DOI:10.1145/3104985

# Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic

**Cyber deterrence, like nuclear deterrence, depends on our adversaries being rational enough to be deterred by our threats but us not by theirs.**

BY MARTIN E. HELLMAN

THE 2015 ACM A.M. Turing Award recognized work I did 40 years ago, so it is understandable that my interests have changed significantly, with my most recent project being a book, *A New Map for Relationships: Creating True Love at Home & Peace on the Planet*, co-authored with my wife Dorothie. While, at first glance, the book might seem to have nothing in common with my work on cryptography, my Turing Lecture drew a number of parallels I will bring out in what follows.

The story starts in March 1975, when the U.S. National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), proposed a Data Encryption Standard (DES) to protect unclassified but sensitive data. Whitfield Diffie, with whom I shared the Award, and I quickly realized that DES's 56-bit key size was inadequate and needed to be increased.

DES had $2^{56}$, or approximately $10^{17}$, keys. We estimated that the 1975 technology would allow a single-chip search engine to check $10^6$ keys per second, so $10^6$ such chips could search the entire key space in $10^5$ seconds. That is approximately one day, and we estimated the equivalent cost to be on the order of $5,000 per recovered key. We also noted that the decreasing cost of computation—roughly a factor of 10 every five years—would rapidly reduce this cost. Even an order-of-magnitude error in our estimate would thus be erased in a short time.[3]

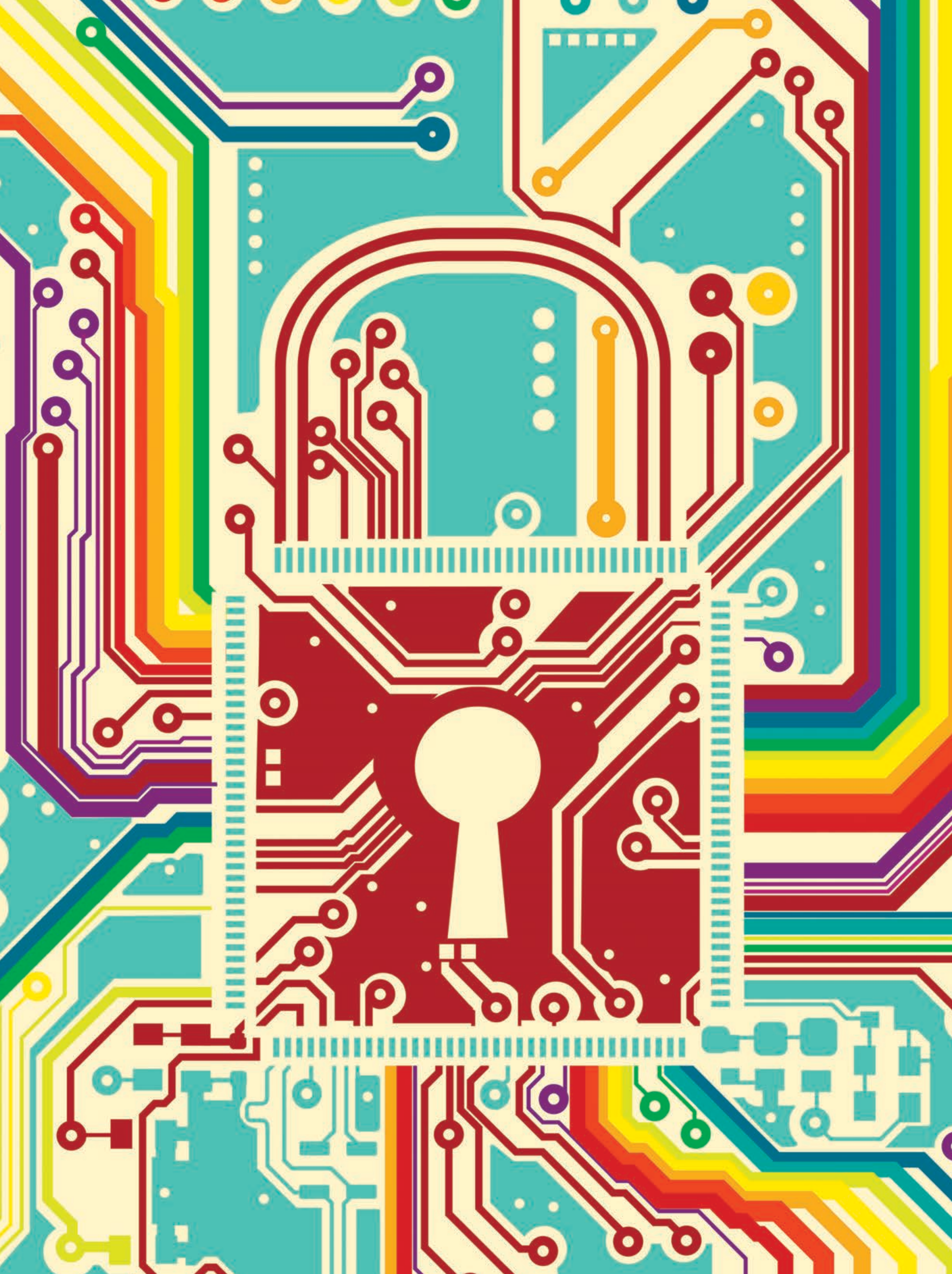
We initially thought the inadequate key size was a mistake that would be corrected once we pointed it out, but NBS resisted, claiming our estimates were off by four orders of magnitude. Our initial estimate had been a rough order-of-magnitude approximation that was adequate to show the need for an increased key size. But NBS's estimate was clearly wrong, and we came to realize we were indirectly battling the National Security Agency (NSA), in addition to NBS.

