COURSE SYLLABUS

CRYPTOGRAPHY

IFSA-Butler Reimagining Europe Semester Program in Prague

Suggested US semester credit hours: 4 credits
Contact Hours: 60
Course Level: 300
IFSA-Butler course code: CS380-32
Course length: Semester
Delivery method: Face to face
Language of Instruction: English

COURSE DESCRIPTION

This unit introduces students to the history of encryption (Roman, Napoleon, Enigma, etc.) understanding the building blocks for methods which are used today: permutation, substitution, Fermat's little theorem combined with understanding “what went wrong,” which were the flaws of older techniques which brought them their demise. This unit presents to the students the modern encryption system based on symmetric and asymmetric methods as well as the current algorithms: DES (though deprecated, it is the root of many older methods), 3 DES, AES, EI Gamal and Diffie-Hellman, RSA, Elliptic Curve.

This unit also contains a practical part which means implementing cryptography for two popular systems: data communication between end users and network communication.

STUDENT LEARNING OBJECTIVES

Students who successfully complete this course will:

- Understand the principles of cryptography and its inherent vulnerabilities if not properly applied
- Understand the advantages, disadvantages, strengths and weaknesses of current cryptographic methods
- Be able to analyze and decide which encryption mechanisms to use in an environment
- Be able to encrypt files with current and open source systems (VeraCrypt)
- Be able to deploy end-to-end communication (email, data) without the existence of a Certification Authority (PGP), with the existence of off-site and free to use Certification Authority (CACert, Comodo, Let's Encrypt) and with the existence of an on-site Certification Authority (based on Windows Server or Unix: MacOS/Linux sytem)
- Strengthen critical thinking skills
- Become familiar with resources available for further research on cryptography

- Make cognitive connections between learning in this course and other learning experiences in the IFSA-Butler Reimagining Europe Semester Program in Prague

PREREQUISITE KNOWLDEGE

- Good knowledge of high school mathematics (algebra and geometry in particular)
- Basic knowledge of networking

COURSE DELIVERY

Students are expected to read or view resources in advance and be prepared to actively discuss them in class. In each meeting, the instructor will overview the topic and then facilitate a group discussion, drawing out relevant themes, following up on specific lines of inquiry, and prompting students' thoughtful engagement with the topic. Students are encouraged to bring their prior learning experiences into class discussions and to make cognitive connections between this course and others in the IFSA-Butler Reimagining Europe Semester Program in Prague whenever possible. Theories of experiential learning and integrative learning therefore undergird the dynamic learning environment of this course.

This course utilizes an interactive approach to teaching that focuses on the individual student's needs. This approach to teaching and learning aims to foster a challenging but caring environment that allows students to explore, create, and test themselves and their ideas in a safe place.

COURSE SCHEDULE

15 weeks	**Content Delivery**
1	History of cryptographic methods: XOR, Roman, Napoleon, Enigma, base steps, complexity analysis
2-3	Block cypher, flow cypher, modern methods
4-5	Symmetric and asymmetric methods
6	Algorithms: DES, 3DES, AES, RSA, ECP, DH, EG
7	Inherent vulnerabilities
8	PGP, properties, implementation of PGP for email and messaging
9	Implement PKI with CACert for encryption
10	Implement PKI with CACert for digital signature
11	Implement PKI with CACert for device authentication

12	Implement PKI with Comodo for email encryption and signature
13	Implement Certification Authority with Windows Server
14	Implement Certification Authority with MacOS
15	Use the CA in a business environment

EVALUATION METHODS

The course instructor will determine specific assignments (including paper topics), projects, and exams for the course. Your work on individual assignments and projects will be guided by grading rubrics provided by the course instructor. Your final grade in the course will be arrived at through assessment methods determined by the course instructor and according to the percentages attached to each assignment and exam by the course instructor. Participation will constitute a determined percentage of your grade. Participation includes attendance, preparation, and engagement in discussion, civility, and respect.

Assignment Number	Type of Assignment	Description and Areas Assessed
1	Survey article	History of cryptography and its links to current methods
2	Technical report, team work	Case study
3	In class activity	Case study

Timely Submissions

Assignments submitted after the deadline will be accepted at the discretion of the course instructor and generally only in the event of a documented illness or emergency.

READING LIST

Martin, K. (2012). Everyday Cryptography: Fundamental Principles and Applications. UK: Oxford.

Stallings, W. (2013). Cryptography and Network Security: Principles and Practice. UK: Pearson.

ACADEMIC INTEGRITY

Any academic endeavor must be based upon a foundation of honesty and integrity. Students are expected to abide by principles of academic integrity and must be willing to bear individual responsibility for their work while studying abroad. Any academic work (written or otherwise) submitted to fulfill an academic requirement must represent a student‘s original work. Any act of academic misconduct, such as cheating, fabrication, forgery, plagiarism, or facilitating academic dishonesty, will subject a student to disciplinary action.

IFSA-Butler takes academic integrity very seriously. Students must not accept outside assistance without permission from the instructor. Additionally, students must document all sources according to the instructions of the professor. Should your instructor suspect you of plagiarism, cheating, or other forms of academic dishonesty, you may receive a failing grade for the course and disciplinary action may result. The incident will be reported to the IFSA-Butler resident director as well as your home institution.