Abstract Algebra Project: Public-Key Cryptosystems

Michael Dougherty
Lafayette College

1 Preface

For most undergraduates earning a degree in mathematics, a course in abstract algebra is likely to contain the most theoretical mathematical concepts they will encounter. Students who enjoy the material often inquire whether there are any real-world applications which make use of this technology, and the answer is almost always the same: cryptography. In addition, many mathematical institutions and professional societies in the United States use this connection to advertise careers for government surveillance agencies. As a result, students who develop an interest in cryptography from a course in pure abstract algebra are often unprepared for the ethical quandaries which can naturally arise in secure communication.

This project aims to introduce a simple cryptographic algorithm (Diffie–Hellman Key Exchange), invite students to consider the historical context of its development, and use ethical reasoning to resolve a challenging scenario involving cryptography which is based on real life. It is designed for use in a first course on abstract algebra, but could easily be adapted for any course which includes modular arithmetic. It is also beneficial if students are already prepared to write short responses on various prompts within the course (e.g. through weekly reflections).

1.1 Background: Diffie–Hellman Key Exchange

Most forms of encryption throughout history (dating back to the origins of writing) have been examples of *private key* cryptography, in which two parties agree on a secret code or password, and messages can be encrypted and decrypted using the code. These methods can provide extremely high levels of security, but require that a secret code is agreed upon in advance. This is impractical over an unsecured communication channel such as the internet—to give a common example, how can you securely share your credit card information with an online retailer without meeting them in person beforehand?

Public key cryptography was developed in the 1970s to address this issue, and it uses mathematical processes which are easy to do in one direction (e.g. multiplication) but difficult to do in reverse (e.g. factoring). In this project, we focus on the *Diffie–Hellman key exchange* algorithm, which is a method for agreeing upon a secret code over an unsecured channel—it is not itself an encryption protocol, but the resulting shared secret can then be used in a more traditional cryptographic algorithm.

The algorithm can be described as follows. Alice and Bob wish to decide on a shared secret (in the form of a number) over an unsecured channel. To start, they publicly decide on a prime number p and a primitive root modulo p called g (i.e. g is a generator for the multiplicative group of integers modulo p). Then Alice chooses a number a in secret, computes $g^a \bmod p$, and publicly sends the resulting number to Bob. Similarly, Bob chooses a number b in secret, computes $g^b \bmod p$, and publicly sends the result to Alice. In the final step, Alice computes $(g^b)^a = g^{ab} \bmod p$ and Bob computes $(g^a)^b = g^{ab} \bmod p$ to arrive at a shared secret of $g^{ab} \bmod p$.

At the heart of the algorithm is the *discrete logarithm problem*: even though an eavesdropper could see g, p, and $g^a \bmod p$, it is extremely difficult to recover the number a from that information.

By choosing a large enough prime p (e.g. 2048 bits), it is virtually impossible for an eavesdropper to decode the shared secret.

1.2 Background: Ethical Reasoning

Part of the motivation for this project is to develop the following knowledge, skills and abilities (KSAs) for ethical reasoning, proposed by Rochelle Tractenberg. Students may benefit from being directly introduced to the framework during class sessions or other assessments.

1. Identify and quantify your prerequisite knowledge. Professional practice standards (including but not limited to the Proto-Ethical Guidelines for Mathematics Practice), local laws, and stakeholder analysis are important knowledge needed for reasoning ethically. This is a necessary KSA for ethical reasoning with any source document—like an ethical practice standard, federal data guidelines, or workplace policy.

2. Identify decision-making frameworks. What would the ethical practitioner do in this case? How can benefits be maximized while harms are minimized? Although these represent the virtue and utilitarian perspectives, respectively, in-depth understanding of ethical decision-making is not as important in the ER process as recognizing which of these two perspectives is most relevant to the case, situation, or task at hand.

3. Identify or recognize the ethical issue. Does something about a case, situation, or task represent an undue imbalance in the harms and benefits identified in the stakeholder analysis? Or, if such guidance is available, is there something about a case, situation, or task that seems inconsistent with that guidance? Note that consideration of harms/benefits (i.e., stakeholder analysis) works as well as ethical practice standards to teach and give practice with ER.

