CRYPTOGRAPHY

Co-funded by the Erasmus+ Programme of the European Union
Grant Agreement n°2019-1- IT02-KA203- 063184

The module aims to make the participants experience and analyse the interdisciplinarity between CS and Math in the context of Cryptography, a crucial topic in today's digital society that sits at the intersection of the two disciplines.

https://identitiesproject.eu/cryptography/

Modular blocks	Goals of the block	Activities	IDENTITIES approach to interdisciplinarity	Role of participants	Mode of interaction	Suggested digital tools	Workload time	Non-editable format	Editable format	Hints for implementation
Exploring historical and societal issues related to cryptography	Introduce the module and make the participants reflect informally on interdisciplinarity while sharing their previous knowledge of cryptography.	The participants introduce themselves and "break the ice" on interdisciplinarity and cryptography				Assignment	3 h	https://identitiesproject.eu/wp-content/uploads/2022/12/01-Introduction-and-Explorer-activities.pdf	https://identitiesproject.eu/wp-content/uploads/2022/11/ID-explorer.odp	
	Motivate the use of cryptography in today's society; make participants grasp the idea of e2e encryption and the complexity of the societal debate about backdoors; share a basic terminology for cryptography.	The participants watch two videos about end-to-end encryption				Assignment		https://www.youtube.com/watch?v=CINVwWHIzTY https://www.youtube.com/watch?v=jkV1KEJGKRA		Give the participants more time than the overall videos' duration to pause them if needed; suggest turning on subtitles if necessary; ensure a reliable Internet connection or download the videos in advance
	Show participants how Math and CS grew and intertwined in cryptography (beginning of the disciplinary projections) by making them read a piece on the history of cryptography.	The participants read a text about the birth of RSA				Assignment		https://identitiesproject.eu/wp-content/uploads/2022/12/02-Short-history-of-RSA.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/02-Short-history-of-RSA-1.odt	Instructions are in the previous presentation
	Make participants reflect on cryptography and interdisciplinarity	The participants reflect on the activities they experienced, guided by some open-ended questions				Survey / questionnaire		https://identitiesproject.eu/wp-content/uploads/2022/12/03-Explorer_-conclusive-questions.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/03-Explorer_-conclusive-questions.odt	It is possible to discuss collectively after the participants reflected for some time on the questions
Interdisciplinary activity, designed with the Theory of Didactical situations	Present main ideas and cryptographic schemes; introduce vocabulary and terminology	The participants participate in a presentation and interactive lecture on fundamental cryptography concepts				Assignment	3 h	https://identitiesproject.eu/wp-content/uploads/2022/12/04-Intro-to-crypto.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/04-Intro-to-crypto.odp	
	Explain how to do encryption in perfect dominating set cryptosystems using an example	The participants are introduced to how to encrypt a message using graphs				Jamboard		https://identitiesproject.eu/wp-content/uploads/2022/12/05-Intro-to-the-PDS-cryptosystem-ENCRYPTION.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/05-Intro-to-the-PDS-cryptosystem-ENCRYPTION.odp	The algorithm is made explicit in the document. Execute the algorithm on slide 2 (i.e. calculate the red and green values) interactively with participants. If there is time, ask participants to apply the encryption algorithm by themselves in order to understand it correctly. A collaborative tool to write on the graph would be ideal.
	Let participants: - experience an activity developed within the Theory of Didactical Situations (TDS) to be able to design a similar activity - understand and manipulate a public-key cryptosystem based on a hard problem - understand the notions of privacy, encryption, decryption, private and public keys, attack models - explore the notion of one-way-functions - experience computational complexity of a hard problem - explore the interdisciplinary nature of one-way-functions, graphs, complexity	The participants in groups try to decrypt a secret message				Jamboard		https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-A.pdf https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-B.pdf https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-C.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-A.odp https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-B.odp https://identitiesproject.eu/wp-content/uploads/2022/12/06-DECRYPTION-Group-C.odp	The participants are divided into three groups and work in parallel. They have the same task (decrypting an encrypted message). They can verify their solution by trying to open the provided treasure chest (at the end of the slides). Each group is given different information. Ideally, the activity is held face-to-face; anyway, it has to be synchronous, ideally with a tutor for each group. The most important aspect is the interaction between different participants in trying to decrypt the message. For Group C, the linear solver should only be given if the participants come up by themselves with the idea of using a system of equations. A collaborative tool to write on the graph would be ideal.
