

Subject Description Form

Subject Code	COMP4134
Subject Title	Biometrics and Security
Credit Value	3
Level	4
Pre-requisite	AMA1104 Introductory Probability or HKDSE Maths Extended Module or equivalent, COMP3422 Creative Digital Media Design or equivalent mathematics subjects.
Co-requisite/ Exclusion	Nil
Objectives	<ul style="list-style-type: none">• To understand the fundamental issues and technologies for network security, in particular the basic technologies for cryptography and various applications• To introduce biometric computing knowledge and methods• To learn some basic biometrics systems with real case studies
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 fundamental issues and challenges for network security2. Get familiar with the basic techniques for cryptography including conventional encryption, public-key cryptograph, message authentication, hash functions and digital signature3. Understand the key issues and importance of biometric systems for security concerns4. Recognize physical and behavior biometric characteristics;5. Apply biometric technology for different security applications. <p><u>Category B: Attributes for all-roundedness</u></p> <ol style="list-style-type: none">6. Communicate effectively with project presentation and technical reports;7. Learn independently for problem solving and solution seeking for various applications.

Subject Synopsis/ Indicative Syllabus	<p>Syllabus:</p> <table border="1" data-bbox="459 210 1410 1592"> <thead> <tr> <th data-bbox="467 210 1402 259">Topic</th> </tr> </thead> <tbody> <tr> <td data-bbox="467 259 1402 398"> 1. <u>Introduction to Information Security</u> Why is information security important? What is information security concerned? How to achieve information security – basic concepts, techniques and applications. </td> </tr> <tr> <td data-bbox="467 398 1402 515"> 2. <u>Conventional Encryption Technology</u> Classic and modern techniques for encryption, stream ciphers and block ciphers, DES (Data Encryption Standard). </td> </tr> <tr> <td data-bbox="467 515 1402 609"> 3. <u>Public-key Cryptography and Message Authentication</u> public-key cipher, classes of public-key algorithms, message authentication </td> </tr> <tr> <td data-bbox="467 609 1402 797"> 4. <u>Digital Watermarking for Information Security</u> watermarking concept, watermarking definition, problems with watermarking, watermark attacks, classification of watermarking, applications of watermarking (copyright protection, authentication and integrity checking, hidden annotation, secure and invisible communication) </td> </tr> <tr> <td data-bbox="467 797 1402 936"> 5. <u>Introduction to Biometrics and Authentication</u> Why biometrics? What about biometrics? How to design biometric systems? Biometrics definitions and notations; biometric applications; information security; security technologies and systems; authentication. </td> </tr> <tr> <td data-bbox="467 936 1402 1115"> 6. <u>Fundamental Techniques</u> Biometrics data acquisition and biometrics database; the related image processing and pattern recognition technologies, including digital image and signal representation, pattern extraction and classification; basic PCA/LDA approaches of automated biometrics identification and verification. </td> </tr> <tr> <td data-bbox="467 1115 1402 1272"> 7. <u>Typical Physical Biometrics</u> Basic physical characteristics of biometrics; some basic introduction of physical biometrics systems (such as fingerprint, palm-print, finger, hand, face, iris, and face etc.). </td> </tr> <tr> <td data-bbox="467 1272 1402 1429"> 8. <u>Typical Behavioral Biometrics</u> Basic behavioral characteristics of biometrics; some basic introduction of behavioral biometrics systems (such as voice, signature, and gesture recognition, etc.). </td> </tr> <tr> <td data-bbox="467 1429 1402 1592"> 9. <u>Multi-Biometrics and Applications</u> Security application: Internet/Intranet; e-commerce; banking services; immigration and naturalization service; computer systems; physical access; telephone systems; time, attendance and monitoring. </td> </tr> </tbody> </table> <p data-bbox="459 1626 1410 1704">Case Study: Network security and biometric applications.</p>	Topic	1. <u>Introduction to Information Security</u> Why is information security important? What is information security concerned? How to achieve information security – basic concepts, techniques and applications.	2. <u>Conventional Encryption Technology</u> Classic and modern techniques for encryption, stream ciphers and block ciphers, DES (Data Encryption Standard).	3. <u>Public-key Cryptography and Message Authentication</u> public-key cipher, classes of public-key algorithms, message authentication	4. <u>Digital Watermarking for Information Security</u> watermarking concept, watermarking definition, problems with watermarking, watermark attacks, classification of watermarking, applications of watermarking (copyright protection, authentication and integrity checking, hidden annotation, secure and invisible communication)	5. <u>Introduction to Biometrics and Authentication</u> Why biometrics? What about biometrics? How to design biometric systems? Biometrics definitions and notations; biometric applications; information security; security technologies and systems; authentication.	6. <u>Fundamental Techniques</u> Biometrics data acquisition and biometrics database; the related image processing and pattern recognition technologies, including digital image and signal representation, pattern extraction and classification; basic PCA/LDA approaches of automated biometrics identification and verification.	7. <u>Typical Physical Biometrics</u> Basic physical characteristics of biometrics; some basic introduction of physical biometrics systems (such as fingerprint, palm-print, finger, hand, face, iris, and face etc.).	8. <u>Typical Behavioral Biometrics</u> Basic behavioral characteristics of biometrics; some basic introduction of behavioral biometrics systems (such as voice, signature, and gesture recognition, etc.).	9. <u>Multi-Biometrics and Applications</u> Security application: Internet/Intranet; e-commerce; banking services; immigration and naturalization service; computer systems; physical access; telephone systems; time, attendance and monitoring.
	Topic										
1. <u>Introduction to Information Security</u> Why is information security important? What is information security concerned? How to achieve information security – basic concepts, techniques and applications.											
2. <u>Conventional Encryption Technology</u> Classic and modern techniques for encryption, stream ciphers and block ciphers, DES (Data Encryption Standard).											
3. <u>Public-key Cryptography and Message Authentication</u> public-key cipher, classes of public-key algorithms, message authentication											
4. <u>Digital Watermarking for Information Security</u> watermarking concept, watermarking definition, problems with watermarking, watermark attacks, classification of watermarking, applications of watermarking (copyright protection, authentication and integrity checking, hidden annotation, secure and invisible communication)											
5. <u>Introduction to Biometrics and Authentication</u> Why biometrics? What about biometrics? How to design biometric systems? Biometrics definitions and notations; biometric applications; information security; security technologies and systems; authentication.											
6. <u>Fundamental Techniques</u> Biometrics data acquisition and biometrics database; the related image processing and pattern recognition technologies, including digital image and signal representation, pattern extraction and classification; basic PCA/LDA approaches of automated biometrics identification and verification.											
7. <u>Typical Physical Biometrics</u> Basic physical characteristics of biometrics; some basic introduction of physical biometrics systems (such as fingerprint, palm-print, finger, hand, face, iris, and face etc.).											
8. <u>Typical Behavioral Biometrics</u> Basic behavioral characteristics of biometrics; some basic introduction of behavioral biometrics systems (such as voice, signature, and gesture recognition, etc.).											
9. <u>Multi-Biometrics and Applications</u> Security application: Internet/Intranet; e-commerce; banking services; immigration and naturalization service; computer systems; physical access; telephone systems; time, attendance and monitoring.											
Teaching/Learning Methodology	<p>The course material will be delivered as a combination of lectures, tutorials and small group project. Students will get familiar with basic concepts and technologies of network security, biometric systems and applications.</p>										

