Course: CS 127/227: Cryptography

Course Level: Upper-level undergraduate

Course Description: "In this fast-paced course, I plan to start from the very basic notions of cryptography and by the end of the term reach some of the exciting advances that happened in the last few years such as the construction of *fully homomorphic encryption*, a notion that Brian Hayes called "one of the most amazing magic tricks in all of computer science", and *indistinguishability obfuscators* which are even more amazing. To achieve this, our focus will be on *ideas* rather than *implementations* and so we will present cryptographic notions in their pedagogically simplest form– the one that best illustrates the underlying concepts– rather than the one that is most efficient, widely deployed, or conforms to Internet standards. We will discuss some examples of practical systems and attacks, but only when these serve to illustrate a conceptual point."[1]

Module Topic: The Ethics of Cryptography: Moral Responsibility, Privacy and Security

Module Author: Marion Boulicault

Semesters Taught: Spring 2020

Tags:

cryptography [CS]
direct proximity sensing [CS]
privacy [phil]
security [phil]
moral responsibility [phil]
interests vs rights [phil]

Module Overview:

In this module, we explore some of the ethical dimensions of cryptography. Using an assigned reading by Phillip Rogaway as a catalyst, we begin with the question: "What are cryptographers morally responsible for?" We then explore this question by looking at two real world case studies. The first explores the case of a 2015 terrorist attack in San Bernardino. During the investigation of the attack, the FBI discovered a suspect's encrypted iPhone and asked Apple to help break the encryption. Apple refused. We analyze the ethical dimensions of this case study using the concepts of security and privacy. We then consider a second case study again using the concepts of privacy and security, but this time focused on the development of smart phone applications to assist with COVID-19 contact tracing. We end the module by drawing on lessons learned from the case studies to return to the starting question of the class: what are the moral responsibilities of cryptographers?

[1] https://cs127.boazbarak.org/syllabus/

Connection to Course Material:

This module directly engages with the course material by asking students to consider traditional ethical questions concerning cryptography (namely, questions related to privacy and security) as a means of considering the moral responsibilities of cryptographers. By focusing the module on the responsibilities of cryptographers, the module encourages and enables students to come to the ethical material from their own perspectives and experiences as cryptographers. The module also incorporates some technical material from the course via the case studies. For example, the first case study – Apple vs FBI – involves a situation in which the FBI asked Apple for assistance in gaining access to encrypted information in a suspect's iPhone, protected by a 6 digit passcode and a secret 128 bit key hardwired into the processor. The FBI asked Apple to create a digitally signed software update to run a brute force search over the 10^6106 passcodes. Students learn about these technical dimensions during the class, so we are able to adeptly discuss the ethical issues using technical terminology and concepts.

Marginal Note:

We chose this topic because it takes a classic issue in the ethics of cryptography (namely, the idea of a trade-off between privacy and security) and applies it to a salient contemporary topic at the time the module was taught (namely, the COVID-19 pandemic). The module topic thus served to create a sense of proximity between the ethical dimensions of cryptography and the students' own everyday experiences. However, a more general module on privacy vs security trade-offs in cryptography would also be a suitable option.

Module Goals:

- Introduce students to two philosophical concepts that are useful for thinking through some of the salient ethical dimensions of cryptography: privacy and security.
- Allow students to practice engaging in ethical discussion and debate through the case studies.
- Provide students with the space and guidance for considering, understanding, and analyzing their own moral responsibilities as cryptographers (or as computer scientists more generally).

Key Philosophical Questions:

1. What are the moral responsibilities of cryptographers (especially those doing more abstract mathematical work that doesn't have obvious direct practical relevance)?
2. Some (e.g. Rogaway – see: assigned reading) have argued that cryptography is inherently political, and that research should acknowledge this and be directed at achieving beneficial political goals. Is this argument right? What might be some counterarguments?
3. How should we understand frequent claims in the media and in academia that, with respect to cryptography, the central ethical issue is how to balance privacy and security concerns?

4. What is the difference between a conception of privacy/security as an ‘interest’ versus a ‘right’?

Marginal Comment:

Questions (1) and (2) are the questions that drive the module: they ask students to consider the moral responsibilities of cryptographers. Questions (3) and (4) – which focus on privacy vs security trade-offs in cryptography – are asked as ways to explore Questions (1) and (2): are cryptographers morally responsible for making this trade-off?

Key Philosophical Concepts:

- Moral responsibility
- Privacy
- Security
- Interests vs rights

Marginal Comment

Moral responsibility is the guiding concept of the module. Public discussions regarding the ethics of cryptography tend to focus on the concepts of privacy and security, so we chose to work with these concepts as a way to explore moral responsibility. The distinction between an interest and a right is introduced to help students understand different interpretations of privacy and security.

