectures), case study, team presentations and group discussions.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes
(Note 4)</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="6">Intended subject learning outcomes to be assessed (Please tick as appropriate)</td></tr>
<tr><td>a.</td><td>b.</td><td>c.</td><td>d.</td><td>e.</td><td></td></tr>
<tr><td>Continuous Assessment*</td><td>100%</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1. Class participation</td><td>20 %</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>2. Group Case study & presentation</td><td>20 %</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>3. Individual Assignment</td><td>20%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>4. Individual Assessment (e.g. Test)</td><td>40%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>Total</td><td>100 %</td><td colspan="6"></td></tr>
</table>
*Weighting of assessment methods/tasks in continuous assessment may be
</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">different, subject to each subject lecturer.

To pass this subject, students are required to obtain Grade D or above in the Continuous Assessment components.

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes: the various methods are designed to ensure that all students taking this subject –

1. Class participation aims to stimulate students to be exposed to various new potential applications of the smart city and urban informatics technologies in different business areas.
2. Group case study in the classroom enables students to work as a team to discuss and analyze the common and different characteristics of different smart city and urban informatics technologies.
3. The short written individual assignment of 2,000 words in the form of review essay will be used to assess individual student's understanding of the latest smart city and urban informatics technologies and student's critical thinking and analysis of any new applications of technologies.
4. Individual assessment is used to assess individual students' ability to have an overall understanding of the inter-relationship of the various technologies and their individual characteristics.</td></tr>
<tr><td rowspan="6">Student Study Effort Expected</td><td>Class contact:</td><td></td></tr>
<tr><td>▪ Lectures</td><td>30 Hrs.</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>▪ Preparation for the class</td><td>30 Hrs.</td></tr>
<tr><td>▪ Preparation for Assignments</td><td>60 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>120 Hrs.</td></tr>
<tr><td>Reading List and References</td><td colspan="2">N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley 2010.

R. Anderson, Security Engineering, Second Edition, Wiley 2008.

William Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons Inc 2016.

Daniel Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, aPress 2017.</td></tr>
</table>