A larger key size would allow foreign governments, criminals, and terrorists to hide their communications from NSA, while 56 bits would not. What we had thought was a technical problem

## » key insights

- **While revolutionary, public key cryptography can also be viewed as a natural step in the evolution of the field of cryptography.**
- **There is greater risk than is generally recognized that a major advance in factoring and discrete logarithms might break existing public key systems.**
- **In making ethical decisions, we need to zealously guard against fooling ourselves about our real motivations.**

IMAGE BY ANDRIJ BORYS ASSOCIATES



turned out to be political. If we wanted to improve the security of the standard, we would have to treat it as a political battle by seeking media coverage and Congressional hearings—which we did.

The fight that followed was part of "the first crypto war." While the media and several members of Congress supported Diffie's and my position, we lost this part of it. DES, including its 56-bit key, was the official encryption standard from 1977 until 2002 when it was superseded by the Advanced Encryption Standard, or AES, which has a minimum key size of 128 bits.

Diffie and I recommended triple-DES[3] as a simple, albeit more expensive, way to improve DES security, but most implementations used the less-secure approach.

### Public Key Cryptography and the DES Controversy

Within a year of DES being proposed in 1975, a development—the invention of public key cryptography by Diffie and me[4] and independently by Ralph Merkle[12]—exacerbated NSA's concerns.

While Diffie and I saw a 56-bit key as small, we now know it looked large from NSA's perspective. Prior to DES, most commercial encryption systems could be broken much faster than DES, and most data was sent unencrypted, allowing access at no cryptanalytic cost.

In comparison, even $5,000 per recovered key was a huge impediment to NSA's communications-intelligence operation. But it appears to have reasoned that cost would limit the frequency of key changes so a recovered key would be useful for months, perhaps years. The invention of public key cryptography allowed keys to be changed as frequently as desired, making $5,000 per key a much more daunting barrier for an adversary.

While Diffie and I saw a 56-bit key as small, we now know it looked large from NSA's perspective.

### Evolution of Public Key Cryptography

While public key cryptography is seen as revolutionary—a characterization I love—after the following explanation, one might wonder why it took Diffie, Merkle, and me so long to discover.

