CERIAS Tech Report 2005-37

THE ETHICS OF CRYPTOGRAPHY

by Courtney Falk

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

THE ETHICS OF CRYPTOGRAPHY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Courtney Falk

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

May 2005

This is dedicated to my family who enabled to do this graduate degree. To Michelle Anderson the fellow graduate student who shares my perpetual quest for knowledge. To professors Victor Raskin and Melissa Dark whom both helped me pursue the research areas in which I was interested. To the entire staff members of CERIAS who are able to help get anything accomplished even when the deadline is passed. To the CERIAS graduate students who know what it is like to be a graduate student; Florian Buchholz, Brian Carrier, and Bill Speirs. And finally to the other members of the Scholarship for Service program who also shared the additional burdens imposed by the requirements of the SFS program; Brad Moseng, Chris Marsico, Matt Meyers, J.D. Burchett, and Mike Hoeschele.

ACKNOWLEDGMENTS

The author would like to thank Harrison Kleiner and Patrick Kain who both introduced him to philosophy in general and ethics in particular. And also thanks goes to Eugene Spafford and Ben Kuperman who taught the classes that showed the necessity of security.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

A posteriori – After experience.

A priori – Priori to experience.

Cipher – mathematical function that takes input data and returns encrypted data as a result or vice-versa.

Cryptanalysis – The study of code breaking.

Cryptography – The study of code making.

Cryptology – The general study of codes. Encompasses both cryptography and cryptanalysis.

Deontology – Theory of morality that determines the ethical permissibility of an action as according to the maxim of its agent.

Hash function – A one-way mathematical function designed to provide an unique digest for a given input data set.

ITAR (International Trade in Arms Regulations) – Act of the United States government meant to prevent the proliferation of weapons and weapons technologies.

Maxim – A personal rule of behavior.

Normative – Definitive of what is normal.

Ontology – Branch of metaphysical philosophy that deals with the existence of concepts and their interrelations.

ABSTRACT

Falk, Courtney Allen. M.A., Purdue University, May, 2005. The Ethics of Cryptography. Major Professors: Eugene Spafford, Victor Raskin, and Melissa Dark.

This thesis explores cryptography and applies a normative ethical theory to determine what if any uses of cryptography are ethically permissible. Cryptography is divided into confidentiality, integrity, and authentication before being considered under the deontological moral theory of Immanueal Kant and other modern philosophers such as Alan Donagan, John Rawls, and Robert Nozick. Brief discussions on the fields of ethics and cryptography are included to aid any reader not familiar with them.

CHAPTER 1. INTRODUCTION

1.1. Objectives

There is much talk and discussion about what is and is not ethical in regards to digital technology. As the digital age becomes more pervasive and integrated into everyday lives it also becomes more important to establish appropriate ethical interpretations. If such interpretations aren't fully realized quickly then it is likely that certain uses of digital technology will become mired in opinion and hearsay instead of theory and logic. Examples of such thought already exist such as cryptography's prior export status as a munition in the United States under the International Traffic in Arms Regulations (ITAR) (Levy 109) and its subsequent repeal by the Clinton White House (Ferrera 376).

While the realm of digital technologies needing ethical treatment is wide there is not room within a single thesis to address them all satisfactorily. Even within the area of cryptology there are the complementary fields of cryptography and cryptanalysis. The same problem of devoting adequate space arises. To fully address cryptology in its entirety requires a dissertation in the least or a book. Therefore this thesis restricts itself to making ethical determinations in regards to cryptography only.

What makes the task of addressing ethical issues in cryptography difficult is the hope of doing so in such a way that is easily accessible by philosophers, computing professionals, and computer users alike. The ethics herein must base itself on established theory but at the same time cannot address every possible objection or problem with the theory in question for risk of alienating non-

philosophers. Likewise, the complex mathematics and dedicated technologies of cryptography are explored only at a shallow level so as to not intimidate non-cryptographers. The best way to effect change in the ethical thinking of all those involved in the problems of cryptography is then to write a text that is accessible to everyone.

The importance of writing technology and ethics material for the widest possible audience can't be understated. Take for example the popular quarterly hacking magazine 2600. In the volume six, number two issue there is one story complaining about inept parental supervision software ("How Parents Spy on Their Children") and another about how to keep parents from spying on their kids ("How to Keep Parents From Spying"). And this is neglecting other articles on such topics as how to have "fun" at Costco by breaking the security on their AS/400 terminals ("Fun at Costco"). These simultaneous and conflicting attitudes are all too common in a world increasingly dependent upon technology. None of the authors of these articles seem to have taken much time to deliberate on the ethical or moral nature of their actions.

The short objective of this thesis is to explore what, if any, uses of cryptography are ethical. Moral uses of cryptography are meant to be utilized by individuals and aren't necessarily meant for public policy or law. There are many difficult questions that don't have satisfactory answers in regards to whether or not what is moral should be law. Conversely, as Martin Luther King Jr. pointed out, there can and are laws that are not moral (215). All ethical determinations are done for the sake of individuals so as to avoid the problems of endorsing public policy.

1.2. Existing Literature

The existing literature concerning cryptography and ethics is sparse and often incomplete. Most books concern ethics and technology in general with little or no focus on cryptography specifically.

Computer Related Risks by Peter Neumann is an extensive collection of cases concerning disasters that had a basis in computers. In terms of ethics Neumann only devotes three pages towards the end for discussing it. This ethical discussion is about technology in general and says nothing about cryptography.

Sara Baase devotes her entire book, A Gift of Fire, to the topic of information technology and its interaction with society and ethics. As the description hints, Baase's text talks from the point of view of sociology as opposed to philosophy. But A Gift of Fire falls prey to the same problems as Computer Related Risks, giving a lot of time and space over to cases and little to the author's original thoughts and conclusions.

Case studies such as those relied upon by both Baase and Neumann are a double-edged sword. Often case studies are a terrific tool for developing critical ethical thinking among individuals. But what is often neglected is the theory or method that should be used when contemplating the cases. Knowing such theories would be a great boon in analyzing the morality of situations and may help accelerate the learning process in ethics courses. Too many case studies, especially from opposing points of view, can cloud the issue at hand. It is always good to consider the other side of the argument but to people unfamiliar with the issues at hand may become overwhelmed.

Computers, Ethics, and Society is a collection of essays from prominent people in the computer security community. A few articles are even devoted to discussing normative ethical theories like utilitarianism and deontology. In this regard Computers stands head and shoulders above both Risks and Fire. But what Computers lacks is any substantive discussion of cryptography and ethics. Dorothy Denning writes a piece arguing for wiretapping of cryptographic communications ("Digital Communications Must Not Weaken Law Enforcement") while Marc Rotenberg takes the opposing stance against wiretaps ("Wiretap

Laws Must Not Weaken Digital Communications"). Both essays skip over the fundamental issue of cryptography use in general in order to leap ahead to the hot button topics of wiretaps and law enforcement intrusion.

One of the primary goals of this thesis should be to provide the fundamental understanding of ethics and cryptography that is lacking currently, and to do so according to formal ethical theories. The ethical theories provide the arguments for/against cryptography more weight than that of only case studies because there is a standard for which there is a right and a wrong answer. Case studies can only support/defend an argument without describing *why* it is right or wrong.

1.3. Organization

This thesis covers two large topics that are intimidating and difficult in their own rights and joins them together in a matter of six chapters. Each chapter builds on the topics discussed in the preceding chapter with the final culmination of ethics and cryptography.

Introductions are done in the first chapter. The tone and organization of the thesis are established with a focus on painting the thesis as important to everyday life, understandable, and not intimidating. Both ethics and cryptography can be daunting areas to dive right into. Each requires a wide breadth of prior knowledge in order to be fully understood. Therefore, certain chapters are dedicated to describing these topics in such a way as to familiarize the reader with all the necessary details for understanding this thesis while not covering every nuance of the area.

Chapters two and three cover areas of interest in the area of ethics. The second chapter gives a brief primer to the area of ethics while the following chapter continues specifically with a particular theory. While the primer is by no means comprehensive it strives to give a good foothold to anyone who has no prior

exposure to ethics as philosophy. At the end of chapter three the reader should possess a solid understanding of the theories utilized by this thesis.

