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. The material covers cryptosystems that are both practical and theoretically interesting. To achieve this goal, we'll also teach 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. Introduction to number theory background
4. Public encryption, RSA, and ElGamal encryption systems
5. Digital signatures
6. Cryptographic hashing and authentication
7. Secret sharing, private information retrieval, differential privacy and introduction to secure computation.

Additional topics may be covered in the course.

ספרות הקורס