Diffie and I had been talking about "trapdoor cryptosystems" (TDCs) for some time before we devised the public key concept, and it is but a small step from TDCs to public key.[4] TDCs occurred to us because, in the military, you want a highly secure cipher for use by your own troops but do not want it to be used to keep secrets from you if it is captured by your adversary. We realized that a solution was to build trapdoor information into the cryptosystem that would allow the designer to break it easily if it was used against him, but without that information his adversary would be unable to cryptanalyze his encrypted messages. While we never developed a workable TDC, the concept figured prominently in a later analysis of DES Diffie and I undertook, with others.[8] We found structures within DES that looked like they might constitute a trapdoor, although later developments indicate they were probably due to efforts to strengthen the algorithm against differential cryptanalysis.[1]

It is also noteworthy that half of the public key concept—public key exchange—occurred independently to three different groups within a short period of time.

According to documents declassified years later,[5] variations occurred in 1970, 1973, and 1974 to researchers James Ellis, Clifford Cocks, and Malcolm Williamson of the Government Communications Headquarters (GCHQ), the British agency responsible for providing signals intelligence and information assurance to that nation, though none of their work envisioned digital signatures.

Ralph Merkle, then a student at the University of California at Berkeley, developed the concept of a public key distribution system in the fall of 1974 and published it, along with a proof of concept ("Merkle puzzles"), in *Communications*, April 1978.[12]

Unaware of the still-secret GCHQ work and Merkle's budding ideas, Diffie and I proposed a more general framework—a public key cryptosystem—in the Spring of 1975. This approach included digital signatures, as well as public key exchange, with digital signatures being an entirely new idea, even within the classified community.

In May 1976, Diffie and I developed the first practical, unclassified system for public key exchange, publishing both it and the public key cryptosystem concept in our paper "New Directions in Cryptography" in *IEEE Transactions* *on Information Theory*, November 1976.[4] That public key exchange system is widely known as Diffie-Hellman Key Exchange, but somewhat ironically, it is an implementation of Merkle's public key distribution system concept, not our public key cryptosystem concept. I therefore refer to it as the "Diffie-Hellman-Merkle Key Exchange."

In light of the frequent interactions Diffie and I had, I regard everything in "New Directions" as joint work, though some scholars have noted (correctly) that Diffie devised the public key cryptosystem concept, while I discovered the Diffie-Hellman-Merkle Key Exchange algorithm. Because those individual insights were based on long-term joint work, I tend not to separate credit.

A full, working public key cryptosystem was not realized until April 1977 when Ron Rivest, Adi Shamir, and Leonard Adleman published their MIT report that, in slightly modified form, became their famous 1978 "RSA paper" in *Communications*.[17]

While Merkle's 1978 publication date—two years after "New Directions"—gives the impression that it followed in our footsteps, he submitted his paper earlier than we did, in August 1975. Its publication was delayed by an editor who initially rejected it, writing, on October 22, 1975, "I … was particularly bothered by the fact that there are no references to the literature. Has anyone else ever investigated this approach?"[6]

In the editor's defense, Merkle was a student unfamiliar with how to write and adequately reference a technical paper; the person who reviewed it (described by the editor as "an experienced cryptography expert") recommended against publishing it, noting that it ". . . is not in the mainstream of present cryptography thinking," and no one else at Berkeley, where Merkle was then a student, appreciated his work. Earlier, in the fall of 1974, a Berkeley professor discouraged him from pursuing public key distribution as a term project, telling him, "Project 2 [a much more mundane proposal] looks more reasonable, maybe because your description of Project 1 is muddled terribly." Merkle dropped the course and pursued public key distribution on his own.

### Born Classified?

NSA's concerns led it to try to control dissemination of our work.[2] In January 1976, soon after Diffie and I realized the need to treat DES's inadequate key size as a political rather than a technical problem, two high-level NSA employees flew out to California and tried to dissuade us from pursuing the matter. They basically told us, "You're wrong, but please be quiet. If you keep talking this way, you will cause grave harm to national security." But that did not compute. What they were really saying was, "You're right, but please be quiet. If you keep talking this way, you will cause grave harm to national security."