Assessment Methods in Alignment with Intended Learning Outcomes	Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)						
			1	2	3	4	5	6	7
	1. Continuous Assessment	60%							
	• Assignments		✓	✓	✓	✓	✓	✓	✓
	• Lab exercises								
	• Project		✓		✓	✓	✓	✓	✓
	• Mid-term								
	2. Examination	40%	✓	✓				✓	✓
Total	100 %								
Student Study Effort Expected	Class contact:								
	• Lecture		39 Hours						
	Other student study effort:								
	• Homework		25 Hours						
	• Project		41 Hours						
	Total student study effort:		105 Hours						
Reading List and References	Reference Books:								
	1. Stallings, W. <i>Cryptography and Network Security: Principles and Practice</i> , Third Edition, Prentice Hall, 2003.								
	2. Zhang, D., <i>Automated Biometrics: Technologies & Systems</i> , Kluwer Publisher, 2000.								
	3. Zhang, D., (Ed.), <i>Biometric Solutions for Authentication in an e-World</i> , Kluwer Publisher, 2002.								
	4. Jain, et al. (Eds.), <i>Biometrics: Personal Identification in Networked Society</i> , Kluwer Publisher, 1999.								
	5. Sid-Ahmed, M.A., <i>Image Processing, Theory, Algorithms, & Architectures</i> , McGraw-Hill, 1995.								
	6. Abrams, M.D., Jajodia, S., and Podell, H.J., <i>Information Security: An Integrated Collection of Essays</i> , IEEE Computer Society Press, 1994.								
	7. Derek Atkins, et al., <i>Internet Security Professional Reference</i> , Second Edition. New Riders Publishing, 1997.								
	8. Russell, D., <i>Computer Security Basics</i> , O'Reilly & Associates, 1991.								
	9. Zhang, D. and Jain, A.K. (Eds.), <i>Proc. First International Conference on Biometric Authentication (ICBA)</i> , 800pp, Springer Verlag, LNCS 3072, 2004								
	10. Zhang, D. and Jain, A.K. (Eds.), <i>Advances in Biometrics</i> , International Conference - ICB2006, Springer Verlag, LNCS 3832, 2006.								
	11. IEEE Transaction on Pattern Analysis and Machine Intelligence.								
	12. IEEE Transaction on Image Processing.								
Last Updated	July 2016								
Prepared by	COMP Department								