Ethics is not a simple topic and especially so when discussed in a philosophical sense. One of the primary focuses of chapter two is to describe various areas that deal with ethics, including philosophy, and discussing which ones are of importance to this thesis. It is difficult to fully address ethics without addressing each of the areas, but time and space constraints dictate that certain assumptions must be made and topics glossed over. For instance, the psychological development of ethics in an individual is a fascinating topic and discussed in several books devoted solely to it, but it is not the most important aspect of ethics for this particular discussion.

The fourth chapter is another brief primer, but this one is in the area of cryptography. The goal of this thesis is to use the historical usage and development of cryptography to highlight problems of the past, present, and future. History shows how the ethical problems facing Julius Caesar of Rome and his uses cryptography are the same as those facing modern intelligence agencies using quantum cryptographic devices.

Chapter five is the central focus of the thesis in that it brings together the ethical and cryptographic parts. Only after understanding the two separately can they then be brought together. Not only does chapter five address the issues inherent between ethics and cryptography, but it also raises and answers possible concerns with the approach. By the point the reader reaches this chapter he or she should have the necessary understanding of both deontological ethics and cryptography in order to comprehend the premises to the arguments made, allowing him or her to focus on the argument itself.

Finally, chapter six brings together all the previous chapters and examines whether or not the goals set forth in the introduction are met. Even though it can be said that “the journey is more important than the beginning or the end”, it is still important to analyze whether or not the goals set out initially have been met satisfactorily.

Some texts are written in a way that chapters stand on their own. Readers are then able to skip between chapters instead of following any linear path. The nature and structure of this thesis prevents such random access. A reader starting in chapter five may find him or herself confused by the terminologies used when in fact said terminologies have been addressed at length in preceding chapters. That being said, the recommended course of action for reading this thesis is from beginning to end.

CHAPTER 2. A BRIEF PRIMER ON ETHICS

2.1. Introduction

Ethics is one of the oldest areas of philosophy, dating back thousands of years to Aristotle and the great Greek philosophical tradition. In fact, Aristotle's theory of ethics is still studied today in its classical and updated forms.

A good place to start is to understand the structure of ethics. Ethics, like most areas of study, is not nearly as homogenous and unified as it first appears. Instead there exist a number of levels of ethical inquiry and various approaches, some from areas outside of philosophy. Peter Neumann talks about how different groups take different views of ethics (275-276). Different approaches to ethics may appeal to different groups in a similar way.

2.2. Areas of Ethics

There are several different areas that approach ethics in different ways. Some examples are philosophy, psychology, sociology, law, and even anthropology. It would be confusing and time consuming to address them all. Instead, three of the largest contributors are chosen and discussed in greater detail than would be possible with all the various fields together.

Of the three fields discussed, two are differing levels of philosophical inquiry into ethics: normative ethics and meta-ethics. It is difficult to separate the two because normative ethics proves central to this thesis and it also makes certain meta-ethical assumptions. Separating the two levels of philosophical ethics

helps to focus on the issues pertinent to ethics and cryptography while not bogging down in explaining or defending certain meta-ethical implications.

The third field, social science, covers various aspects of observable human behavior. Psychology typically studies the individual, how they development, and the decision making processes used. Sociology deals with entire societies and the rules that govern them. What psychology and sociology share is their scientific methodology, collecting observations, and interpreting data.

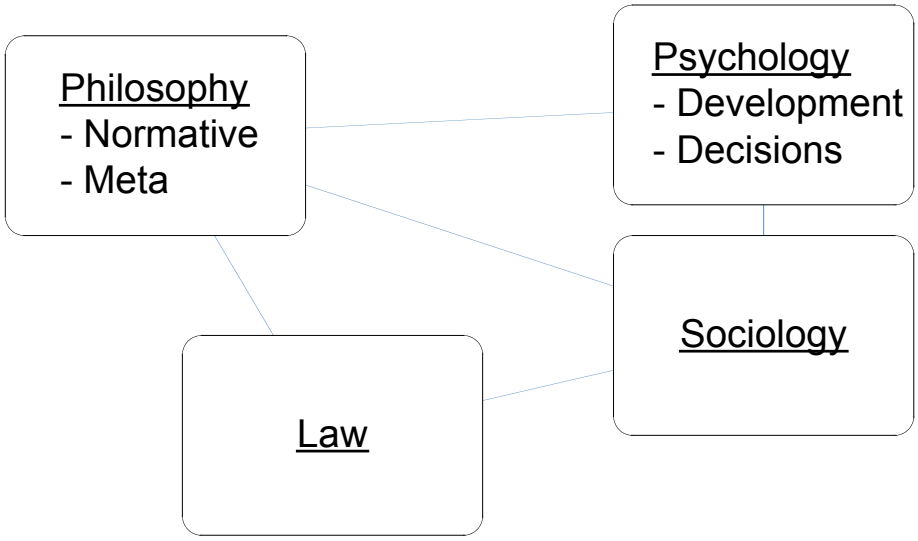

Figure 2.1 Relations of fields studying ethics

2.2.1. Social Science

The social sciences take a phenomenological to ethics. Examples of phenomenon measured by the social sciences are actions and attitudes exemplified by persons. Psychology and sociology, both areas of social sciences, offer much to the understanding of ethics.

A large focus of psychology is development such as physical, mental, and even ethical. Jean Piaget is often held up as one of the pillars of developmental psychology. Piaget writes extensively about the physical development process

of infants and newborns. Psychologist Lawrence Kohlberg focused mostly on the ethical development as opposed to Piaget's physical development (The Meaning and Measurement of Moral Development).

What is interesting about Kohlberg's theory are the described stages of moral judgment (Damon 73). The three main levels are self-interest, social approval, and abstract ideals, moving from the former as the least developed and the latter as the most developed. Each level encompasses two of the stages of moral judgment.

Table 2.1 Kohlberg's Six Stages of Moral Judgment

Level 1: Self-Interest	
Stage 1: Punishment	"I won't do it, because I don't want to get punished."
Stage 2: Reward	"I won't do it, because I want the reward."
Level 2: Social Approval	
Stage 3: Interpersonal Relationships	"I won't do it, because I want people to like me."
Stage 4: Social Order	"I won't do it, because it would break the law."
Level 3: Abstract Ideals	
Stage 5: Social Contract	"I won't do it, because I'm obliged not to."
Stage 6: Universal Rights	"I won't do it, because it's not right, no matter what others say."

Whenever anyone attempts to describe ethics in terms of statistics or surveys they are actually engaging in sociology instead of philosophy. Sociology measures the ethical attitudes of members of a given society. But sociology, like other social sciences, is limited in that sociologists cannot derive theories of action from the data gathered. This is a "problem" created by mankind's rational abilities, to seemingly do contrary to what the laws of nature, or even prudence, require.

What sociology would like to do is develop a theory of how people in a society act. This is not the focus of ethics. Philosophy has an advantage in that it describes how people *ought* to act and not how they *do* act. It then seems that sociology and philosophical ethics are at odds, but this is not necessarily so. The two fields merely take opposite approaches.

A common misunderstanding between sociology and philosophy in respect to ethics is the difference between values and value-opinions (Kreeft 82). While values are thinks like pride, honor, honesty, and thrift, value-opinions are a society's ordinal list of values. Japanese society may favor pride over thrift while a poor third world country values the opposite. Persons not familiar with this distinction may view the two as equivalent, leading to a culturally relative way of moral thinking.

Furthermore, there is a theory of ethics called moral projectivism such as the one discussed by John McDowell (215). This theory says that there is not really such a thing as ethics and that when a person says, "That is wrong," they are actually saying, "*I feel that* that is wrong." It seems likely that projectivism draws on common persons' misunderstandings of the differences between sociological and philosophical studies of ethics.

But the projectivist's arguments rest on the philosophical naïveté of the speaker. Certainly it can be admitted that statements like those referred to by McDowell lack a certain moral force. The only way to add such a moral component is for the speaker to replace "I feel" with "According to ____", where blank represents some structured theory of ethics and actions. Such theories are what's known as normative ethics.

However, there is somewhat of a bridge between sociology and normative ethics. Contractarianism is an ethical theory focusing primarily on the idea of justice; rights and duties between individuals in a social contract. This ideally suits the earlier discussion of Kohlberg's theory of ethical development in general and the fifth stage in particular (Damon 73).