	Revise the three groups' different approaches, highlight different elements of Math and CS in the solutions	The participants present their results; instructors discuss the approaches and formalise some aspects of the activity (institutionalisation)				Assingment		https://identitiesproject.eu/wp-content/uploads/2022/12/07-Institutionalisation.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/07-Institutionalisation.odp	The discussion should be based on what happened in the different groups. Participants should be able to present (es. connecting their laptop or uploading a presentation to be shown with a projector).
Analyzing in terms of interdisciplinarity the previous learning activity	Introduce interdisciplinarity frameworks and the boundary metaphor	The participants watch divulgation videos about interdisciplinary frameworks				Assignment	2 h	https://www.youtube.com/playlist?list=PLMH8Z9BCUrxMyQHCYqaGJ6ICA6Qoop7Hk		
	Make participants analyse the previous experience from an interdisciplinary point of view in light of the presented frameworks and recognise the role of the disciplines and the type of interdisciplinarity emerged	The participants reflect on interdisciplinarity in activities they experienced, guided by some open-ended questions				Survey / questionnaire		https://identitiesproject.eu/wp-content/uploads/2022/12/08-Questions-about-interdisciplinarity.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/08-Questions-about-interdisciplinarity.odt	This can be the last activity in a short version of the module; in a longer one, the questions about interdisciplinarity can be spread out in the following activities. Reflection and discussion can be individual and/or led by the instructor
Analyzing and designing other teaching materials by leveraging on the previous analysis in terms of both the TDS and interdisciplinary frameworks	Provide participants with raw teaching material with interdisciplinary potential; let them explore the computational complexity of different algorithms, or how a function is easy to calculate but difficult to invert.	The participants explore individually "raw" teaching material that has the potential to be used to design interdisciplinary activities between CS and Math (inside and outside cryptography)				Assignment	3 h	https://identitiesproject.eu/wp-content/uploads/2022/12/09-Crypto-raw-teaching-material.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/09-Crypto-raw-teaching-material.odt	Introduce the materials briefly and then leave the participants explore them individually
	Make participants analyse the raw material in light of disciplinary projections and its interdisciplinary potential	The participants analyse in groups the teaching materials guided by some open questions				Assignment		https://identitiesproject.eu/wp-content/uploads/2022/12/10-Analysis-of-the-raw-teaching-material.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/10-Analysis-of-the-raw-teaching-material.odt	Understanding the material requires a (basic) programming background; each group should include participants with a CS/programming background Students can work on a collaborative text editor.
	Explain TDS, specifically referring to didactical variables	The participants follow a lecture about the Theory of Didactical Situations				Assignment		https://identitiesproject.eu/wp-content/uploads/2022/12/11-Theory-of-Didactical-Situation.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/11-Theory-of-Didactical-Situation.odp	
	Make participants design an interdisciplinary lesson between Math and CS based on the previous analysis and the TDS	The participants design an interdisciplinary learning activity				Assignment		https://identitiesproject.eu/wp-content/uploads/2022/12/12-Design-and-plan-a-lesson.pdf	https://identitiesproject.eu/wp-content/uploads/2022/12/12-Design-and-plan-a-lesson.odt	Students can work on a collaborative text editor.

CRYPTOGRAPHY

Co-funded by the Erasmus+ Programme of the European Union
Grant Agreement n°2019-1- IT02-KA203- 063184

The module aims to make the participants experience and analyse the interdisciplinarity between CS and Math in the context of Cryptography, a crucial topic in today's digital society that sits at the intersection of the two disciplines.

https://identitiesproject.eu/cryptography/

Modular blocks	Goals of the block	Activities	IDENTITIES approach to interdisciplinarity	Role of participants	Mode of interaction	Suggested digital tools	Workload time	Non-editable format	Editable format	Hints for implementation

Legend

Keywords for the IDENTITIES approach to interdisciplinarity

- Identities of the disciplines ● mathematics ■ physics ▲ computer science
- Interdisciplinarity zone
- Boundary objects
- Boundary-crossing mechanisms
- Epistemological activators
- Linguistic activators

Keywords for the participants' roles in the module

- Role of explorer
- Role of student
- Role of analyst
- Role of teacher-designer

Keywords for the type of participants' engagement in the activities

- Individual activity
- Group activity
- Interactive activity trainer-trainees