Introduction to Cryptography (COMP0025)

Description

Aims:
For many centuries the goal of cryptography was the protection of privacy of communications. Computers, digital communication and in particular the internet have brought an abundance of new security goals. Examples are: anonymity, authenticity, non-repudiation, authorized wiretapping (called law enforcement), and traceability. To each need corresponds security mechanisms to achieve it. The goal of the course is to make students familiar with such techniques and some of the foundations of these methods. In particular students will be confronted with a range of security objectives, different levels of security that can be achieved and some available cryptographic techniques that can be used.

Learning outcomes:
On successful completion of the module, a student will be able to:
1. Model security precisely and formally in terms of adversarial objective and system access;
2. Explain and reason about basic cryptographic tools to protect and authenticate data;
3. Suggest security parameters that protect against standard attacks;
4. Read scientific articles and international standards in the field of cryptography;

Content:
Classical ciphers:
- Cryptanalysis of classical ciphers;
- Probability theory;
- Perfect security; Block ciphers:
  - DES;
  - AES;
- Block cipher modes of operation; Private-key encryption:
  - Chosen plaintext attacks;
  - Randomised encryption;
  - Pseudorandomness;
  - Chosen ciphertext attacks;

Key information

Year: 2019/20
Credit value: 15 (150 study hours)
Delivery: UG L6, Campus-based
Reading List: View on UCL website
Tutor
Term: Term 1
Timetable: View on UCL website

Assessment

Find out more

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk

Disclaimer: All information correct as of June 2019. Please note that aspects of the module may be subject to change. UCL will make best efforts to inform applicants of major changes.
Message authentication codes:
- Private-key authentication;
- CBC-MAC;
- Pseudorandom functions;
- CCA-secure private-key encryption;

Hash functions:
- Integrity;
- Pre-image resistance;
- Collision-resistance;
- SHA-256;
- NMAC/HMAC;

Key distribution:
- Key distribution centres;
- Modular arithmetic and group theory;
- Diffie-Hellman key exchange;

Public-key Distribution:
- ElGamal encryption;
- Cramer-Shoup encryption;
- Discrete logarithm problem;

Digital Signatures:
- RSA signatures;
- RSA-FDH and RSA-PSS signatures;
- DSA signatures;
- 509 certificates;
- Certification paths;

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 AND must have EITHER (i) passed BSc/ MEng Computer Science (Years 1 and 2) at UCL; OR (ii) passed MEng Mathematical Computation (Years 1 and 2) at UCL; OR (iii) be registered on a Taught Postgraduate programme and have completed a module in mathematics or probability theory at FHEQ Level 6 (or higher).

The module is theoretically and mathematically demanding.
Introduction to Cryptography (COMP0025)

Description

Aims:
For many centuries the goal of cryptography was the protection of privacy of communications. Computers, digital communication and in particular the internet have brought an abundance of new security goals. Examples are: anonymity, authenticity, non-repudiation, authorized wiretapping (called law enforcement), and traceability. To each need corresponds security mechanisms to achieve it. The goal of the course is to make students familiar with such techniques and some of the foundations of these methods. In particular students will be confronted with a range of security objectives, different levels of security that can be achieved and some available cryptographic techniques that can be used.

Learning outcomes:
On successful completion of the module, a student will be able to:
1. Model security precisely and formally in terms of adversarial objective and system access;
2. Explain and reason about basic cryptographic tools to protect and authenticate data;
3. Suggest security parameters that protect against standard attacks;
4. Read scientific articles and international standards in the field of cryptography;

Content:
Classical ciphers:
- Cryptanalysis of classical ciphers;
- Probability theory;
- Perfect security; Block ciphers:
  - DES;
  - AES;
  - Block cipher modes of operation; Private-key encryption:
    - Chosen plaintext attacks;
    - Randomised encryption;
    - Pseudorandomness;
    - Chosen ciphertext attacks;

Key information

Year
2019/20
Credit value
15 (150 study hours)
Delivery
PGT L7, Campus-based
Reading List
View on UCL website
Tutor