4. Identify and evaluate alternative actions (on the ethical issue). Just like real life, every ethics case analysis requires a decision to be made. To ensure viable options are considered, at least two plausible alternative options (decisions, actions) are always available to be identified and evaluated. These actions always include, do nothing/ignore the issue identified and do something about the issue identified. Even without a formal process for dealing with identified ethical problems, learners can evaluate these alternatives, either in the stakeholder analysis (i.e., comparing harms to benefits in terms of their severity and/or to whom they accrue) or by appealing to ethical practice standards.

5. Make and justify a decision. What to do in the face of the ethical challenge that was identifiedincluding at least some discussion of how stakeholder effects were considered. An essential part of the ethical reasoning normalization process, notifying practitioners.

6. Reflect on the decision. What makes this case hard? What additional information would be/would have been helpful? How can you get better at these challenging features of ethical reasoning? How does a case/analysis like this one help create the culture that promotes fluency in ethical reasoning and/or a more ethical workplace?

2 Assignment

2.1 Purpose

Throughout history, most cryptographic systems were *private-key* in the sense that two parties who wanted to share encrypted messages needed to meet in private to agree on their secret code

beforehand. A *public-key* cryptosystem uses advanced mathematics to enable correspondents to agree on a secret code in an unsecured channel (e.g. the internet). The purpose of this project is to master the mathematics behind a public-key cryptosystem (*Diffie–Hellman key exchange*) and explore its impact on society.

2.2 Assignment

For each prompt below, write a short (2-3 paragraphs) response. Feel free to reference outside articles or other materials with appropriate citation. You will be graded on the accuracy of your reasoning, the depth of your responses, and the clarity of your writing.

Part I: Diffie–Hellman Key Exchange

1. Write a careful example of how two people could implement the Diffie–Hellman protocol with the public numbers $p = 23$ and $g = 5$. To keep things interesting, choose the private numbers a and b to be different numbers, each at least 6. What number do the two parties share at the end of the exchange?

2. Using the same p and g as in the first part, suppose you eavesdrop on two parties who exchange the numbers 16 and 18. Use this information to deduce a and b, as well as the shared secret number. Why does this become much more difficult if we choose p to be larger (e.g. hundreds of digits)?

Part II: Public vs. Private Cryptography

3. The first public-key cryptosystems were developed in the late 1970s, just before internet access broadened dramatically in the 1990s. How lucky! Imagine that things didn't work out this way, and only private-key cryptography was available to use on the internet today—this would mean that in order to communicate securely (including emails, text messages, and online orders), you would need to meet with the recipient privately in advance. How might this change the way you use the internet?

4. How might other groups be impacted by this change? You may want to consider parties such as online retailers, researchers who collaborate online, activist organizations, government agencies, or any others.

Part III: Applying a Code of Ethics

5. Suppose the year is 1977 and you are an editor for a journal on mathematics and computer science, and a researcher sends you an article which introduces a new idea: public-key cryptography. The article suggests that this cryptosystem will enable users of the upcoming "world wide web" to communicate securely over a public channel, thus democratizing an electronic means of communication. However, you also receive a stern message from a US surveillance agency which claims that publishing this type of protocol could damage the agency's ability to detect threats to national security, and they urge you to reject the article. What is the ethical issue in this situation, and how would you respond?

6. Guidelines from professional societies provide a way to address ethical questions like the one posed above. Two applicable sets of guidelines in this case might be the ACM (Association for Computing Machinery) Code of Ethics and Professional Conduct and the recently-proposed

Mathematics Ethical Guidelines—see the appendices. Read through these two frameworks and consider which guidelines would apply in this example. Explain which guidelines are applicable and why (highlighting any cases where the two frameworks differ).

7. Now that you have examined two different guidelines for ethical reasoning, would you change your answer for Question 5? Explain why you would or explain why your answer was supported by the ethical guidelines. In your explanation, discuss at least one alternative action to the one you chose and explain why your choice was preferable in comparison.

8. The situation described in Question 5 is based on real life. Read the article *Keeping Secrets* by Henry Corrigan-Gibbs (https://stanfordmag.org/contents/keeping-secrets) and write a brief reflection. Did you find anything particularly surprising or interesting?

2.3 Appendix 1: Ethical Reasoning

This framework provides steps for reasoning through an ethical issue (in mathematics and beyond).

1. Identify and "quantify" your prerequisite knowledge (e.g. professional practice standards).
2. Identify decision-making frameworks ("What would the ethical practitioner do? How can benefits be maximized while harms are minimized?")
3. Identify or recognize the ethical issue.
4. Identify and evaluate alternative actions on the ethical issue.
5. Make and justify a decision.
6. Reflect on the decision.

