CO 487/687 Applied Cryptography

Instructor: Douglas Stebila

Cryptography is concerned with the mathematical, algorithmic, and implementational aspects of information security. It is one of the core technologies for securing the emerging information infrastructure. Its applications range from (conceptually) simple tasks such as encryption, authentication, and key management to sophisticated tasks such as Internet security, electronic cash payments, and electronic voting.

This course is a comprehensive introduction to modern cryptography that is aimed primarily at those interested in applications. The topics discussed will include an introduction to classical cryptography: encryption algorithms, hash functions, and message authentication codes. In the area of public-key cryptography, topics will include an overview of specific systems (Diffie--Hellman, RSA, DSA, etc.) and a few advanced protocols. The security of these schemes and the use of public-key techniques for generating digital signatures will be described. An emphasis will be placed on tools that are currently being used to secure the Internet and enable secure electronic commerce.

Topics to be covered will be drawn from the following partial list.

- *Symmetric-key encryption*: Classical ciphers, one-time pad, stream ciphers (RC4), Feistel networks, DES, AES, modes of operation.
- *Hash functions and data integrity*: Hash functions (SHA-1, SHA-2), parallel collision search, message authentication codes (CBC-MAC, HMAC).
- *Authenticated encryption*: Encrypt-then-MAC, AES-GCM.
- *Public-key encryption*: RSA, ElGamal, Elliptic curves, Post-quantum.
- *Signature schemes*: RSA, DSA, ECDSA, Post-quantum.
- *Key establishment*: Diffie--Hellman key exchange.
- *Key management*: Certification authorities, public-key infrastructures.
- *Deployed cryptography*: IEEE 802.11 WEP, IEEE 802.11 WPA2, Secure Sockets Layer (SSL) / Transport Layer Security (TLS), cryptocurrencies (Bitcoin), Fast IDentity Online (FIDO), Signal protocol (WhatsApp), privacy-enhancing technologies (Tor, OTR), Pretty Good Privacy (PGP).

Suggested reading:

- C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2009. Available as a free download from the university library website: https://ocul-wtl.primo.exlibrisgroup.com/permalink/01OCUL_WTL/156lh75/springer_s978-3-642-04101-3_159109
- D. Stinson, *Cryptography---Theory and Practice*, 4th edition, CRC Press, 2006.

Prerequisites:

- Elementary number theory. Some exercises will involve basic programming in either Python or a language of your choice.