Aims:
Understanding how cryptography and security works in practice, and how it fails. Understanding attacks and vulnerabilities of major industrial standards. Study of real-life applications of encryption, Message Authentication Codes (MACs) and Digital Signatures in areas of telecom, government/identity, buildings/transportation, payment and crypto currency systems. Study of selected topics in cryptanalysis. Understanding the maths, the security design principles, the internal structure and important properties of major cryptosystems. Side channel attacks and countermeasures.

Learning outcomes:
Learning how security problems are solved in the industry, and understanding why specific choices are made. Understanding multiple ways to attack and defend in applied cryptography. Understanding the role of keyed operations, non-linearity, randomness, one-wayness, diffusion, side-channel vulnerabilities, permutations, security reductions, etc in cryptographic engineering. Understanding fraud crime and attacks in payment systems. Study or practical applications of digital signatures in electronic commerce, TLS and crypto currency. Understanding security (attacks and defences) in complex real life systems and the role of keys, cryptographic algorithms and protocols, tamper resistant hardware and other types of countermeasures. Understanding different types of attacks (e.g. key recovery vs. decryption) and different security definitions.

Content:
The module covers the following:
- Symmetric cryptography. Historical cryptanalysis since WW2 and Enigma. Block ciphers. Structural high-level and self-similarity attacks. Differential cryptanalysis, linear cryptanalysis, software and algebraic cryptanalysis;
- Groups, finite fields. Number theory. Attacks on public key cryptosystems. RSA, factoring, discrete logarithms;
- Public key cryptography. Elliptic Curve crypto and digital signatures;
- Secure email/messaging, digital signatures, certificates. Electronic commerce, SSL/TLS, Forward Security, attacks on TLS;
- Smart cards and cryptographic protocols. RFID technology, data and entity authentication, challenge-response. EMV Bank cards and terminals, security, fraud, attacks. E-passports;
- Hardware Security and Side-channel attacks (timing, SPA, DPA and DFA). Side-channel attack countermeasures;
- Financial cryptography, payment systems, blockchains and crypto currencies;

Labs:
Exercises and programming with Sage Maths. Optional crypto implementation, crypto wallets and blockchain data exploration labs and projects;

Requisites:
In order to be eligible to select this module, a student must be registered on a programme for which it is a formally-approved option or elective choice.
Applied Cryptography and Cryptanalysis (COMP0058)

Description

Aims:
Understanding how cryptography and security works in practice, and how it fails. Understanding attacks and vulnerabilities of major industrial standards. Study of real-life applications of encryption, Message Authentication Codes (MACs) and Digital Signatures in areas of telecom, government/identity, buildings/transportation, payment and crypto currency systems. Study of selected topics in cryptanalysis. Understanding the maths, the security design principles, the internal structure and important properties of major cryptosystems. Side channel attacks and countermeasures.

Learning outcomes:
Learning how security problems are solved in the industry, and understanding why specific choices are made. Understanding multiple ways to attack and defend in applied cryptography. Understanding the role of keyed operations, non-linearity, randomness, one-wayness, diffusion, side-channel vulnerabilities, permutations, security reductions, etc in cryptographic engineering. Understanding fraud crime and attacks in payment systems. Study or practical applications of digital signatures in electronic commerce, TLS and crypto currency. Understanding security (attacks and defences) in complex real life systems and the role of keys, cryptographic algorithms and protocols, tamper resistant hardware and other types of countermeasures. Understanding different types of attacks (e.g. key recovery vs. decryption) and different security definitions.

Content:
The module covers the following:
-Symmetric cryptography. Historical cryptanalysis since WW2 and Enigma. Block ciphers. Structural high-level and self-similarity attacks. Differential cryptanalysis, linear cryptanalysis, software and algebraic cryptanalysis;
-Groups, finite fields. Number theory. Attacks on public key cryptosystems. RSA, factoring, discrete logarithms;

Key information

Year 2019/20
Credit value 15 (150 study hours)
Delivery UGM L7, Campus-based
Reading List View on UCL website
Tutor Dr Nicolas Courtois
Term Term 2
Timetable View on UCL website

Assessment

- Group project: 50%
- Written examination (departmentally managed): 50%

Find out more

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk
- Public key cryptography. Elliptic Curve crypto and digital signatures;
- Secure email/messaging, digital signatures, certificates. Electronic commerce, SSL/TLS, Forward Security, attacks on TLS;
- Smart cards and cryptographic protocols. RFID technology, data and entity authentication, challenge-response. EMV Bank cards and terminals, security, fraud, attacks. E-passports;
- Hardware Security and Side-channel attacks (timing, SPA, DPA and DFA). Side-channel attack countermeasures;
- Financial cryptography, payment systems, blockchains and crypto currencies;

Labs:
Exercises and programming with Sage Maths. Optional crypto implementation, crypto wallets and blockchain data exploration labs and projects;

**Requisites:**
In order to be eligible to select this module, a student must be registered on a programme for which it is a formally-approved option or elective choice.