2.4 Appendix 2: ACM Code of Ethics and Professional Conduct

See https://www.acm.org/code-of-ethics for more detail.

1. **General ethical principles**
   A computing professional should...
   (a) Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
   (b) Avoid harm.
   (c) Be honest and trustworthy.
   (d) Be fair and take action not to discriminate.
   (e) Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
   (f) Respect privacy.
   (g) Honor confidentiality.
2. **Professional Responsibilities**
   A computing professional should...
   (a) Strive to achieve high quality in both the processes and products of professional work.

(b) Maintain high standards of professional competence, conduct, and ethical practice.

(c) Know and respect existing rules pertaining to professional work.

(d) Accept and provide appropriate professional review.

(e) Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

(f) Perform work only in areas of competence.

(g) Foster public awareness and understanding of computing, related technologies, and their consequences.

(h) Access computing and communication resources only when authorized or when compelled by the public good.

(i) Design and implement systems that are robustly and usably secure.

3. **Professional Leadership Principles**
   A computing professional should...

   (a) Ensure that the public good is the central concern during all professional computing work.

   (b) Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

   (c) Manage personnel and resources to enhance the quality of working life.

   (d) Articulate, apply, and support policies and processes that reflect the principles of the Code.

   (e) Create opportunities for members of the organization or group to grow as professionals.

   (f) Use care when modifying or retiring systems.

   (g) Recognize and take special care of systems that become integrated into the infrastructure of society.

4. **Compliance with the Code**
   A computing professional should...

   (a) Uphold, promote, and respect the principles of the Code.

   (b) Treat violations of the Code as inconsistent with membership in the ACM.

2.5 Appendix 3: Proto-Ethical Guidelines for Mathematical Practice

Another set of ethical guidelines, targeted to practitioners of mathematics, was recently proposed by Rochelle Tractenberg, Catherine Buelle, and Victor Piercey (https://osf.io/x5ur9/).

The ethical mathematics practitioner...

In general

1. Is honest about their qualification to complete work they accept; articulates any limitation of expertise, and consults others when necessary or in doubt. They accept full responsibility for their professional performance and practice.

2. Treats others with respect. Promotes the equal dignity and fair treatment of all people, and neither engages in nor condones discrimination based on personal characteristics. Respects personal boundaries in interactions, and avoids harassment, including sexual harassment; bullying; and other abuses of power or authority. Takes appropriate action when aware of disrespectful behaviors by others.

3. Accepts full responsibility for their own work; does not take credit for the work of others; and gives credit to those who contribute. Respects and acknowledges the intellectual property of others.

4. Should be forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgment. Discloses conflicts of interest, financial and otherwise, and manages or resolves them according to established (institutional/regional/local) rules and laws.

5. Recognizes any mathematical descriptions of groups may carry risks of stereotypes and stigmatization. Practitioners should contemplate, and be sensitive to, the manner in which information in their work across education, research, public policy, and in the public in general, is framed to avoid disproportionate harm to vulnerable groups.

6. Avoids condoning or appearing to condone mathematical, scientific, or professional misconduct. Takes appropriate action when aware of unethical conduct by others.

7. Avoids, and acts to discourage, retaliation against or damage to the employability of those who responsibly call attention to possible mathematical error or to scientific or other misconduct.

8. Is informed about applicable laws, policies, rules, and guidelines; follows these unless there is a compelling ethical reason to do otherwise.

9. Must know how to work ethically in collaborative environment. When conducting their work in conjunction with other professions, must continue to abide by mathematicians' responsibilities, as well as any guidelines of the other professions. When there is a conflict or an absence in the partner profession's guidelines, the mathematical practitioners' responsibilities should be followed.

10. Respects others, and promotes justice and inclusiveness, in all work. Fosters fair participation of all people. Avoids and mitigates bias and prejudice. Does nothing to limit fair access.

11. Opposes marginalization of people on the basis of human differences. Strives to resist institutional confirmation bias and systematic injustice.

12. Minimizes the possibility of harming others; whether directly or indirectly, intentionally or unintentionally

As a member of the profession

13. Strives to make new mathematical knowledge as widely available as is feasible.

14. Maintains high standards of professional competence, conduct, and ethical practices.

15. Recognizes that if they engage in mathematics practice, they do so in a social and cultural context, acknowledging that all people are stakeholders in mathematics.