I went home that evening to decide the right thing to do. NSA was telling me the right thing was to be quiet, while my intellect told me the opposite, even from a purely national perspective. The U.S. was the world's most computerized nation, with the most to lose from insecure encryption. The Soviet Union had much less to lose and much more to gain from leaving the DES key at 56 bits. Also, NSA's request occurred soon after the Watergate revelations had shown that claims of national security could be misused to the detriment of the nation.

As I was trying to decide the right thing to do, an idea popped into my head: "Forget about what is right and wrong. You have a tiger by the tail and will never have as much chance to influence events. Run with it!"

Somehow, what would normally be an unconscious "shadow motivation" had managed to bubble to the surface and become a "devil on my shoulder," like in the movies. At the time, I thought I had brushed the devil off my shoulder and made a rational decision to go public with our analysis of the standard's weakness. But five years later, in trying to understand the motivation of the Manhattan Project scientists who developed the atom bomb during World War II, I realized I had fooled myself. Instead of doing what was right, I had figured out what I wanted to do, and then had come up with the rationalization for doing it.

I was fortunate that my decision to go public was the right one, even though I had fooled myself about my motivation. But that was sheer luck. If I had been working on the Manhattan Project, the consequences of fooling myself would have been far more grave, I vowed never to fool myself again, although implementing that decision proved tricky during Stanford University's patent fight with RSA Data Security. Space does not allow me to provide the details here, but the interested reader can find a description on pages 46–54 of our book;[7] a free .pdf file is also available at http://tinyurl.com/HellmanBook, expanding to http://www-ee.stanford.edu/%7Ehellman/publications/book3.pdf. Those same pages explain why I believe the Manhattan Project scientists fooled themselves about their motivation for working on the bomb.

The fight Diffie and I were having with NSA came to a head on July 7, 1977, when one of its employees wrote to the IEEE, claiming it was breaking the law by publishing our papers.[14] He cited the International Traffic in Arms Regulations (ITAR), which, at the time, defined anything cryptographic as an implement of war, requiring an export license. An export license was required not only for physical devices but also for technical data related to them. He claimed our papers constituted such technical data and they were, of course, exported when published internationally.

The IEEE wrote back, telling the NSA employee it was aware of ITAR, but "the burden of obtaining any Government approval for publication of technical data [was] on the person or company seeking publication," namely me and Stanford University.[14] A copy of this reply was sent to me, and I took it to Stanford's General Counsel John Schwartz both because Stanford was potentially liable and because I wanted to ensure it would defend me if I was prosecuted.

Schwartz took a few days to review the matter, after which we had a second meeting. He believed that publishing my papers was lawful but noted there was "at least one contrary view" (expressed by the NSA employee) and "should such view be adopted by the Federal Government you could be subjected to prosecution." He went on to assure me that, should that occur, "the University would defray the reasonable costs of your defense . . . nevertheless, there would always remain a risk to you personally of fine or imprisonment if the government prevailed in such a case."[19]

Schwartz also advised me to change my plans for having two students, Ralph Merkle and Stephen Pohlig, deliver joint papers at the upcoming 1977 IEEE Symposium on Information Theory. He explained that a long court case might kill the career of a newly minted Ph.D., whereas I had tenure. I relayed this to Merkle and Pohlig, telling them I had no qualms about delivering the papers but would leave the decision to them. Both said they would deliver the papers anyway but later changed their minds to assuage fears expressed by their parents.

Wanting these students to get the credit they deserved, when it was time for each paper to be delivered, I had the student co-author stand next to me at the podium. I then told the audience that, on the advice of Stanford's counsel, I would be delivering the papers, but to give the student the credit he deserved, they should consider the words coming from my mouth as if they were coming from his. This gave Merkle and Pohlig even more credit for their work than if they had delivered the talks without any threats.

## Get Curious, Not Furious

This first round of the crypto wars had mixed results. We established that independent researchers could publish papers free of government interference, but NSA was able to keep DES's key size at 56 bits.

