# Big Ideas of Cryptography

ACM SIGCSE Special Projects 2020 Final Report

MICHAEL LODI, MARCO SBARAGLIA, and SIMONE MARTINI, Università di Bologna, Italy

## 1 BACKGROUND

In today's digital society, cryptography is at the core of many activities and tools (e.g., instant messaging, e-commerce, stock exchange, cryptocurrency). Various frameworks (e.g., DigComp [2]) and curricula (e.g., CSTA K–12 CS Standards [5] and the UK computing curriculum [3]) include cybersecurity competencies. Some of them are more oriented on using security for personal purposes, others on understanding how digital security works, but they all recognize that cybersecurity skills are essential for students to be active citizens of digital society. Cryptography is one of the foundations of cybersecurity. In addition, novices identified cryptography "as an interesting context for computer science lessons" [6, p. 3]. K-12 education does not aim to train professionals but to help students understand our world and act in it, therefore it is important to help them understand the principles of cryptography and their importance in our society.

## 2 RESEARCH ACTIVITIES

We designed a short course with no prerequisites, built around different types of activities. Since educational research has shown the effectiveness of active and cooperative learning methodologies [10, p. 304], we designed non-traditional hands-on activities to be interactive and meaningful for students. We developed cryptography playgrounds for students to use, understand, and attack emblematic cryptosystems (e.g., Caesar cipher, One-time pad) and a "remote-unplugged" activity to perform the Diffie-Hellman (DH) key agreement in pairs. We realized both types of activities with Snap!, a visual block-based programming language. Due to the ongoing COVID-19 pandemic, we had to design the first iteration of our intervention as remote-only.

Our pathway includes a few emblematic cryptographic systems and schemes, carefully selected as representatives of cryptography core ideas. With the aim to create a motivating progression, the introduction of a new scheme is always triggered by the *necessity* (which we stimulate in students [11]) to overcome the limitations of the previous one(s).

### 2.1 Outputs

The project has two primary outputs.

(1) A learning progression to teach fundamental cryptography ideas by making students encounter some representative cryptosystems (from classical to modern) and experience their limitations, and consequently the necessity to overcome those limitations (towards more secure systems). The cryptography learning progression is presented at https://bigideascryptok12.bitbucket.io/#progression and discussed in [9].

(2) Teaching materials for 4/5 lessons (suitable for high school students) following the path of point 1, consisting of
  - ad-hoc Snap! environments to experience firsthand how relevant cryptosystems work, their weaknesses, and possible attacks (see fig. 1)
  - unplugged activities (which can also be used in remote teaching): for example, a Diffie-Hellman key agreement simulation through color mixing (with the mixing based on the actual math of the protocol) (see fig. 2)

Authors' address: Michael Lodi, michael.lodi@unibo.it; Marco Sbaraglia, marco.sbaraglia@unibo.it; Simone Martini, simone.martini@unibo.it, Dipartimento di Informatica - Scienza e Ingegneria, Università di Bologna, Mura Anteo Zamboni, 7, 40126, Bologna, Italy.

- animated slides showing the high-level functioning of asymmetric encryption scenarios step by step and a narrative evaluation summary

All materials are freely available at https://bigideascryptok12.bitbucket.io/#playgrounds

### 2.2 Outcomes

Students appreciated the course and felt that, despite being remote, it was fun and engaging. According to the students, the course helped them understand the role of cryptography, CS, and Math in the society and sparked their interest in cryptography and CS.

The “remote-unplugged” Diffie-Hellman, where the meeting chat was a metaphor for the public channel, engaged the students in understanding this groundbreaking protocol.

Overall, the students praised the activities as engaging, even when challenging. However, remote teaching induced strong “instructor blindness”, often preventing us from giving the students the right amount of guidance during the exploration activities.

The final assessment showed that the cryptography ideas addressed were well understood.

## 3 ONGOING AND FUTURE RESEARCH

This grant, for which we thank the SIGCSE Board, was the starting point for a broader line of research on teaching Cryptography.

### 3.1 Big ideas

We interviewed cryptography and CS education experts with the aim of distilling the "Big Ideas of Cryptography." The development of big ideas for K-12 education is currently underway, for example, for science education [4], more specifically for computer science education [1], artificial intelligence [12], and so on.

It is useful to distill the fundamental concepts of a topic in a way that is understandable to students and teachers who are not necessarily experts in that particular field so that these fundamental ideas can serve as "beacons" to guide teaching and learning.

While we are still analyzing the interview transcripts and planning more structured questionnaires to circulate among experts, many of the emerged ideas have been integrated into our learning progression (see 2.1) built around representative cryptosystems to teach the fundamental ideas of cryptography.