Contractarian theories are not new as they date back to the works of Thomas Hobbes and Jean-Jacques Rousseau. One modern contractarian derives much of his work from the same normative ethics as is the focus of this thesis. John Rawls is renowned for his work in the treatise, A Theory of Justice, and later, The Law of Peoples. Even virtue ethicist Alasdair MacIntyre agrees with one of Rawls' assertions that community groups play an important role not fulfilled by either nation-state or family group, "Neither the state nor the family then is the form of association whose common good is to be both served and sustained by the virtues of acknowledged dependence. It must instead be some form of local community…" (135). Rawls' work in some respects offers a foil of other modern contractarians such as Robert Nozick. But it is still Rawls who builds the best bridge between political science/sociology and normative ethics.

2.2.2. Normative Ethics

Normative ethics are of principle concern to this thesis. Normative theories of ethics are prescriptive. In other words, they tell people how they ought to act in

certain circumstances. They outline rules of conduct and behavior for living a good life. Most philosophers take the stance that a good life is a happy one.

There are many branches and theories concerning normative ethics. The bulk of the tradition can be divided into three separate types of theories: agent-centered, consequentialist, and action-centered. Each type of theory can make a different ethical judgment based on identical situations.

Agent-centered theories tend to focus on characteristics that make for a good agent or person. Aristotle's Nicomachean Ethics is an early example of one such theory. It focuses on the idea that there are virtues one can possess and that acting in a moral way is knowing how to use the virtues in the proper way. Agent-centered theories such as virtue ethics aren't dead. Catholic philosophers such as St. Augustine and St. Aquinas revised virtue ethics to meet their theological needs. Philosophers like Alasdair MacIntyre and Rosalind Hursthouse carry on modern virtue ethics work.

Consequentialist theories concern themselves with the outcomes of actions. Often the way an outcome is reached isn't as important as the consequences of that outcome. Utilitarianism is such a theory first suggested by Jeremy Bentham in "The Principle of Utility". He outlines a "hedonistic calculus" that determines whether or not an action was good or bad based on the aggregate sum of pleasure or pain created by the action. John Stuart Mill revised and refined this theory in the aptly named book Utilitarianism, which goes into greater detail as to what pleasures are better than others.

The third and final type of normative ethical theory is action-centered. While the previous two types of theories talk about good people or good consequences, the action-centered theory talks about what makes an act good. Whether or not the person committing the act or the consequences are good or bad are largely

irrelevant. This appeals to the common sense notions that even bad people can do good acts or that sometimes good acts can have bad consequences. Immanuel Kant discusses one such theory called deontology in his book, The Grounding for the Metaphysics of Morals. Deontological moral theories such as Kant's are addressed at greater length in the following chapter.

Table 2.2 Normative Ethical Theories

Theory	Normative Focus	Example Philosophers
Virtue Ethics	Agents	Aristotle, Aquinas, Hursthouse, MacIntyre
Utilitarianism	Consequences	Bentham, Mill, Hare
Contractarianism	Agreements	Hobbes, Rousseau, Nozick, Rawls
Deontology	Maxims	Kant, Donagan, O'Neill

Another normative ethical theory to consider in passing is that of contractarianism. There are many contractarian theories that have sprung up over the centuries. Contractarian theories often refer to a "state of nature" in which humans originally lived. This state of nature describes how humans typically act. For Hobbes this is cynical and egotistical while Rousseau takes an idyllic and selfless attitude towards humanity's behavior.

Modern contractarian theories tend to treat the "state of nature" not as how humans acted out in the wild before civilization but rather the natural abilities of humans. Chief among these abilities is reasoning. Both Robert Nozick and John Rawls frame their contractarian theories around the ability for collections of humans to reason together and reach mutually beneficial agreements.

Contractarianism is an interesting normative ethical theory. The reason that contractarianism is not discussed in more detail is because this thesis focusing

on deontology as its normative ethical theory of choice. Reflecting on Table 2.1, the structure of Kohlberg's theory of moral development, suggests that deontology as the embodiment of universal rights is greater than contractarianism's social contracts.

2.2.3. Meta-Ethics

Meta-ethics is a field that gained popularity and attention in the twentieth century. The goal of meta-ethics is to address problems common to all ethical theories such as how a person may obtain ethical knowledge, what normative theories have merit, or whether there is even such a thing as good or bad (moral projectivism, discussed earlier, is one such theory that discusses the latter problem).

Some meta-ethical theories attempt to answer how one becomes aware of what is and is not a moral action. A popular theory championed by the likes of G. E. Moore at the beginning of the twentieth century is known as "intuitionism." The title of "intuitionism" is somewhat incomplete because the theory states that all people can intuit an action's moral rightness or wrongness without any prior knowledge. This is *a priori* intuitionism as opposed to *a posteriori* intuitionism, which states that an answer is intuited from previously learned knowledge. Intuitionism is not a largely abandoned theory and much more work in the development of moral thinking is done in the social sciences such as psychology as opposed to meta-ethical philosophy.

As a field, meta-ethics is difficult to grasp and understand to the layman, making it outside the realm of non-philosophers. The topics discussed are both complex and hard to answer. Because of these facts meta-ethics is largely irrelevant to and ignored by the general population.

2.3. The Course of Action

Now that the general area of ethics is described this thesis can concentrate on the field of normative ethics since the stated goal is to determine prescriptive moral actions for the use of cryptography. At the same time, certain sociological data is introduced to give examples of problems in existing ethical thought concerning cryptography. Also, certain meta-ethical assumptions particular to the chose normative ethical theory are mentioned in passing. But the primary focus of the thesis remains on normative ethics.

Why is a normative ethical theory necessary? Without a theory to work from all ethical judgments are going to be morally projective. If all judgments are projective then no one person's opinion is necessarily any more valid than another persons. Working from an ethical theory allows the prescriptive actions derived from it to be valid according to the specified outlines.

Examples of weak, morally projective arguments are common among everyday computer professionals who have no ethical training. Peter Kreeft's A Refutation of Moral Relativism debunks several such weak arguments.

A primary goal of this thesis is to use a set methodology in making ethical determinations. Using a methodology gives more credence to the arguments because a structured methodology is subject to scrutiny and criticism that individual opinions are not. The lack of use of methodologies, as opposed to opinions, is a source of concern in the ongoing discussions related to cryptography and ethics.

Normative ethical theory provides the basis for conclusions of this thesis. The reason why normative theory is being used is because the normative approach best applies itself to real-life situations. Such situations should make the conclusions of the thesis more approachable to the target audience of computing

professionals because applications don't necessarily require the level of in-depth understanding that more high-level or meta theories do.

Other fields such as psychology, sociology, and law all deserve attention but space requirements for a thesis demand their exclusion. Connecting ethics to law raises enough questions to warrant a thesis or dissertation entirely of its own. And social sciences such as psychology and sociology have such a corpus of writings to date that the time required to adequately address them is longer than the amount of time available to write this thesis.

CHAPTER 3. DEONTOLOGY

3.1. Introduction

Deontology is an ethical theory that relies on certain metaphysical assumptions. The claim is that ethical knowledge exists independent of human perception. The implication of this is that there is an external, universal law of morality. Deontological theories typically rely on rights and duties. Rights are inherent to all rational beings of which humans are a member while duties are actions required of agents by the moral law.

3.2. Kant's Theory

German philosopher Immanuel Kant established the first deontological moral theory with The Grounding for the Metaphysics of Morals. This was an earlier, shorter version of his more developed theory discussed in The Metaphysics of Morals. Kant is a notoriously difficult writer to understand. Philosophers often joke about the tongue-twisting labels Kant assigns his convoluted philosophical ideas. It could be argued that he was even a poor writer in his native language of German. Translating any awkwardly written text into another language is always fraught with difficulties, but German presents a special challenge because many German words have no equivalent or even close English version. It is somewhat of a consolation then that Kant tended to write a shorter, preliminary text before unleashing his larger final work. The way Grounding precedes Metaphysics of Morals is one, but not the only, such example from Kant.

Kant's primary contribution is that of the categorical imperative and the deontological moral theory that encompasses it. Imperatives are in essence

commands for actions. Again, Kant divides them into two types: categorical and hypothetical. Hypothetical imperatives may or may not be the case, or in other words, they don't require any particular action. These are typically structured as if… then statements. An example of a hypothetical action is, "If I am hungry then I will eat a hamburger." Categorical imperatives are different because they are both universal and necessary. They always have to be the case. One categorical imperative is, "Don't kill anyone merely for the sake of killing." Hypothetical imperatives are neither universal nor necessary. In the given example, even if I'm hungry I don't need to eat a hamburger. However, I should never kill anyone merely for the sake of killing.