Commercial encryption did not become truly secure until some parties on both sides of the battle learned a lesson my wife and I later emphasized in our book[7]—the need to get curious, not furious. Since the emphasis here is cybersecurity, I refer those interested in more personal details to the book's Chapter 3, also called "Get Curious, Not Furious." That same shift started a process that led to the strong encryption available on today's commercial products. It started in 1978 when I received a call from NSA saying its Director, Admiral Bobby Inman, would like to visit me and asking if I was open to the idea.

Up to that point, we had fought these battles indirectly, with no direct interchange, so I jumped at the opportunity. When Admiral Inman came to my office, he told me he was meeting with me against the advice of all the other senior people at the Agency but saw no harm in talking. He was curious, not furious. He also said it was nice to see I did not have horns—which must have been how I was being depicted at the Agency. I returned the compliment, since I had seen myself as Luke Skywalker to NSA's Darth Vader. I was in my early 30s at the time, so the young-hero model was more appropriate than it would be today, when I am 72 years old. My relationship with Inman was cautious at first but it grew into friendship as we came to appreciate one another's concerns.

Cryptography pioneers Ralph Merkle, Martin E. Hellman, and Whitfield Diffie, 1977.

The real break came in the mid-1990s when Congress requested the National Research Council undertake a study of national cryptographic policy. The study committee represented all major stakeholders, including law enforcement, national security, industry, health care, and privacy. By talking to one another—and, more important, listening to one another—we were able to reach unanimous conclusions that encouraged a significant loosening of the export restrictions on encryption products. This further example of getting curious instead of furious laid the foundation for widespread availability of strong encryption in commercial products, with export restrictions being significantly relaxed soon thereafter.

The value of adversaries talking and listening can also be seen in a 2014 interview with Admiral Inman conducted by Stanford cryptography student Henry Corrigan-Gibbs. When asked if he now would make the same decision he did 40 years ago to try to suppress our work, Inman replied, "Rather than being careful to make sure they [were not] going to damage [NSA's intelligence operations] . . . I would have been interested in how quickly they were going to be able to make [encryption widely] available." He cited the theft of portions of the F-35 jet fighter design as proof that strong commercial encryption was in the U.S.'s broader national security interests.[2]

## How Logical Is Cyber-Deterrence?

Nuclear deterrence is viewed so positively that cyber-deterrence is frequently suggested as a promising analogous next step. For example, the current Director of NSA and U.S. Cyber Command, Admiral Michael S. Rogers, told a Senate committee in 2015, "We also need to think about how can we increase our capacity on the offensive side here, to get to that point of deterrence."[18]

But how logical is cyber-deterrence? The answer depends in part on a related question treated in Chapter 8 of our book[7] (pages 243–264): "How logical is nuclear deterrence?" To summarize, consider these key points:

*We must behave irrationally.* For deterrence to work in a standoff between

PHOTO CREDIT: CHUCK PAINTER/STANFORD NEWS SERVICE

the U.S. and another nuclear-armed nation, that adversary must be rational enough to be deterred by our threats, but we must be irrational enough for its equally dire threats not to deter us. This need for irrationality on our part is usually swept under the rug, but a 1995 U.S. Strategic Command report, *Essentials of Post-Cold War Deterrence* (http://www.nukestrat.com/us/stratcom/SAGessentials.PDF), was unusually candid. After noting that instilling fear in our adversaries is "the working force of deterrence," it advised "that the U.S. may become irrational and vindictive if its vital interests are threatened should be part of the national persona we project to all adversaries."

*Nuclear deterrence must be carefully defined.* The U.S. has not carefully defined what it means by "nuclear deterrence." For example, does it mean we have nuclear weapons solely for the purpose of deterring a nuclear attack on us or our allies? That is the impression given by many statements from the U.S. government. But if that is the case, why do we use nuclear threats when the stakes are far lower?

*Impaired decision making.* World leaders have the power to start a nuclear war even when they cannot legally drive a car. Documented examples of persistent problems with alcohol[7] (pages 250–251) include Russian President Boris Yeltsin, U.S. President Richard Nixon, and British Prime Minister Tony Blair. I suspect most leaders with "fingers on the button" are occasionally similarly impaired.