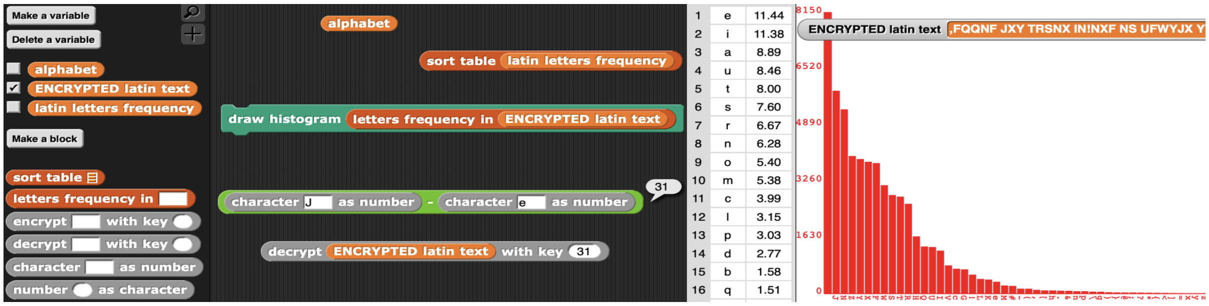
### 3.2 Course iterations

We tested our course two more times.

The second iteration was very similar to the first. The main difference was that the course was held face-to-face, in the same context, but during the following school year (with the new tenth graders). We added a lesson to get the students used to Snap! in a more gradual way. In addition, we dedicated an hour to modern asymmetric systems. Finally, homework was more creative and geared toward thinking about how to overcome the challenges cryptography has faced during its development. Preliminary results show that the students received the course even better, indicating its soundness and applicability in both online and face-to-face teaching.

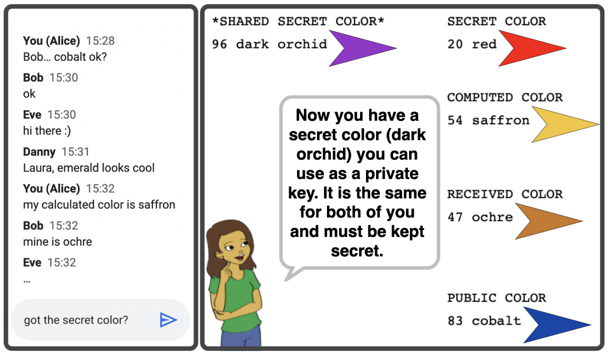
A third iteration took place in a different context, with more students from different school paths and ages (grades 11-12-13). The focus was on the interdisciplinarity between CS and Math, with longer lessons that also touched on topics such as modular arithmetic, probability, and discrete logarithms. Research is ongoing, also in the context of interdisciplinary teacher training under the Erasmus+ IDENTITIES Project[1].

[1] https://identitiesproject.eu/


Make a variable
Delete a variable
□ alphabet
☑ ENCRYPTED latin text
□ latin letters frequency
Make a block
sort table
letters frequency in
encrypt with key
decrypt with key
character as number
number as character
alphabet
sort table latin letters frequency
draw histogram letters frequency in ENCRYPTED latin text
character J as number - character e as number
31
decrypt ENCRYPTED latin text with key 31
ENCRYPTED latin text ,FQQNF JXY TRSNX IN!NXF NS UFWYJX Y
8150
6520
4890
3260
1630
0

| | | |
|---|---|---|
| 1 | e | 11.44 |
| 2 | i | 11.38 |
| 3 | a | 8.89 |
| 4 | u | 8.46 |
| 5 | t | 8.00 |
| 6 | s | 7.60 |
| 7 | r | 6.67 |
| 8 | n | 6.28 |
| 9 | o | 5.40 |
| 10 | m | 5.38 |
| 11 | c | 3.99 |
| 12 | l | 3.15 |
| 13 | p | 3.03 |
| 14 | d | 2.77 |
| 15 | b | 1.58 |
| 16 | q | 1.51 |

Fig. 1. Attacking Caesar cipher with frequencies - Snap! playground


**You (Alice)** 15:28
Bob… cobalt ok?

**Bob** 15:30
ok

**Eve** 15:30
hi there :)

**Danny** 15:31
Laura, emerald looks cool

**You (Alice)** 15:32
my calculated color is saffron

**Bob** 15:32
mine is ochre

**Eve** 15:32
...

got the secret color?

*SHARED SECRET COLOR*
96 dark orchid
SECRET COLOR
20 red
COMPUTED COLOR
54 saffron
RECEIVED COLOR
47 ochre
PUBLIC COLOR
83 cobalt
Now you have a secret color (dark orchid) you can use as a private key. It is the same for both of you and must be kept secret.