The words "ought" and "should" plays an important part in the semantics of Kant's deontological moral theory. This is because Kant describes imperatives as "expressed by an *ought* and thereby indicate the relation of an objective law of reason to a will that is not necessarily determined by this law because of its subjective constitution" (Grounding 24). A simpler version would be, "The moral laws are how one *ought* to action. But this action may not be the case since people are independent, practical reasoners and have personal feelings and emotions that conflict with reasoning."

Grounding continues on to three formulations derived from the idea of the categorical imperative. The formulas are the structure of the deontological theory since the categorical imperative by itself is too vague to easily make ethical judgments. The first formula is the idea of a universalizable maxim, or as the overly simplified version, the golden rule.

> Act only according to that maxim whereby you can at the same time will that it should become a universal law. (Grounding 30)

A right maxim is one that can be universalized without contradiction. If an agent thinks it is alright for himself or herself to do an action then it must also be agreeable to that agent for anyone else to do that same action. A maxim that contradicts itself is, “I will lie when I want to but everyone else must tell the truth.” The contradiction is if everyone thinks this then they know everyone else is in fact lying instead of telling the truth at they desire.

A common misconception is that universalizability makes for a rigid interpretation. If lying is wrong in situation A then it is wrong in every possible situation. Kant himself advocated this position briefly before recanting in a later talk. Although Kant later changed his interpretation this mistaken impression is being perpetuated in Introducing Ethics, a modern introductory ethics text. Such a wrongheaded notion needs to be dispelled immediately before it can cause more confusion.

The second formula describes the relationship between ends and means that is central to the deontological theory. It establishes an intrinsic worth in every human being.

> Act in such a way that you treat humanity, whether in your own person or in the person of another, always at the same time as an end and never simply as a means. (Grounding 36)

No human being should ever be treated merely as a means to some other end. Backstabbing someone in order to gain a promotion uses that victim as a means to the promotion as the ends. A key feature to notice of this formulation is the use of the word “merely.” There are admittedly times in which a person offers willingly to be a means to some other end. Most jobs function in this manner where people agree to work towards some end in return for a paycheck (O’Neill 547).

"Merely" quickly becomes an important part of the second formulation of the categorical imperative. Onora O'Neill discussed how there are situations in which a person may consent to beings a means to an end. But it is virtue ethicist Alasdair MacIntyre who points out the necessity of such relationships. Families and other supportive human groups are the focus of MacIntyre's Dependent Rational Animals. He writes of families and how "They are constitutive means to the ends of our flourishing" (102). Indeed without using members of families as means a person could not grow and learn or perhaps even survive.

> According to this principle all maxims are rejected which are not consistent with the will's own legislation of universal law. The will is thus not merely subject to the law but is subject to the law in such a way that it must be regarded also as legislating for itself and only on this account as being subject to the law (of which is can regard itself as the author). (Grounding 38)

Finally, the third formulation is the autonomy of the will. For an action to moral it first has to be the case that the agent could have done otherwise. If a robot takes a person's fist in a way that they cannot break free and uses it to punch another person in the face, the person at the mercy of the robot did not perform an amoral action because they could not possible have done otherwise.

The three formulations of the categorical imperative form the foundation for Kant's normative moral theory. This structure provides an outline for deriving prescriptions for moral actions such as those at the heart of this thesis.

3.3. Donagan's Theory

Alan Donagan takes the work of Kant and extends it into the twenty-first century. What Donagan calls his fundamental moral theory is easily recognizable as a derivation of Kant's second formulation of the categorical imperative. The

fundamental moral theory is stated by Donagan, “It is impermissible not to respect every human being, oneself or any other, as a rational creature” (66).

One of the first steps Donagan takes is to establish a separation between fundamental ethical natures and specificatory premises. His idea is that every concept has a fundamental nature to be permissible or not. Such fundamental natures are determined by whether a concept or action is permissible when examined in isolation. But sanitized, isolated environments are hardly practical to any normative ethical theory. Enter the specificatory premise, a condition that identifies whether or not the given ethical situation is compatible, or respects human beings.

Robert Nozick says there is no one who believes that there are “any or very many exceptionless moral principles” (4). It is a common misconception of Kant that a categorical imperative makes it always the case that action X is right or wrong regardless of the circumstances. The subtitle of Hackett’s version of Grounding for the Metaphysics of Morals suggests that such a conception is wrong. It reads, “On a Supposed Right to Lie because of Philanthropic Concerns.” So perhaps the categorical imperative doesn’t mean “never lie,” but does admit of some exceptions. Indeed, Kant’s original position was “Every lie is objectionable and contemptible in that we purposely let people think that we are telling them our thoughts and do not do so. We have broken our pact and violated the right of mankind.” (Lectures on Ethics 228) Kant later retracts his position when he talks about how a criminal “knows full well that [you] will not, if [you] can help it, tell him the truth and that he has no right to demand it of [you]. (227) Donagan agrees that “the principle of respect for man as a rational creature does not require that the truth be told in such a case.” (89)

Thus, the importance of the specificatory premise in Donagan’s ethical theory is to determine whether or not a given situation fits the act’s fundamental

permissibility. In effect this gives more substance to Kant's structure. The exception to the rule is no longer a blemish but rather fully incorporated into the theory as a whole.

3.4. Deontic Logic

Logic began to come into its own with the development of predicate logic by Gottfried Leibniz (10-11). Predicate logic extends standard symbolic logic by adding quantifiers and predicates. Quantifiers can be either universal (∀) or existential (∃) while predicates are used to describe properties about a given object.

Modal logic in turn extends predicate logic by including various modes along with predicate logic's standard quantifiers. Deontic logic is a member of the modal logic family, which also includes the likes of temporal and epistemic logics. The deontic logic, being influenced by deontological moral theory, is concerned with ethical logic. Modes used by deontic logics are that of permissibility (P) and obligation (O).

Ernst Mally did the first work into deontic logic (Lokhorst). This early work in deontic logic by Mally proved unsuccessful, generating a self-contradicting system. This is ironic, considering the Kant's first formulation of the categorical imperative and how it speaks of avoiding contradictions.

Georg Henrik von Wright wrote extensively on the field of deontic logic. Not only does von Wright develop his own axiomatic system of deontic logic in the same vein as Mally ("A New System of Deontic Logic"), but he does Mally one better by suggesting a conditional logic instead of a context-free system like the predecessors ("Deontic Logic and the Theory of Conditions"). It's the conditional logic and seems to be in the same line of thinking as Donagan's ethical theory.

Of additional interest is how deontic logic holds some interest among computer scientists. The Deontic Logic in Computer Sciences series of conferences discusses primarily uses of deontic logic in a computing environment. The use of deontic logic in computer science, along with the computer science basis for much of modern cryptologic theory, hints at a compatibility between the two ideas.

3.5. Summary

Deontology is a normative ethical theory that bases its conclusions on logic. While the writing style of Immanuel Kant makes the topic of deontology an imposing task it is not as complicated as it seems. The main pillar of deontology is the idea of a categorical imperative, which is something that is both universal and necessary.

The categorical imperative manifests itself in three formulations. The first is universalizability. To universalize a maxim is to be able to say that anyone else could have the same maxim without causing a contradiction or conflict. Second is ends and means. At no time should another person be used merely as a means to some other end. It should be noted that a person could be a means but only by consenting to it. Third and final is the autonomy of the will. A person must be able to do otherwise.

Universalizability causes a lot confusion for people not acquanted with deontology. To universalize doesn't mean that a particular action is always one way or another. Rather, universalizing is to take a personal maxim and see what the consequences would be if everyone had that same maxim. A maxim that causes persons to act in such a way that they contradict their own maxims is not universalizable and therefor not ethically permissible. An example of one such maxim is "I'll lie when it suits me but everyone else needs to tell the truth." If this

maxim were universalized then everyone would lie while expecting all other persons to tell the truth.