Assigned Readings:

● Rogaway, P. (2015, December). *The Moral Character of Cryptographic Work*. 2015 IACR Distinguished Lecture. (parts 1 – 3) (link)	This reading is a paper written by a cryptographer Phillip Rogaway. In the paper, Rogaway argues that “cryptography rearranges power: it configures who can do what, from what.” As such, it is an inherently political tool, with intrinsically moral dimensions. This means that cryptographers have moral responsibilities to direct their work towards beneficial ends. This paper is assigned because it directly motivates the central question of the module: what are the moral responsibilities of cryptographers? Another important feature of this paper is that it is written by a practicing cryptographer, who is thereby able to adeptly integrate the technical aspects of cryptography into his

	philosophical argument. Assigning a reading written by a cryptographer also functions to demonstrate to the students that ethical reflection and argumentation is accessible to everyone, not only trained philosophers.
● *Apple, The FBI and iPhone Encryption: A Look at What's at Stake*. (n.d.). NPR.Org. Retrieved May 25, 2020, from https://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake	This is an NPR article giving background information on the first of the module's two case studies: Apple vs FBI. Assigning this reading allows the Embedded EthiCS TA to jump more quickly into the philosophical dimensions of the first case study, rather than spending more time on sharing the background information. It also provides students with a 'lighter' non-academic reading assignment, to complement the more academic piece by Rogaway.

Class Agenda:

1. Introduction
2. What are the moral responsibilities of cryptographers?
3. Case study one: Apple vs FBI
4. Theory: What do we mean by privacy? Interests vs rights.
5. Case study two: COVID-19 tracing applications
6. Return to starting question: What are the moral responsibilities of cryptographers?
7. Conclusions

Sample Class Activity:

After the first case study (Apple vs FBI) is introduced, the Embedded EthiCS TA conducts an online poll to solicit students' initial intuitions on which side of the conflict – Apple or the FBI – they support. The results of the poll are projected on a slide for the whole class to see. The students then split into pairs and are asked to defend the opposite side to that which they voted (e.g. if they voted for Apple, their task would be come up with arguments to defend the FBI). The Embedded EthiCS TA then calls on volunteers to share arguments for each side.

Finally, the Embedded EthiCS TA conducts the online poll again and the new results are displayed for the class to see if the discussion caused the class' initial intuitions to change. The Embedded EthiCSTA ends this activity by asking students to share with the class why they either did or did not change their vote, making vivid the sometimes back and forth, dialectical nature of philosophical reasoning and debate.

Marginal Comment:

The aim of this activity is to give students practice in thinking through both sides of a philosophical debate. To achieve this aim, the Embedded EthiCS TA asks students to imagine themselves as a lawyer for either Apple or the FBI. This role-play activity enables students to temporarily let go of their own viewpoints and consider the issue from the opposite perspective.

Module Assignment:

This module had no assignment.

Marginal Comment

Although this module had no assignment, it would certainly be possible to include one. For example, one could ask students to draw on the concepts of privacy and security to write a legal brief supporting either the FBI or Apple in a course case (see: Sample Class Activity).

Lessons Learned

Student response to this module was very positive. The students were highly engaged and seemed to grasp the key concepts, and class discussion was energetic and fruitful.

- This module is distinctive in the way it integrates a real-world case study directly relevant to the students' experiences. The module took place in April 2020, when all the students had left campus and were learning from home due to the COVID-19 pandemic. This was also when initial plans were being proposed for creating encrypted smart phone applications for assisting with COVID-19 tracing in the US. Basing the case study on comparing the security vs privacy trade-offs in two hypothetical versions of a COVID-19 tracing application created a sense of immediacy and relevance in the ensuing ethical discussion, demonstrating to the students the ways in which the ethical questions faced by cryptographers have direct, real-world impacts.
- This module was taught online (using Zoom). We found that using the Zoom breakout rooms feature was extremely effective for generating discussion and providing students with a space to feel comfortable in expressing their opinions. For example, in the discussion of the second case study, students were randomly assigned into 5-person breakout rooms. Each group was tasked with discussing how they would balance the privacy vs security concerns evoked by the development of direct proximity sensing Covid-19 contact tracing applications. The Embedded EthiCS TA visited each breakout room over the 10-minute discussion period to answer any questions and listen in to some of the discussion. Each breakout room was lively and engaged, and conversation flowed more naturally than it did in the larger group setting.