Term
Term 1
Timetable
View on UCL website

Assessment

- Written examination (main exam period): 75%
- Coursework: 25%

Find out more

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk

Disclaimer: All information correct as of June 2019. Please note that aspects of the module may be subject to change. UCL will make best efforts to inform applicants of major changes.
Message authentication codes:
- Private-key authentication;
- CBC-MAC;
- Pseudorandom functions;
- CCA-secure private-key encryption;

Hash functions:
- Integrity;
- Pre-image resistance;
- Collision-resistance;
- SHA-256;
- NMAC/HMAC;

Key distribution:
- Key distribution centres;
- Modular arithmetic and group theory;
- Diffie-Hellman key exchange;

Public-key Distribution:
- ElGamal encryption;
- Cramer-Shoup encryption;
- Discrete logarithm problem;

Digital Signatures:
- RSA signatures;
- RSA-FDH and RSA-PSS signatures;
- DSA signatures;
- 509 certificates;
- Certification paths;

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 AND must have EITHER (i) passed BSc/MEng Computer Science (Years 1 and 2) at UCL; OR (ii) passed MEng Mathematical Computation (Years 1 and 2) at UCL; OR (iii) be registered on a Taught Postgraduate programme and have completed a module in mathematics or probability theory at FHEQ Level 6 (or higher).

The module is theoretically and mathematically demanding.
Introduction to Cryptography (COMP0025)

**Description**

**Aims:**
For many centuries the goal of cryptography was the protection of privacy of communications. Computers, digital communication and in particular the internet have brought an abundance of new security goals. Examples are: anonymity, authenticity, non-repudiation, authorized wiretapping (called law enforcement), and traceability. To each need corresponds security mechanisms to achieve it. The goal of the course is to make students familiar with such techniques and some of the foundations of these methods. In particular students will be confronted with a range of security objectives, different levels of security that can be achieved and some available cryptographic techniques that can be used.

**Learning outcomes:**
On successful completion of the module, a student will be able to:
1. Model security precisely and formally in terms of adversarial objective and system access;
2. Explain and reason about basic cryptographic tools to protect and authenticate data;
3. Suggest security parameters that protect against standard attacks;
4. Read scientific articles and international standards in the field of cryptography;

**Content:**
Classical ciphers:
- Cryptanalysis of classical ciphers;
- Probability theory;
- Perfect security; Block ciphers:
- DES;
- AES;
- Block cipher modes of operation; Private-key encryption:
- Chosen plaintext attacks;
- Randomised encryption;
- Pseudorandomness;
- Chosen ciphertext attacks;

**Key information**

<table>
<thead>
<tr>
<th>Year</th>
<th>2019/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit value</td>
<td>15 (150 study hours)</td>
</tr>
<tr>
<td>Delivery</td>
<td>UGM L7, Campus-based</td>
</tr>
<tr>
<td>Reading List</td>
<td>View on UCL website</td>
</tr>
<tr>
<td>Tutor</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Term 1</td>
</tr>
<tr>
<td>Timetable</td>
<td>View on UCL website</td>
</tr>
</tbody>
</table>

**Assessment**

**Find out more**

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk

Disclaimer: All information correct as of June 2019. Please note that aspects of the module may be subject to change. UCL will make best efforts to inform applicants of major changes.
Message authentication codes:
- Private-key authentication;
- CBC-MAC;
- Pseudorandom functions;
- CCA-secure private-key encryption;

Hash functions:
- Integrity;
- Pre-image resistance;
- Collision-resistance;
- SHA-256;
- NMAC/HMAC;

Key distribution:
- Key distribution centres;
- Modular arithmetic and group theory;
- Diffie-Hellman key exchange;

Public-key Distribution:
- ElGamal encryption;
- Cramer-Shoup encryption;
- Discrete logarithm problem;

Digital Signatures:
- RSA signatures;
- RSA-FDH and RSA-PSS signatures;
- DSA signatures;
- 509 certificates;
- Certification paths;

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 AND must have EITHER (i) passed BSc/MEng Computer Science (Years 1 and 2) at UCL; OR (ii) passed MEng Mathematical Computation (Years 1 and 2) at UCL; OR (iii) be registered on a Taught Postgraduate programme and have completed a module in mathematics or probability theory at FHEQ Level 6 (or higher).

The module is theoretically and mathematically demanding.