Modern cryptography provides algorithms and protocols for protecting honest parties from distrusted or malicious parties that can eavesdrop to communication or modify it. Basic topics in cryptography include secure encryption, digital signatures, and authentication. In this course we will discuss these topics, their realizations, and applications. We will cover some background in number theory that is necessary to understand modern cryptosystems such as RSA.

Topics:

1. Classical encryption systems and perfect encryption systems
2. Symmetric encryption, DES, AES
3. Cryptographic hash functions and authentication
4. Number theory background
5. Public encryption, RSA, and ElGamal encryption systems
6. Digital signatures
7. Cryptographic protocols, e.g., SSL, IPsec, bitcoin, and secure multiparty computation

Books:


Notes:

- Final exam. Students MUST PASS the exam to pass the course.
- Homework assignments. There will be about 5 homework assignments.
- Final grade: If Exam < 65 then Exam else 0.8*Exam+0.2*Homework.

http://www.cs.bgu.ac.il/~crypt171/