*Risk.* No one knows how risky nuclear deterrence is—a subject discussed in the next section—that then relates the problem to a critical issue in encryption.

> **" . . . nevertheless, there would always remain a risk to you personally of fine or imprisonment if the government prevailed in such a case."**

## Nuclear Deterrence and Cryptography

Surprisingly, there is no evidence that the U.S. government has investigated the risk that nuclear deterrence might fail and thereby destroy civilization. (I strongly suspect the same is true of other nuclear-armed nations but have not investigated them as deeply.) No unclassified information indicates that any such studies exist. While I currently hold no clearances and could therefore be unaware of classified studies, I have discussed the possibility of such studies with sympathetic, high-level people with appropriate clearances and no evidence surfaced there either. I also have discussed undertaking such studies with high-level personnel within the U.S. Strategic Command, the successor to the Strategic Air Command, and that, too, did not produce any claims of studies, nor any real interest in investigating the level of risk.

This dearth of information on one of the most important questions facing humanity led me to spend much of the past 10 years working to bring a risk-informed framework to nuclear deterrence. As part of that effort, I published a simplified, preliminary risk analysis[9] indicating the level of risk is unacceptable.

To put such risk in perspective, even if nuclear deterrence could be expected to work for 500 years before it failed and destroyed civilization—a time horizon that sounds optimistic to most people—it would be equivalent to playing Russian roulette with the life of a child born today. That is because that child's expected lifetime is roughly one-sixth of 500 years. If the time horizon is more like 100 years, the child's odds are worse than 50/50.

My work applying risk analysis to nuclear deterrence led me to see an important and largely overlooked question in cryptography. There is much talk today about the need for "post-quantum crypto," meaning systems that would remain secure even if large quantum computers[20] could be built. But there is much less concern about possible advances in algorithms that would render both RSA and the "usual" Diffie-Hellman-Merkle Key Exchange insecure. There should be concern, as we will see. For simplicity in what follows, I talk only about factoring and RSA, but the same arguments apply equally to discrete logarithms and Diffie-Hellman-Merkle Key Exchange.

Factoring algorithms took a major step forward in the 1970s when Morrison and Brillhart[15] used Lehmer's and Powers's "continued fraction method"[11] to factor the seventh Fermat number, which is 128 bits long.

A second major advance occurred in the 1980s when American mathematician Richard C. Schroeppel used sieving to roughly double the size of the numbers that could be factored. He never published his algorithm but circulated it to many relevant researchers, and Carl Pomerance credits Shroeppel's algorithm as "the forerunner of [Pomerance's better known] quadratic sieve and also its inspiration."[16]

A third major advance in factoring occurred in the 1990s with development of the "number field sieve," again roughly doubling the size of numbers that could be factored.

While major advances in factoring occurred in the 1970s, 1980s, and 1990s, no similar advances have occurred in roughly the past 25 years, leading many mathematicians and cryptographers to believe that factoring has hit a brick wall. But I see the situation quite differently as a result of my work applying risk analysis to nuclear deterrence.[10]

Think of each decade as a coin toss that shows heads if a major advance occurs in factoring and tails otherwise. The 1970s gave us heads, as did the 1980s and 1990s, but the next decade gave us tails, and the current decade is more than half over without a major advance, so it seems more likely than not to also give us tails. Even under the optimistic assumption that no major advance occurs in the remaining years of this decade, the coin-toss sequence would be HHHTT. If a coin showed such a sequence in its first five tosses, it would be foolish to project tails into even the next decade of the 2020s with any reasonable degree of confidence.