16. In reviews, considers the potential for unjust or inequitable implications of the proposal or work.

17. Understands the differences between questionable mathematical, scientific, or professional practices and practices that constitute misconduct. The ethical mathematics practitioner avoids all of the above and knows how each should be handled.

18. Helps strengthen the work of others through appropriate peer review; assesses methods, not individuals. Strives to complete review assignments thoroughly, thoughtfully, and promptly.

19. Avoids and addresses exclusionary practices in hiring, teaching, and recruiting. When assessing or evaluating mathematics practitioners or their work, uses relevant subject matter-specific qualifications. Uses qualifications, performance, and contributions as the basis for decisions regarding mathematical practitioners of all levels.

20. Upholds, promotes, and respects the ethical responsibilities of the mathematics community.

21. Accepts their accountability to build an inclusive mathematics community that values its members.

22. When involved in advising graduate students, should fully inform them about the employment prospects they may face upon completion of their degrees.

In their scholarship

23. Strives to support and achieve quality work in both the process and products of professional work. Works in a manner intended to produce valid, interpretable, and when applicable, reproducible results.

24. Identifies and mitigates any efforts to predetermine or influence the results or outcomes of mathematical practices; resists pressure to solve unethical problems/support predetermined outcomes.

25. Strives to follow, and encourages all collaborators to follow, an established protocol for authorship.

26. Is candid about any known or suspected limitations, assumptions, or biases when working with methods, models, or data. Objective and valid interpretation of the results requires that the underlying analysis recognizes and acknowledges the degree of reliability and integrity of the method, model, or data.

27. Assesses, and is transparent about, the origin and source of the tools and methods they use, including prior results and data. Practitioners, when possible, acknowledge and disclose the origin of the problems they are solving and the interests that their work is intended to serve.

28. Strives to promptly correct any errors discovered while producing the final report or after publication. As appropriate, disseminates the correction publicly or to others relying on the results.

29. Understands and conforms to confidentiality requirements of data collection, release, and dissemination and any restrictions on its use established by the data provider (to the extent legally required), protecting use and disclosure of data accordingly.

30. Strives to ensure that data sources, choice of methods, and applications do not create or perpetuate social biases or discrimination. Seeks to avoid confirmation bias.

31. Avoids plagiarism. The knowing presentation of another person's mathematical discovery as one's own constitutes plagiarism and is a serious violation of professional ethics. Plagiarism may occur for any type of work, whether written or oral and whether published or not.

32. Promotes sharing of data, methods, scholarship as much as possible and as appropriate without compromising propriety.

33. Recognizes the inclusion of mathematics practitioners as authors, or acknowledgement of their contributions to projects or publications, requires their explicit permission because it implies endorsement of the work.

An ethical mathematics practitioner who is a leader, employer, supervisor, mentor, or instructor follows all of the above items and also...

In general

34. Maintains a working environment free from intimidation, including discrimination based on personal characteristics; bullying; coercion; unwelcome physical (including sexual) contact; and other forms of harassment.

35. Articulates these ethical responsibilities to mathematics practitioners as well as non-practitioners.

36. Ensures that they enhance, not degrade, the quality of working life. Leaders should consider accessibility, physical safety, psychological well-being, and human dignity of all community members.

37. Does not exploit the offer of a temporary position at an unreasonably low salary and/or an unreasonably heavy workload.

As a member of the profession

38. Recognizes that mathematicians' ethical responsibilities exist and were articulated for the protection and support of the mathematics practitioner, the mathematics user, and the public alike.

39. Encourages and promotes sound and ethical mathematical practice, and exposes incompetent or corrupt mathematical practice.

40. Strives to protect the professional freedom and responsibility of mathematical practitioners who comply with these guidelines.

41. Articulates, applies, and supports policies and processes that reflect the principles of mathematicians' responsibilities. Designing or implementing policies that deliberately or negligently violate, or tend to enable the violation of, mathematicians' responsibilities is ethically unacceptable.

42. Ensures that opportunities are available to mathematics practitioners to help them improve their knowledge and skills in the practice and dissemination of mathematics, in ethical practice, and in their specific fields, and encourages people to take those opportunities.

43. Demonstrates and educates students, employees, and peers on the ethical aspects of their teaching, ethical implications of their work, and the ethical challenges within the practice of mathematics.

44. Takes full responsibility for their contributions to the certification/granting of a degree in mathematics by ensuring the high level and originality of the Ph.D. dissertation work, and sufficient knowledge in the recipient of important branches of mathematics outside the scope of the thesis.