The second formulation of ends and means also proves somewhat confusing to deontology novices. The formulation says not to use another human being merely as a means to some other end. Every person has an intrinsic worth. The implied premise to the second formula is that the person being used isn't consenting to beings a means. With this premise now known it becomes apparent that a person could in principle consent to being merely a means to some other person's ends. A majority of jobs rely exactly on such a consent from workers to be a means towards some product as an end. Of course these workers are consenting to be a means in return for some kind of compensation.

The third and final formula from Kant's categorical imperative requires for the agent of an action to have an autonomous will. A simplified version of the formula could be phrased as "For an action to be right or wrong the agent must have been able to do otherwise." If a football player took the fist of a person half his size and used it to hit another person then the fist's owner couldn't have done something ethically impermissible because he or she couldn't possible have done otherwise.

All three of the formulations form a core of Kant's ethical theory. Various misunderstandings of the material still exist to this day, making the theory itself confusing to newcomers. The material of this chapter should provide the reader with an understanding of Kant's deontological theory sufficient for comprehending the rest of the thesis.

CHAPTER 4. HISTORY AND NATURE OF CRYPTOGRAPHY

4.1. Introduction

The nature of cryptography is one not usually contemplated in everyday life. Most of the general population regards cryptography to be the realm of spies, clandestinely trading envelopes full of government codes. The fact of the matter is that these people use cryptography on a daily basis often without noticing it.

While cryptography was originally the domain of armies and politicians with Machiavellian machinations it is now used by a variety of technologies in an attempt to transfer data securely. Modern web browsing software incorporate strong cryptographic technologies as a necessary feature.

If a person on the street were asked what they thought the use of cryptography was, assuming they even know what cryptography is, they would likely say, “To encode things.” But this is a recursive non-definition. Few actually consider that cryptography does not exist solely in and of itself. Also, people often equate cryptography and steganography, which is the hiding of data in plain sight.

But cryptography and steganography have differing, non-exclusive uses. Cryptography changes the actual data without trying to hide it from view. Steganography instead hides the data from view without changing any of its contents. In fact, cryptography and steganography can be used in conjunction with one another.

4.2. From Paper to Photon

Cryptography grew naturally from the earlier steganography. It was easier and more readily apparent to early humans to hide data out of sight. Later, when mathematics advanced to a sufficient stage of development, steganography matured from merely hiding data into cryptography, using mathematics to obscure the meaning of data even when in plain sight.

The Spartan *scytale* was a rod around which a length of leather strap was wound. A message was written across the strip and then unwound. The unwound strip would appear as a meaningless jumble of letters unless it was rewound on another scytale of correct length. While the jumbling of the letters was a side effect of the winding process it is effectively a transposition cipher.

Use of cryptography was prevalent in the ancient world. The Spartans paved the way for Julius Caesar and Roman politicians. The European Renaissance gathered a wealth of new knowledge both for math and cryptography. European armies relied on mathematicians to safeguard their communications.

Advancements in mechanics allowed the speed with which cryptography is conducted to increase hundred-fold. The most (in)famous instance of mechanical cryptography is the German Enigma cipher machine of World War II. Enigma was used in various instances by the German army, luftwaffe, and submarine forces most notably. Even popular culture has grasped upon the Enigma by using it as the central plot point in the movie U-571. World War II offers lots of fodder for popular cinema concerning cryptography with stories like the Enigma machine and the American Navajo code talkers, such as in John Woo's Windtalkers.

History seems to have a sense of irony because it was during the Second World War, the hey day of mechanical cryptography, that the seeds of digital

cryptography were sown. This ironic link takes on the human face of Alan Turing who is often cited as the father of computer science. Turing worked at Bletchley Park during World War Two, which is now known to have been Britain's foremost center for cryptanalysis. The cryptanalysis work Turing did at Bletchley revolved around the use of electromechanical machines. But what Turing is most renowned for is the idea of the Turing machine ("Computing Machinery and Intelligence"). Essentially a Turing machine is the most abstract digital computer possible. Later he and Alonzo Church were able to show via the Church-Turing thesis that any digital computer is reducible to a Turing machine.

Cryptography appears to be leaving the realm of digital into a new world, that of quantum mechanics. This new branch of cryptography uses physical properties as the basis of its security instead of merely mathematical principles as the current batch of digital cryptosystems do. Quantum mechanics hasn't become much easier to understand since the first days when Niels Bohr founded it. At no time can the location of a quantum particle be known for certain unlike traditional Newtonian physics, which can predict motions such as a baseball leaving a bat (Milburn 20-21).

Quantum cryptography is based on the transmission of photons, individual particles of light, polarized in a certain direction (Singh 333). The order and direction of polarizations make up the key to be used in the secured communications. What makes quantum cryptography so strong is that without knowing the proper direction of filter to use the reader effectively destroys one bit of the transaction. If an eavesdropper were to drop even a single bit, which is becomes more likely as the number of bits transmitted increases, then the two parties are effectively out of sync and the key becomes worthless. So any attempt at eavesdropping guarantees itself to fail. This is the ultimate manifestation of an unbreakable code; a code that upon which can't physically be spied.

Table 4.1 Brief timeline of cryptography developments

400 B.C.	Spartan Scytale
50 B.C.	Caesar Shift Cipher
1465	Vignère Cipher
1800	Jefferson Wheel Cipher
1917	Vernam Stream Cipher/One-Time Pad
1920	German Enigma
1976	Data Encryption Standard (DES)
1977	RSA Public Key Cryptosystem
Present	Quantum Cryptography

4.3. The Nature of Cryptography

Determining the nature of cryptography may not be as easy as it seems to be. Obviously, the interpretation of cryptography solely as a military tool is wrong as borne out by its transfer from under the auspices of the ITAR code to the Department of Commerce in the United States (Ferrera 376). This move seems to indicate cryptography as a tool not just of the military but of the commercial sector, and by correlation through the products the commercial sector produces, the average citizen.

The change in ruling from the United States government suggests that cryptography isn't necessarily the sole domain of the military but belongs to the population in general. Therefore, any normative interpretation of cryptography should consider all persons instead of solely a select group such as the military, commercial sector, or government.

What ties together people is communications. Communications allows people to share ideas, work in common, and achieve greater things than they could have alone.

4.3.1. Communications

Cryptography does not exist solely by itself. Since the purpose of cryptography is to create a random or misleading output, the purpose can't be cryptography purely for cryptography's sake because the end product is either garbage or intentionally wrong. The logical conclusion then is that cryptography is a function of communications. Without communications cryptography would have no purpose. As an example, the Information Assurance directorate of the National Security Agency, one-half of the agency's efforts, is devoted to protecting and defending the nation's communications.

Cryptography as communications requires two parties: a sender and a receiver. These may be the same person or group separated by time such as encrypting personal diary or journal entries. The goal of using cryptography is to ensure that only explicitly selected parties can gain access to the actual meaning contained in the communication. This is usually done by way of distributing a key value or password.

The uses of cryptography have developed as analogs to physical world counterparts in communication. Examples are public-private key systems such as RSA allowing digital signatures, assuring recipients of the validity of the data's author. Earlier shared key systems function like two tin cans attached by a length of string. Only the persons with the cans are able to listen to the messages.

A model often used in discussions on security, of which cryptography is an integral part, describes three aspects of security: confidentiality, integrity, and authentication. Confidentiality is often described as the equivalent of privacy in that the goal is to control the flow and access of information. Integrity is the property of that data has not been changed, destroyed, or lost in an unauthorized

or accidental manner (Shirey). Authentication combines parts of both confidentiality and integrity to verify an identity.

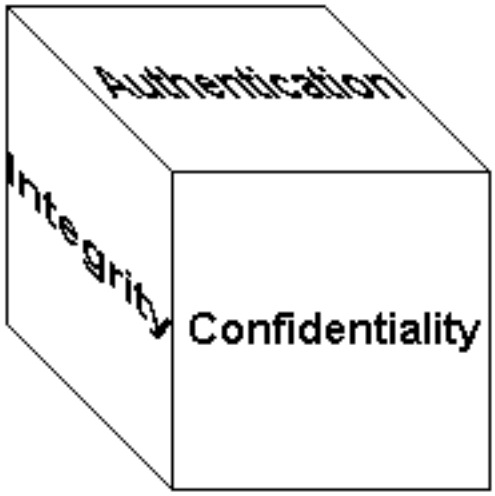

Figure 4.1 Confidentiality, integrity, and authentication as three parts of cryptography.

