COMPUTER SECURITY AND DATA PROTECTION

INF/01 - 6 CFU - 1° semestre

Docente titolare dell’insegnamento

DARIO CATALANO
Email: catalano@dmi.unict.it
Edificio / Indirizzo: viale A. Doria 6
Telefono: 0957383030
Orario ricevimento: Lunedì dalle 10 alle 12

OBIETTIVI FORMATIVI

Nowadays data controllers must design information systems that provide the highest possible privacy guarantees. A fundamental enabler to achieve this is cryptography.

This class is intended to provide an introduction to the main concepts of modern cryptography and their usage to protect data and build secure systems. The main focus will be on constructions of various building blocks, such as encryption schemes, message authentication codes and digital signatures. We will try to understand what properties we expect from these objects, how to define these properties and how to construct schemes that realize them. We will also focus on schemes that are widely used in practice. These include, for instance, AES, SHA, HMAC and RSA. However, rather than using these tools as black box, we will show how they are built and the security level they provide. No programming will be required for this class.

The goals of this course, in terms of expected results, are

1. **Knowledge and understanding (Conoscenza e capacità di comprensione).** Students will learn the fundamental ideas and principles underlying modern cryptography and modern secure systems.
2. **Applying knowledge and understanding (Capacità di applicare conoscenza e comprensione).** On completion, the student will be able to securely use cryptographic tools like encryption schema and digital signatures and to understand their exact role in secure systems.
3. **Making judgements (Autonomia di giudizio).** By studying concrete examples and common mistakes students will learn how to use solutions that provide high security guarantees.
4. **Communication skills (Abilità comunicative).** On completion, students will acquire communication skills that will allow them to fluently communicate using the technical language of computer security.
5. **Learning skills (Capacità di apprendimento).** On completion, students will acquire methodologies that will allow them to securely deal with problems that require the usage of secure solutions.
MODALITÀ DI SVOLGIMENTO DELL'INSEGNAMENTO

Lecture based (via slides).

Should teaching be carried out in mixed mode or remotely, it may be necessary to introduce changes with respect to previous statements, in line with the programme planned and outlined in the syllabus.

PREREQUISITI RICHIESTI

Basics of Discrete math
Basics of Algorithms

FREQUENZA LEZIONI

Not mandatory but strongly suggested

CONTENUTI DEL CORSO

Introduction to the main ideas of this class.
Source: Cap 1 from [1]

Source: Cap 2 from [1]

Block Ciphers – AES The blockcipher Rijndael. Pseudorandom functions and relations to block ciphers. AES in practice. Birthday Paradox.
Source: Cap 3,4 from [1]

Symmetric encryption: Modes of operation. ECB, CBC$, CTRC and CTR$. Security notions for symmetric encryption.
Source: Cap 5 from [1]

Integrity and Hash functions. Collision resistant hash functions. Generic attacks to collision resistance. SHA3.
**Message Authentication.** Notion of security for MACs. The PRF as a MAC paradigm. CBC-MAC. HMAC.

Source: Cap 7 from [1]

**Intro to asymmetric cryptography.** One way functions and Trapdoor (one-way) functions. Number theory basics. Discrete logarithms. Computation Diffie Hellman problem and Key Exchange. Factoring and RSA.

Source: Cap 9, 10 from [1], relevant parts from [2]

**Asymmetric encryption.** Notions of security for asymmetric cryptosystems. The El-Gamal encryption scheme. Homomorphic Encryption (basics). RSA-OAEP.

Source: Cap 11 from [1] and slides

**Digital Signatures.** A notion of security for digital signatures. The Hash then invert paradigm for digital signatures. Digital Signatures in practice.

Source: Cap 12 from [1].

**Bonus Application:** Bitcoin

Source: Slides and Chapter 2 of [4]

**TESTI DI RIFERIMENTO**


**ALTRO MATERIALE DIDATTICO**

https://catalano.dmi.unict.it/teaching/
PROGRAMMAZIONE DEL CORSO

<table>
<thead>
<tr>
<th>Argomenti</th>
<th>Riferimenti testi</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Some classical ciphers and their cryptanalysis. Perfect Security and One time pad.</td>
<td>Cap 2 from [1]</td>
</tr>
<tr>
<td>2 Block Cipher and AES</td>
<td>Cap 3,4 from [1]</td>
</tr>
<tr>
<td>3 Symmetric Encryption</td>
<td>Cap 5 from [1]</td>
</tr>
<tr>
<td>4 Integrity and Hash Functions</td>
<td>Cap 6 from [1]</td>
</tr>
<tr>
<td>5 Message Authentication</td>
<td>Cap 7 from [1]</td>
</tr>
<tr>
<td>6 Intro to Asymmetric Cryptography. One way Functions and Trapdoor Functions. Discrete Logarithms, Factoring and RSA.</td>
<td>Cap 9, 10 from [1], relevant parts from [2]</td>
</tr>
</tbody>
</table>

VERIFICA DELL'APPRENDIMENTO

MODALITÀ DI VERIFICA DELL'APPRENDIMENTO
The exam consists in a written test followed by an oral exam. The written test typically consists in 5 (open) questions.

To pass the written part one should get a minimum of 18.

Midterms: There might be the possibility of a midterm exam followed by a final exam. The midterm covers the part on asymmetric encryption whereas the final will be on PK cryptography and Bitcoin.

Learning assessment may also be carried out on line, should the conditions require it.

ESEMPI DI DOMANDE E/O ESERCIZI FREQUENTI
- Exercises on the crypto primitives (example: show that a given encryption scheme is not secure by providing an attack)
- Algorithms (ex: presenta and explain some of the algorithms studied in class)