MATH 3094 - SPRING 2018
MATHEMATICS OF ENCRYPTION

Modern cryptography lies at the intersection of mathematics and computer science, involving number theory, algebra, algorithmic complexity, and potentially quantum mechanics. Many people think of codes in terms of spies, but in the information age, highly mathematical codes are used every day by almost everyone, whether at the bank ATM, at the supermarket, or when you send a text or purchase products online. Here is the same message encrypted in four different ways:

GUVF PBHEFR VF NJRFBZR (Caesar cipher)

DLGC GMEVQO MQ KACCSKO (Vigenère cipher)

OPGN NKLT KCBA BUSD ZDO (Enigma machine)

408 917 591 951 578 323 532 369 919 951 171

578 591 951 578 1010 754 171 951 532 508 171 (RSA, modulus 1073, public key 3)

This course will provide a historical and mathematical tour of cryptography, from classical ciphers to quantum cryptography. The topics will include: classical ciphers (e.g., Caesar and Vigenère ciphers) and the attacks on them, the Enigma system, public-key RSA (including a complete mathematical proof that it works), detecting and correcting errors, primality testing and digital signatures, and elliptic curve cryptography (if time permits).

Prerequisites: MATH 3240 (Intro. to Number Theory) or instructor consent to substitute MATH 3240 by CSE 2500 (or a strong grade in 2710). Enrollment requires instructor permission.

Questions? Email the instructor, Álvaro Lozano-Robledo, at `alvaro@uconn.edu`.