4.3.2. Confidentiality

Privacy using cryptography is the ability to restrict, deny, or allow access to a given communication. The term most often used by computer scientists to describe this property is “confidentiality”. While privacy, or confidentiality, is often viewed as the sole purpose of cryptography there are indeed multiple uses of cryptographic techniques other than merely hiding data.

The constitution of the United States declares that all persons have rights to “life, liberty, and the pursuit of happiness”. These are examples of negative rights, freedoms to live without interference so long as it’s down peacefully (Baase 10). As a negative right confidentiality most likely is something that should be available to all persons. This idea is pursued in more detail in the next chapter

by examining confidentiality under the scope of Kant and Donagan's ethical theories.

4.3.3. Integrity

As the pervasiveness of computing continues to increase so too does the importance that integrity plays. A lack of data integrity, leading to corruption, could cause a variety of problems such as lowered credit ratings, lost product orders, or improper medication prescriptions for patients. These problems vary in severity from annoyances to life threatening.

Integrity relies on one-way mathematical functions (Bishop 237). Such functions are simple to compute in a single direction but not both (Stinson 119). Cyclic redundancy checksum (CRC) is an early and simple example of a one-way function. A CRC is calculated by adding up all the bytes in the data, taking any overflow past a specified length and adding it back into the CRC. The advantage of CRC is that it is fast and easy to calculate, which is why it was included in the Internet Protocol (IP) from the early inception of the Internet. The disadvantage to CRC is the limited ability to detect errors. If there are too many errors then CRC won't be of much help.

The currently used method of data integrity is that of the hash function such as MD5 or SHA-1. A hash function is a one-way function like a CRC. Both functions compress a message, which is to say that a large, varying input file is always shortened to a small, fixed length output. What a hash function provides is a way of accurately detecting far more errors than CRC ever can. Furthermore, a specified property of a hash function is that any change in the input file causes multiple changes in the output file. This increases the level of security provided with hash functions because an attacker can't use trial and error, changing a sample input bit by bit, to determine what the original source of the hash was.

4.3.4. Authentication

The third and final aspect of security typically embraced is that of authentication. Authentication typically involves using both confidentiality and integrity together. Confidentiality allows the authenticating process to be certain that only the part it is communicating with can listen in while integrity makes sure that the data necessary to authenticate a source is indeed correct and accurate.

Often authentication is done through a challenge and response sequence of communications. There are several ways of doing this. One is for the challenger to ask the challangee something that he or she should know. This is the idea behind passwords. Another approach can involve public-private key encryption. Before the authentication process can begin the party being challanged needs to receive the challenger's public key in a non-repudiable way in order to be certain that the public key does indeed correspond to the person who claims it. Then, the challanger sends the challanged a piece of data that the challanged in turn signs with his or her private key and returned. If the signed data can be decrypted with the corresponding public key and is the same as was sent then the authentication succeeds.

CHAPTER 5. THE ETHICS OF CRYPTOGRAPHY

5.1. Introduction

The ideas behind deontology as an ethical system and cryptography are now explored in detail. Kant's moral theory provides an outline for what makes an ethical action. Alan Donagan continued in the Kantian tradition to explore the differing fundamental and specificatory natures of actions. The preceding chapter explored cryptography as communication and its constituent parts of confidentiality, integrity, and authentication. Each of the three parts has its own fundamental ethical nature as to whether or not it is predisposed to respecting humans as rational beings.

The difficult task undertaken by this thesis, understanding how cryptography and ethics interrelate, can now begin in earnest. The goal of this thesis is to derive prescriptions for what makes a moral act when using cryptography. Cryptography has a fundamental ethical nature and also possible exceptions, according to Donagan's deontological theory. The exceptions to an action's fundamental nature, and their related specificatory premises, could never be fully iterated. It is therefore the hope of this thesis not to provide a complete and final list of exceptions, but rather a wide and general list of exceptions that can provoke further discussions.

5.2. Fundamental Ethical Nature of Cryptography

Cryptography is a function of communications and security. A separation developed in the preceding chapter divides security into three parts: confidentiality, integrity, and authentication. The possibility exists that each of

the three aspects of security will have differing fundamental natures and specificatory premises.

5.2.1. Confidentiality

Cryptography is at its most general a way of restrictions the participants in a communication channel. It's a facilitation of both privacy and communication. Privacy qua privacy is a morally good thing since it allows people the choice of who can access certain personally important information. Kant's deontology demands an autonomy of the will in which a person must be able to do otherwise. Cryptography allows persons to do otherwise by not requiring them to shout their messages in the open (Falk 5).

Some interpretations may even require the use of cryptography in a confidential mode as part of one's moral duty. Tactical military operations is one such example. Soldiers of modern, technically advanced armies require highly sophisticated communications systems. Information can flow rapidly from individual infantrymen to a centralized command center and out to supporting air and artillery forces in a matter of minutes or even seconds. This information can contain such information as a unit's location, strength, and disposition (i.e. supplies, morale, whether or not they are currently under attack). Information like this can prove to be fatal if it were to fall into enemy hands. If an armed force were not to use encrypted communications channels they are leaving their own fighting men and women vulnerable. The military in such a situation then has a moral duty to use cryptography.

In a somewhat related way, governments too may be required to use cryptographic technologies. Certainly in an ideal world there would be no such need for nation states to hide away information. As Cordell Hull put it, "Gentlemen don't read other gentlemen's mail." But the world is not an ideal place and a much more pragmatic view is needed.

Let it be taken for granted at the time being that nation states and even societies can be morally right or wrong. Any morally right nation would surely see the wickedness they are surrounded with and realize that less scrupulous nations are going to make every attempt to steal whatever important information they possess. With this knowledge the nation now assumes the moral duty of protecting said information with strong cryptography. Not using such cryptographic protection because a nation wishes for all nations to operate in morally permissible ways is naïve at best while offering no real impetus for the morally wrong nations to change. This “cryptographic pacifism” is morally irresponsible because it leaves the citizens of the nation unprotected. Pragmatically speaking, merely acting as a moral role model ignores that changes occurring from watching such a role model only occur at later stages of ethical development, and earlier stages still require more rigid means of instruction.

5.2.2. Integrity

Integrity as defined by the Internet Security Glossary, “The property of that data has not been changed, destroyed, or lost in an unauthorized or accidental manner” (Shirey). The benefit of integrity is that is can be examined in regard to a single agent or interactions among multiple agents.

A single agent would require integrity to prevent his or her data from becoming accidentally corrupted by errors or intentionally altered or deleted by a malicious attacker. Data integrity provides rational agents with an ability to ensure the data necessary for their day-to-day lives. Therefore, data integrity is intrinsically important to living in a digital society.

Integrity between multiple agents becomes more complicated. Such integrity can be used in various communications channels. Using cryptography to ensure data integrity in such a situation may be necessary. It is not necessary to

prevent data corruption because the two parties can always retransmit, but cryptographic data integrity would facilitate matters greatly. Integrity can also be used to prevent poisoning where an attacker intentionally causes errors in the data transmission. In the case of Clifford Stoll and his story as told in The Cuckoo's Egg this may be as easy as waving a key ring full of keys through an interference-prone component of the communications channel.

It is fundamentally permissible to use cryptography as a means to enforce data integrity. Since the ability to enforce data integrity already exists, withholding it may infringe upon the negative rights of persons. As a corollary, because withholding integrity is not justified, it must be the case that integrity fundamentally respects human beings. Of course, integrity tends to respect those who use it for preserving personal information on private systems.

What about companies who are entrusted with data from persons as a part of their business plan? These companies, by taking possession of third party data, have a moral duty to use integrity for preservation. Any company who does not use integrity is negligent and allows the possibility of data corruption on its customers' data. Clearly this is not respecting the customers. This goes especially for situations when loss of data may be dangerous or even fatal such as hospitals, insurance providers, or even military or intelligence agencies. However, regardless of the consequences of the data loss, any data loss at all means a lack of respect for those whose data it is.

5.2.3. Authentication

Authentication is the product of both confidentiality and integrity. First, confidentiality is required so that the two parties involved in the authentication process are the only witnesses to the process, and to prevent outside sources from introducing erroneous data. Second, integrity guarantees that the data

party B receives is indeed what party A sends. Authentication likely fails without either constituent part.

