LAGUARDIA COMMUNITY COLLEGE
CITY UNIVERSITY OF NEW YORK
MAC227: Introduction to Cryptography and Applications
3 Credits, 4 hours (Lecture – 2 hours, Lab – 2hours)

Course Description

Introduction to Cryptography and Applications course is an introduction to cryptography and its history. It introduces students to classical as well as modern concepts of cryptography. Topics covered in this course include, substitution, transpositions, shared key cryptosystems (DES, 3DES, and AES), public key cryptosystems (RSA), key exchange, digital signatures, digital certificates, PGP, e-mail security, Secure Socket Layer and IPSec.

Prerequisite – MAT115

Pre/Corequisite – MAC108

Textbook

"Cryptography Decrypted" by H. X. Mel, Doris M. Baker, Doris M. Baker, Doris M. Baker, 1st edition. Publisher: Addison Wesley, ISBN – 9780201616477.

Instructional Objectives

1. Introduce students to the history of cryptography and substitution and transposition concepts.
2. Familiarize students with block cyphers: DES, 3DES and AES.
3. Familiarize students with public key encryption, RSA in particular.
4. Introduce students to message digests, hashes, digital signatures and digital certificates.
5. Familiarize students with PGP and e-mail security.
6. Introduce SSL and IPSec.

Performance Objectives

Upon completion of this course students should:

1. Describe how substitution and transposition work. Use substitution and transposition ciphers to encrypt/decrypt a message.
2. Explain how DES, 3DES and AES work. Use these ciphers to encrypt/decrypt a message.

3. Describe how keys are generated in RSA. Generate public/private keys and use them to encrypt/decrypt a message.
4. Explain message digest and hash and how they are used in authentication and integrity. Create a digital signature.
5. Describe how PGP works, use digital certificate to send an encrypted/signed e-mail.
6. Explain how SSL and IPSec work.

Grading Guidelines

A-, A	90-100
B-, B, B+	80-89
C-, C, C+	70 – 79
D-, D, D+	60 – 69
F	Below 60
WU	Unofficial Withdrawal (Students who have stopped attending at any time before the final exam week, and did not officially withdraw will receive this grade)

Grading Standards

CATEGORY	PERCENTAGE
Labs (10 @ 6.25% each)	50%
Midterm Exam	20%
Final Exam	30%
Total	**100%**

ACADEMIC INTEGRITY

This class will be conducted in compliance with LaGuardia Community College's academic integrity policy.

ATTENDANCE

The maximum number of unexcused absences allowed is 15% of the total class meetings (about 7 hours). Unexcused absences beyond this maximum will result in a grade of WU or F.

COMMENTS

The grading standards listed above, and the suggested homework problems listed in the course outline are both subject to modification by the instructor.

For more details about the academic requirements and grading policy, see the following link: https://www.laguardia.edu/uploadedFiles/Main_Site/Content/Academics/Catalog/PDFs/AcademicRequirementsAndPolicies.pdf

Weekly Topics

Week	Lecture Topics	Labs
1	Locks and keys. Cryptographic terms. Substitution and Caesar's Cipher.	Caesar's Cipher.
2	Transposition Ciphers. Combining Substitution and Transposition.	Substitution and Transposition Ciphers.
3	Diffuse and Confuse DES Cipher.	DES, 3DES Ciphers.
4	Secret Key Assurances Confidentiality, Authentication, Integrity using MAC.	Message integrity using MAC
5	Secret Key Exchange and its problems. Key Distribution Center, Introduction to Public Key Cryptography	Generating private/public keys using OpenSSL.
6	Confidentiality using Public Keys Distribution of Public Keys.	Using public/private keys to encrypt/decrypt messages.
7	Making Public Keys, Math Tricks.	Midterm Exam
8	Creating Digital Signatures using Private Key. Authentication and Integrity Using Private and Secret Keys. RSA, DSA.	Creating Digital Signatures. Verify Integrity and Authenticity of Message.
9	Message Digest Assurances. Non-keyed and keyed message digests. Comparing Secret Key, Public Key, and Message Digests.	Creating message digests.

10	Digital Certificates. Verifying a Digital Certificate. Issuer Authentication. X.509 Public Key Infrastructure.	Getting your first Public Key
11	Pretty Good Privacy (PGP), E-mail security.	Create a PGP message.
12	Secure Socket Layer, IPSec	Final Exam