Form 2B

City University of Hong Kong

Information on a Course

offered by Department of Computer Science
with effect from Semester A in 2012 / 2013

Part I

Course Title: Cryptography: Theory and Practice

Course Code: CS5288

Course Duration: One Semester

Credit Units: 3

Level: P5

Medium of Instruction: English

Prerequisites: CS5222 Computer Networks and Internets or equivalent and
MA2144 Discrete Mathematics or equivalent

Precursors: Nil

Equivalent Courses: Nil

Exclusive Courses: Nil

Part II

Course Aims

The course provides an in-depth study of cryptographic techniques and their role in practical computer systems and applications. It covers the algorithms for symmetric and asymmetric encryption, hash functions, and pseudo random number generation; and the protocols to achieve practical security objectives such as confidentiality, authentication, data integrity, non-repudiation. Associated protocols such as key distribution and public key infrastructure systems will also be dealt with.

Course Intended Learning Outcomes (CILOs)

Upon successful completion of this course, students should be able to:

No.	**CILOs**	**Weighting** **(if applicable)**
1.	apply modular arithmetic mathematic and basic group theoretic/finite field operations related to cryptographic techniques;	
2.	describe basic concepts and algorithms of cryptography, including encryption/decryption, hash functions, pseudo random number generation;	
3.	make critique and assessment on the security of cryptographic functions, and evaluate their strength;	
4.	create and analyze protocols for various security objectives with cryptographic tools;	
5.	explain the impact of potential future development of cryptography such as quantum cryptography.	

Teaching and Learning Activities (TLAs)

(Indicative of likely activities and tasks designed to facilitate students' achievement of the CILOs. Final details will be provided to students in their first week of attendance in this course)

Teaching pattern:

Suggested lecture/tutorial/laboratory mix: 2 hrs. lecture; 1 hr. tutorial.

CILO No.	**Lectures**	**Tutorials**
CILO 1	✓	✓
CILO 2	✓	✓
CILO 3	✓	
CILO 4		✓
CILO 5	✓	✓

Assessment Tasks/Activities

(Indicative of likely activities and tasks designed to assess how well the students achieve the CILOs. Final details will be provided to students in their first week of attendance in this course)

CILO No.	**Assignment #1**	**Assignment #2**	**Quiz**	**Exam**
CILO 1	5%	5%	4%	20%
CILO 2	4%	5%	4%	20%
CILO 3				10%
CILO 4	1%			20%
CILO 5			2%	
Total	10%	10%	10%	70%

Grading of Student Achievement: Refer to Grading of Courses in the Academic Regulations for Taught Postgraduate Degrees.

Examination duration: 2 hours

Percentage of coursework, examination, etc.: 30% CW; 70% Exam

Grading pattern: Standard (A+AA-…F)

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Part III

Keyword Syllabus

Basic number theory, one-way functions, basic randomness, symmetric encryption, one-tine Pad, Feistel structure, DES, IDEA, AES, brute force attacks, strength of encryption functions, block and stream cipher, key distribution problem, secret sharing, asymmetric encryption, RSA, prime number generation, public key protocol, hybrid encryption, key exchange protocol, Diffie-Hellman, authentication protocols, hash functions, MD5, SHA, data integrity, message integrity code, non-repudiation, digital signature, RSA signature, ElGamal, DSA, elliptic curve cryptosystem, trust model, digital certificate, PKI, zero knowledge proofs, blind signature, quantum cryptography.

Recommended Reading

Text(s)

Handbook of Applied Cryptography
Online version: *http://www.cacr.math.uwaterloo.ca/hac/*