Being the product of different parts authentication is subject to the most stringent ethical demands of any one constituent part. This is akin to how the result of a binary AND only contains the bits common to all of the operands. What this means for the ethical uses of cryptography as a means of authentication is that it is limited to either the constraints of confidentiality or integrity, whichever is more restrictive.

Integrity is defined in the earlier part of this chapter as being necessary to the positive rights of all individuals (Baase 10). Since integrity needs to be universally available then surely it isn't this component that places restrictions on authentication. Instead, it is the constraints of confidentiality that carry their burden over into authentication.

5.3. Exceptions

While cryptography is generally a morally good activity to engage in it does have its immoral uses. Cryptography in the hands of a pedophile or other criminal is a tool for morally bad actions. Just as cryptography has exceptions to its general moral nature so does cryptanalysis. Even though cryptanalysis is generally a morally bad activity there are still situations in which it can be morally good. Parents may need to monitor their children's computing activities by using cryptanalysis, or cryptanalysis may be a part of fair use for digital media such as DVD that incorporate a cipher ("The Impact of Quantum Mechanics on Cryptology and Ethics" 6).

The trend throughout this chapter as to whether or not a particular aspect of cryptography is fundamentally good is to examine the situation in which the aspect of cryptography is being used. A general rule derived from this is that

cryptography is only as good or as bad as the action it is being used in pursuit of. Cryptography is secondary to some other primary action. It is possible that determining the morality of the primary action is impractical. If one primary action relies on the determination of another then infinite regress may occur. Despite the problem of possible infinite regress, cryptography as secondary in nature never falls prey to the same problem since it is always atomic and singular unlike the complex primary action.

CHAPTER 6. CONCLUSIONS

6.1. Review

One problem with asking ethical questions about technology is the intrinsic ethical nature of a given piece of technology. This is a misunderstanding commonplace in the general populace. Technology has no intrinsic ethical nature. Take for instance a hammer sitting on a table. It seems foolish to talk about the ethical nature of this piece of technology because it isn't being used. Therefore, the real issue in question is not the technology itself but rather the actual uses of it. A hammer could be used to build a house or to bludgeon a person to death. Building a house is generally an ethically good thing because it provides shelter to persons while the brutal murder is obviously unethical. The technology can be used both for good and for bad.

Cryptography specifically has been a focus of the good versus bad debate. The collection of technological ethics writings, Computers, Ethics, and Society, contains papers from Dorothy Denning and Marc Rotenberg. Both papers deal with the strength of privacy in digital communications. Denning takes the position that wiretap laws should not be jeopardized by increasingly strong cryptographic technologies. Rotenberg writes from the opposite position of the privacy of digital communications shouldn't be compromised in order to accommodate law enforcement's ability to wiretap.

But what is an ethical action? In deciding whether or not an action is ethically permissible there are several criteria that can be examined, including the consequences of the action, the agent performing the action, and the maxim

behind the action itself. The choice used by this thesis is the latter, which is described in Immanuel Kant's deontological moral theory. The rationale behind the choice is that consequences are irrelevant because bad things can have good results and the agent is irrelevant because good people can still cause bad things, which leaves maxims and their subsequent actions.

Kant's theory outlines what specifically makes a maxim ethically permissible: it can be universalized without contradiction, it treats no one merely as a means to some other end, and the agent could choose otherwise. Contemporary philosopher Alan Donagan focuses on the second of Kant's three formulas but proposes the idea of general ethical natures and specificatory premises. Generally an action is ethically permissible or not but under certain circumstances (specificatory premises) the permissibility of an action may changed. For example, killing is ethically impermissible but there are conditions under which killing in self-defense becomes the only way to survive, making killing ethically permissible.

Peiter Zatko, the hacker better known as Mudge of L0pht fame, talks at length about dual-use technologies. Cryptanalysis tools are one such example. L0phtcrack (now known as LC5) allows uses to retrieve passwords from a Windows NT password file. The tool originally came under attack due to its popularity with criminal hackers. But Mudge defends such tools as having more than one possible use. Technology often falls prey to a "functional fixation" where often a person's first impression of the uses of the technology is what he or she carries with themselves.

The functional fixation that Mudge refers to is often a malignment of a technical tool as a device used by neer-do-wells. The converse is true with cryptography. Most people who use computers view cryptography as necessarily good because it prevents other parties from snooping in on your communications. But the truth

of the matter is that even while cryptography is a valuable tool for individuals to protect their identities it is also becoming popular among criminals who want hide their illicit activities.

Popular functional fixation concerning the uses of cryptography does prove to be somewhat correct. The popular use of cryptography, confidentiality, is indeed a generally permissible use of cryptography. But there also exist circumstances under which this usually permissible activity becomes impermissible such as criminal situations. It should be noted though that such activities aren't impermissible merely because they are illegal. Laws vary widely across nations and should by no means be taken as always morally based. Instead, criminal in this sense of the word means one who uses other people via the technology to achieve some other end. The intersection between immoral and illegal behavior is limited at best.

Confidentiality is privacy and privacy is a right to be free from outside intrusions or interference. Therefore, generally privacy is permissible because it is controlling who can or cannot influence a person's life. But the circumstances can change such that a person cannot demand the right of privacy while at the same time committing morally impermissible acts. For instance, pedophilia is impermissible because it uses children merely as a means to sexual gratification as an end. Therefore, a pedophile cannot demand the right of privacy for his immoral actions, and by corollary cannot morally use cryptography to hide his actions.

Integrity, or data integrity, is a major usage of cryptography that goes largely unnoticed by the general population. Or rather, it goes unnoticed so long as it works. When integrity of data is lost, and consequences felt, that is when people call for more integrity.

Data integrity is of use to every person, company, government, or organization. It helps prevent the accidental or intentional alteration of data. This ability to preserve and protect makes the use of cryptography for purposes of data integrity morally permissible because it is not merely protecting data for data's sake. Rather, that data belongs to a certain person and its loss may have unforeseen and dire consequences. For that reason data integrity has fewer if any possible circumstances under which it may be morally impermissible to use it. Indeed there may be circumstances for which not using cryptography for data integrity is morally impermissible such as the examples of insurance or health care providers.

Using cryptography for purposes of authentication becomes slightly more complex. Authentication by its very nature utilizes aspects of both confidentiality and integrity. Confidentiality because the number of parties in an authentication procedures needs to be tightly controlled. Think of it as the old prohibition-era gangster movies where a person walks up to a door and a slit opens to reveal a pair of beady eyes and a gruff voice challenging him or her. Integrity is used in authentication to ensure that the necessary information is indeed correct. This may include preventing tampering of the data before reaching its destination and also using hash functions to store passwords in a form that's easily verifiable yet difficult to reverse in case the file is stolen.

The composite nature of authentication makes an ethical determination for it more difficult to reach. While both are generally morally permissible, confidentiality proves to be more restrictive in its permissibility than that of integrity. It is logical then that if authentication is constructed of two parts whose ethical nature is already determined then authentication's ethical nature is determined by the most restrictive of its parts.

This is clearer when authentication is viewed also as a device for confidentiality. Essentially any authentication mechanism whether it be password, ID card, or biometric is designed to restrict access. Then the ethical nature of authentication is just as in confidentiality, depending on the actions that it is being used to conceal. For if the act is morally permissible then the person using authentication and/or confidentiality services has ever right to use them, but if the act is morally impermissible then the person has no right to demand their protection.

So cryptography is ethically permissible under different circumstances depending on the facet of security for which it is being used; confidentiality, integrity, or authentication. But all three share a common trait of having a fundamentally ethical permissible nature. That is to say in general, and the most abstract sense, using cryptography is ethically permissible.

6.2. Final Words

6.2.1. Ethical Theories

There are right actions in the world and there are wrong actions. Or, another way of phrasing it, actions can be permissible or impermissible. Moral relativism is nothing more than a temporary phase on the way to a better understanding of ethics in general. Remaining a moral relativist would merely be a person cheating himself or herself out of a large part of what makes ethics whole.

Permissibility is determined according to some normative ethical theory. Varying normative theories from the flavors of utilitarianism, virtue ethics, and deontology among others define permissibility according to differing criteria. Deontology, as the normative theory of choice for this thesis, defines permissibility according to whether or not the maxim behind the action can be universalized to all people

without contradiction, whether the action treats other people merely as means, and also whether the agent behind the action could do otherwise. This is deontology according to Immanuel Kant.