Fig. 2. Meeting chat and support app for the DH activity

## 4 PUBLICATIONS

An experience report paper [9] on the first iteration of the course has been accepted and will be presented at ITiCSE 2022 in Dublin.

Our work was presented at the 2021 Cryptography and Coding Theory Conference[2]. A short paper (in Italian) will be published in the conference proceedings [7].

Journal papers describing or comparing different aspects of the three iterations have been submitted or are in preparation.

## 5 DISSEMINATION

A website[3] has been set up with all the material in English and Italian [8]. All material is available under an open license to promote its dissemination and reuse.

The project has been presented several times to hundreds of teachers and several educational researchers. For example,

- at the "Bologna Linux Day 2021"[4] (Bologna, 23rd October 2021);
- at a meeting of the Cryptography and Coding Theory subgroup of the Italian Mathematical Union working on cryptography teaching and outreach (Online, 23rd June 2021);

[2] https://sites.google.com/view/crittografiaecodici/convegno-annuale
[3] https://bigideascryptok12.bitbucket.io/
[4] https://docs.google.com/document/d/1kpOo3tAvhhI6dCzrZVkYBWgg8j7lQkF_zICf4rSW35k/

- at a meeting between Computer Science and Math Education Researchers (University of Milan, 1st February 2022)

The course will be repeated a fourth time as part of the "Science Degree Project" (PLS), an Italian project to attract high school students to enroll in science degrees.

## 6 FINANCES

The received funds were used to finance part of Lodi's postdoctoral research grant.

## REFERENCES

[1] Tim Bell, Paul Tymann, and Amiram Yehudai. 2018. The Big Ideas in Computer Science for K-12 Curricula. *Bulletin of EATCS* 1, 124 (2018).

[2] European Commission. Joint Research Centre. 2017. *DigComp 2.1: the digital competence framework for citizens with eight proficiency levels and examples of use.* Publications Office. https://doi.org/10.2760/38842

[3] Department of Education. 2013. *National curriculum in England: computing programmes of study.* https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study

[4] Wynne Harlen. 2015. *Working with Big Ideas of Science Education.* Science Education Programme (SEP) of IAP, Trieste, Italy.

[5] K-12 CS Framework. 2016. *K–12 Computer Science Framework.* Technical Report. http://www.k12cs.org

[6] Anke Lindmeier and Andreas Mühling. 2020. Keeping Secrets: K-12 Students' Understanding of Cryptography. In *Proceedings of the 15th Workshop on Primary and Secondary Computing Education* (Virtual Event, Germany) *(WiPSCE '20)*. ACM, New York, NY, USA, Article 14, 10 pages. https://doi.org/10.1145/3421590.3421630

[7] Micahel Lodi, Simone Martini, and Marco Sbaraglia. 2022. Crittografia a blocchi al Liceo Matematico. In *Cryptography and Coding Theory Conference 2021*. Collectio Ciphrarum, Vol. 3. Aracne, Roma. https://drive.google.com/file/d/1DtTFZpHTX5ibrHGbPd8PUN6gWm6G5foP/view In Italian. To appear.

[8] Michael Lodi, Marco Sbaraglia, and Simone Martini. 2021. Big Ideas of Cryptography in K-12. https://bigideascryptok12.bitbucket.io/

[9] Michael Lodi, Marco Sbaraglia, and Simone Martini. 2022. Cryptography in Grade 10: Core Ideas with Snap! and Unplugged. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 1 (ITiCSE 2022), July 8–13, 2022, Dublin, Ireland* (Dublin, Ireland) *(ITiCSE '22)*. Association for Computing Machinery, New York, NY, USA, 7 pages. https://doi.org/10.1145/3502718.3524767

[10] Michael C. Loui and Maura Borrego. 2019. Engineering Education Research. In *The Cambridge Handbook of Computing Education Research*. Cambridge University Press, 292–322. https://doi.org/10.1017/9781108654555.012

[11] Marco Sbaraglia, Michael Lodi, and Simone Martini. 2021. A Necessity-Driven Ride on the Abstraction Rollercoaster of CS1 Programming. *Informatics in Education* 20, 4 (2021), 641–682. https://doi.org/10.15388/infedu.2021.28

[12] David Touretzky, Fred Martin, Deborah Seehorn, Cynthia Breazeal, and Tess Posner. 2019. Special Session: AI for K-12 Guidelines Initiative. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (Minneapolis, MN, USA) *(SIGCSE '19)*. ACM, New York, NY, USA, 492–493. https://doi.org/10.1145/3287324.3287525