ENCS5322 — Network Security Protocols

Birzeit University
ENCS, Computer Engineering
First Semester 2024/2025

Instructor:	Dr. Ahmad Alsadeh	**Time:**	S, M, W 09:00 - 09:50
Email:	asadeh@birzeit.edu	**Room:**	Aggad221

Course Description: Network and distributed systems security threat model, TCP/IP security attacks, Authentication protocols, Kerberos, e-mail security, Transport Layer Security (TLS), IPsec, Internet Key Exchange (IKE), Domain Name System security (DNSSEC), WLAN security, Cellular network security and Routing Security. Other topics; anonymity and privacy, electronic-identity (single sign on), Remote electronic voting.

Course Page: Please check Ritaj. `https://ritaj.birzeit.edu`

Office Hours: Check Ritaj, or by appointment, or send your questions by email.

Recommended Readings:

- **Mark Stamp**, *Information Security: Principles and Practice.* 3rd Edition, John Wiley & Sons. 2021
- **Wenliang Du**, *Computer & Internet Security: A Hands-on Approach, 2019*
- **William Stallings**, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Prentice Hall, 2020
- RFCs and standards

Objectives: After successful completion of this course, the students should:

- understand the different security goals and how they can be achieved by means of cryptography.
- know cryptographic mechanisms: encryption, data authentications, entity authentication, digital signatures
- understand protocols for key agreement and PKI
- able to identify and investigate network threats
- understand how these basic cryptographic mechanisms are used in several modern applications:
  - Internet security mechanisms (SSL/TLS, IPsec)
  - Email security
  - WLAN Security (WEP, WPA)
  - Cellular security (GSM Security & pitfalls)
- analyze and design network security protocols
- conduct research in network security

Prerequisites: An undergraduate-level understanding of probability, statistics, computer network, and programming languages (C/C++/Java) is needed.

Tentative Course Outline:

01: Threats and goals for Network Security
02: Replay a freshness and Classical Protocol flaws
03: Diffie-Hellman and Goals of Authenticated Key Exchange
04: TLS1.3 and QUIC
05: IPsec and IKEv2
06: Kerberos
07: Firewalls
08: WLAN Security: WPA2, WPA3
09: Bluetooth security
10: Cellular network security (GSM Security)
11: Virtual private networks

Grading Policy (Tentative):

Project	(25%)
Term paper	(20%)
Midterm	(20%)
Final Exam	(35%)

Class Policy:

- Regular attendance is essential and expected.
- Make-up will be allowed only for students who miss the final exam with an acceptable excuse according to the university regulations.

Academic Honesty: Lack of knowledge of the academic honesty policy is not a reasonable explanation for a violation. All students are expected to comply with University rules and regulations on academic Integrity and honesty.