Later developments upon deontology by Alan Donagan divide the permissibility of an action into a general nature and sets of specificatory premises, or circumstances under which permissibility may or may not conform to the action's general nature.

The theories of deontology and contractarianism appeal to different levels of ethical understanding, according to Kohlberg's model of ethical development. Deontology would fit the sixth stage, which concerns universal rights. The fifth level is described as social contracts, fitting perfectly the theories espoused by Rawls and Nozick. Together the two types of theories form the entire third level of Kohlberg's theory (73).

6.2.2. Normative Interpretations

These theories provide an excellent basis for examining ethical uses of cryptography. In fact, Donagan's theory has already been applied in regards to hacking ("Hacking According to Donagan"). Hacking and cryptography are two not unrelated concerns of security in general. One of the popular worries in recent years is for strong cryptographic technologies to become common among neer-do-wells such as hackers.

But the proper usage of cryptography at its highest and most abstract is all about the responsibility of the individual. For any person to use cryptography morally he or she must be using cryptography for another moral action. This is because using cryptography merely for the sake of cryptography is meaningless and without moral essence.

Sufficiently ethically mature individuals recognize the necessity of considering the universal impact of their actions. This is not as daunting as it may seem because in order to consider an action universally a person must only imagine himself or herself in another person's shoes. At no time is it necessary to consider each and every individual in existence because the preceding exercise takes everyone into account by abstracting all people to a single, proto-human.

It is for this reason that this thesis favors deontology over contractarian ethics because any person who can follow deontological ethics necessarily follows contractarianism also. Deontology is the best of all possible normative ethical theories. This is why Kant and Kohlberg have found favor in modern cosmopolitan law theorist Jürgen Habermas.

The goal to develop a normative ethical interpretation of ethics has been met in this thesis. Cryptography is in general morally permissible to use. At no time should cryptographic technologies be withheld from the general population because there are some situations in which the use of cryptography is a duty, and preventing such a fulfillment of duty is unethical in and of itself. Even the unethical uses of cryptography by a few is no reason to deprive the many of the benefits of it.

LIST OF REFERENCES

@stake LC5 – The Award Winning Password Recovery and Auditing Tool. 2004. @stake. 1 Mar. 2005 <http://www.atstake.com/products/lc/>.

Aristotle. Nicomachean Ethics. Trans. Martin Ostwald. Upper Saddle River: Prentice Hall, 1999.

Baase, Sara. A Gift of Fire, 2nd Edition. Upper Saddle River: Pearson Education, 2003.

Bentham, Jeremy. "The Principle of Utility." Introduction to Philosophy, 3rd Edition. Eds. John Perry, and Michael Bratman. New York: Oxford University Press, 1999. 483-485.

Bishop, Matt. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.

Damon, William. "The Moral Development of Children." Scientific American Aug. 1999: 72-78.

Demonologist. "How Parents Spy on Their Children." 2600: The Hacker Quarterly 16.2 (1999): 20.

Denning, Dorothy. "Digital Communications Must Not Weaken Law Enforcement." Computer, Ethics, and Society, 2nd Edition. Eds. M. David Ermann, Mary B. Williams, and Michele S. Shauf. New York: Oxford University Press, 1997. 247-263.

Donagan, Alan. The Theory of Morality. Chicago: The University of Chicago Press, 1979.

Falk, Courtney. "The Impact of Quantum Mechanics on Cryptology and Ethics." 2005 Philosophy, Interpretation, and Culture. Binghamton University, Binghamton. 22 April 2005.

---. "Hacking According to Donagan."

Ferrera, Gerald R., Stephen D. Lichtenstein, Margo E. K. Reder, Robert C. Bird, and William T. Schiano. CyberLaw, 2nd Edition. Mason: West Legal Studies in Business, 2004.

JediMaster666. "How to Keep Parents from Spying." 2600: The Hacker Quarterly 16.2 (1999): 40.

Kant, Immanuel. Grounding for the Metaphysics of Morals. Trans. James W. Ellington. Indianapolis: Hackett Publishing Co., 1993.

---. Lectures on Ethics. Trans. Louis Infield. New York: Harper and Row, 1963.

King, Jr., Martin Luther. "Letter from Birmingham Jail." Philosophical Problems in the Law, 3rd Edition. Ed. David M. Adams. Belmont: Wadsworth, 2000. 213-219.

Kreeft, Peter. A Refutation of Moral Relativism. San Francisco: Ignatius Press, 1999.

Kohlberg, Lawrence. The Meaning and Measurement of Moral Development. Worcester: Clark University, Heinz Werner Institute, 1981.

Leibniz, Gottfried Wilhelm. Philosophical Essays. Trans. Roger Ariew, and Daniel Garber. Indianapolis: Hackett, 1989.

Levy, Steven. Crypto. New York: Penguin Books, 2002.

Lokhorst, Gert-Jan. "Mally's Deontic Logic." The Stanford Encyclopedia of Philosophy. 5 Nov. 2004. Stanford University. 8 Mar. 2005 <http://plato.stanford.edu/archives/win2004/entries/mally-deontic/>.

MacIntyre, Alasdair. Dependent Rational Animals. Chicago: Open Court, 2001.

McDowell, John. "Projection and Truth in Ethics." The Lindley Lecture. Lawrence: University of Kansas, 1987.

Mill, John Stuart. Utilitarianism, 2nd Edition. Ed. George Sher. Indianapolis: Hackett Publishing Co., 2001.

Milburn, Gerard J. Schrödinger's Machines. New York: W.H. Freeman and Company, 1997.

Neumann, Peter G. Computer Related Risks. New York: ACM Press, 1995.

Nozick, Robert. "Moral Complications and Moral Structures." Natural Law Forum 13 (1968): 1-50.

nux. "Fun at Costco." 2600: The Hacker Quarterly 16.2 (1999): 12-13.

O'Neill, Onora. "Kantian Approaches to Some Famine Problems." Introduction to Philosophy, 3rd Edition. Ed. John Perry, and Michael Bratman. New York: Oxford University Press, 1999. 546-551.

Rawls, John. The Law of Peoples. Cambridge: Harvard University Press, 2003.

---. A Theory of Justice, Revised Edition. Cambridge: Harvard University Press, 1999.

Richardson, Dave, and Chris Garratt. Introducing Ethics, 2nd Edition. New York: Totem Books, 2001.

Rotenberg, Marc. "Wiretap Laws Must Not Weaken Digital Communications." Computer, Ethics, and Society, 2nd Edition. Eds. M. David Ermann, Mary B. Williams, and Michele S. Shauf. New York: Oxford University Press, 1997. 263-268.

Shirey, R. "Request for Comments: 2828 – Internet Security Glossary." May 2000. The Internet Engineering Task Force. 5 Feb. 2005 <http://www.ietf.org/rfc/rfc2828.txt>.

Singh, Simon. The Code Book. New York: Anchor Books, 2000.

Stoll, Clifford. The Cuckoo's Egg. New York: Pocket, 1990.

Stinson, Douglas R. Cryptography: Theory and Practice, 2nd Edition. Boca Raton: Chapman & Hall/CRC, 2002.

Turing, Alan M. "Computing Machinery and Intelligence." Mind 49 (1950): 433-460.

U-571. Dir. Jonathan Mostow. Perf. Matthew McConaughey, Bill Paxton, Harvey Keitel, and Jon Bon Jovi. Universal, 2000.

Von Wright, Georg Henrik. "A New System of Deontic Logic." Deontic Logic: Introductory and Systematic Readings. Ed. Risto Hilpinen. Dordrecht, Holland: D. Reidel Publishing Co., 1971.

---. “Deontic Logic and the Theory of Conditions.” Deontic Logic: Introductory and Systematic Readings. Ed. Risto Hilpinen. Dordrecht, Holland: D. Reidel Publishing Co., 1971.

Windtalkers. Dir. John Woo. Perf. Nicholas Cage, Christian Slater, Adam Beach, and Peter Stomare. MGM, 2002.

Zatko, Peiter “Mudge”. “Re: Source Citations for Dual-Use Technologies.” E-mail to the author. 23 Feb. 2005.

LIST OF REFERENCES