BIRZEIT UNIVERSITY

Faculty of Engineering and Technology
ENCS, Computer Systems Engineering
First Semester 2021/2022

SYLLABUS

Course number and name: ENCS4320, Applied Cryptography

Credits and contact hours: Credit: 3 (Lecture: 3, Lab.: 0)

Instructor's or course coordinator's name:

- Dr. Ahmad Alsadeh: Office: Masri215, email: asadeh@birzeit.edu
- Mr. Hanna Alzughbi: halzughbi@birzeit.edu
- **Office hours**: please check Rritaj

Textbook:

- A Graduate Course in Applied Cryptography (V 0.5) by D. Boneh and V. Shoup
- Introduction to Modern Cryptography (2nd edition) by J. Katz and Y. Lindell.
- **Reference**:
- William Stallings. "Cryptography and Network Security: Principles and Practice", 6/E, Pearson, 2014, ISBN-10: 0133354695. http://williamstallings.com/Cryptography/

Specific course information

- **Description**: Cryptographic primitives and how they are applied within security systems, number theory foundations, finite fields, brief overview of classical cryptographic algorithms, symmetric-key encryption algorithms, Stream ciphers, Block cipher modes of operation, secure hash algorithms, message authentication codes, asymmetric ciphers, digital signatures, public key infrastructure, pseudorandom number generation, and design of cryptographic protocols, such as user authentication protocols.

- **Prerequisites:**
  - COMP233: Discrete Mathematics
  - COMP133: Computer programming
- Core course for Computer Engineering

Specific goals for the course

Upon the successful completion of this course, a student should:

- be familiar with basic and classical encryption techniques.
- be familiar with network security threats and countermeasures.
- understand theory of fundamental cryptography, encryption and decryption algorithms.
- apply the encryption algorithms.
- analyze network security protocols.

(ABET) Relationship of course to Computer Engineering Program Student Outcomes:

- (**a**): Ability to apply mathematics, science and engineering principles.
- (**e**): Ability to identify, formulate and solve engineering problems.
- (**k**): Ability to use the techniques, skills and modern engineering tools necessary for engineering practice.

Brief list of topics to be covered (Tentative)

Week	Topic
1	Course Overview What is cryptography
2	Classical Encryption Techniques • Caesar Cipher • Vigener cipher • Rotor Machines • Discrete probability
3	Stream Cipher • Information theoretic security and the one time pad • Stream ciphers and pseudo random generators • Attacks on stream ciphers and the one time pad • Real-world stream ciphers • PRG Security Definitions • Semantic Security
4	Block Ciphers • What are block ciphers- • The Data Encryption Standard • Exhaustive search attacks • More attacks on block ciphers • The AES block cipher • Block ciphers from PRGs
5	Using Block Ciphers • Review- PRPs and PRFs • Modes of operation- one time key • Security for many-time key • Modes of operation- many time key (CBC) • Modes of operation- many time key (CTR)
6	Message integrity • Message Authentication Codes • MACs Based On PRFs • CBC-MAC and NMAC • MAC padding • PMAC and the Carter-Wegman MAC
7	Collision Resistance • Generic birthday attack • The Merkle-Damgard Paradigm • Constructing compression functions • HMAC • Timing attacks on MAC verification
8	Authenticated Encryption • Active attacks on CPA-secure encryption • Definitions • Chosen ciphertext attacks • Constructions from ciphers and MACs • Case study- TLS • CBC padding attacks • Attacking non-atomic decryption

Midterm	
10	Odds and ends • Key Derivation • Deterministic Encryption • Deterministic Encryption-SIV and wide PRP • Tweakable encryption • Format preserving encryption
11	Key exchange • Trusted 3rd parties • Merkle Puzzles • The Diffie-Hellman protocol • Public-key encryption
12	Intro. Number Theory • Notation • Fermat and Euler • Modular e-'th roots • Arithmetic algorithms • Intractable problems
13, 14	Public Key Encryption from trapdoor permutations • Definitions and security • Constructions • The RSA trapdoor permutation • PKCS 1 • Is RSA a one-way function • RSA in practice
15	Public key encryption from Diffie-Hellman • The ElGamal Public-key System • ElGamal Security • ElGamal Variants With Better Security • A Unifying Theme • Farewell

Grading (Tentative):

- Homework assignments 20%
- Quizzes (~3) 15%
- Midterm Exam 25%
- Final Exam 40%

Policies:

- No late submissions will be accepted.
- Class attendance is required by the university regulations. Come to **All** lectures and activities.
- Make-up will be allowed only for students who miss the final exam with an acceptable excuse according to the university regulations.
- All students are expected to comply with University rules and regulations on academic Integrity and honesty.