Given the impact another major advance in factoring would have on the global economy, I have argued that it would be prudent to already have backup systems for both key exchange and digital signatures in place and in use. For key exchange, two keys could be generated and hashed or XORed. One key would be produced by public key exchange and the other by the backup system. Such a system would provide seamless security even if one of the methods of key exchange were compromised. One possible backup system would be a key distribution center that shares a master key with each user and distributes session keys on demand, encrypting the session key in each relevant user's master key. Likewise, two digital signatures could be used to sign each message, with a possible backup system being Merkle's tree signatures.[13]

**Logic is just one way of knowing about the world, and an incomplete one at that.**

## Alan Turing and My Illogical Use of Logic

The section "Illogical Logic" in our book[7] (pages 244–251) describes how supposedly highly logical people can misuse logic. In keeping with the book's aim to move from blame to responsibility, the first story in the section describes how, years ago, I misused logic as a weapon to win arguments with my wife. While I may have been winning arguments (at least in my mind), I was losing something much more important—my relationship with her. Illogical logic loses every time.

That section also describes how I felt like I was having a mental breakdown when confronted with Gödel's Incompleteness Theorem in my second year of graduate studies at Stanford. I had based my whole life on logic—not just my professional life—and logic was telling me it was literally incomplete. Because it would have complicated matters too much for the average reader, we purposely left out of that section Alan Turing's role in creating my angst. But my ACM Turing Lecture provided a wonderful opportunity to highlight how Turing helped open my mind to new possibilities.

In that second-year graduate math course, we studied the cardinality of infinite sets. The positive integers are "countably infinite" because you can count or enumerate them 1, 2, 3, . . . It was easy to see that the set of all integers is also countably infinite, with one enumeration being 0, −1, +1, −2, +2, and so on. Every integer is eventually reached in that enumeration.

It was slightly more difficult to see that the set of rational numbers is countably infinite. For simplicity, I show only the argument for positive rational numbers, though it extends easily to all rational numbers. The countably infinite sequence 1/1; 1/2, 2/1; 1/3, 2/2, 3/1; 1/4, 2/3, and so on includes all positive rational numbers. (I use semicolons to demark the end of subsequences in which numerators and denominators have a common sum, as in 1/3, 2/2, and 3/1.)

Things became much more interesting when the professor showed that the real numbers were "uncountably infinite"; that is, they form a larger infinite set that cannot be enumerated. The proof was by contradiction, using Georg

Cantor's "diagonalization argument." Assume there is an enumeration of the real numbers

$$R_1 = I_1 \,.\, b_{11}\, b_{12}\, b_{13} \ldots$$
$$R_2 = I_2 \,.\, b_{21}\, b_{22}\, b_{23} \ldots$$
$$R_3 = I_3 \,.\, b_{31}\, b_{32}\, b_{33} \ldots \text{ and so on}$$

where $R_i$ is the (assumed) $i^{th}$ real number, $I_i$ is its integer part, and $b_{ij}$ is its $j^{th}$ binary decimal place . To complete the proof, consider the real number

$$R = 0 \,.\, {\sim}b_{11}\, {\sim}b_{22}\, {\sim}b_{33} \ldots$$

where ${\sim}b_{jj}$ is the complement of $b_{jj}$. This real number R is different from $R_1$ since they differ at least in their first binary decimal places. It is different from $R_2$, since they differ at least in their second binary decimal places. Similar arguments apply to each $R_i$ in the assumed list. We had assumed the list included all the reals, but R is not in the enumeration, so the reals are not countably infinite.

So far, I was not too perturbed. But then the professor defined the computable real numbers, a concept first introduced by Turing in his brilliant 1936 paper.[21] A computable real number is one that can be computed to as many decimal places as desired in a finite (though indeterminate) time by a finite-length program. While, at first, this set might seem to depend on the machine being used, that problem was removed by using a Universal Turing Machine that can simulate any other physical computer with only a finite increase in program size and run time over what would be needed on the machine being simulated.

The set of finite-length programs can clearly be enumerated, as in 0, 1, 00, 01, 10, 11, 000, and so on. Since not every finite-length program produces a computable real number—some get hung up in infinite loops and provide no output—the set of computable real numbers is also countably infinite. But the professor then seemed to prove that the computable real numbers were uncountably infinite by writing the following program:

```
Print 0 and a (binary) decimal
point, so that what follows
is the binary expansion of a
computable real number.
FOR i=1, i++
{Compute $b_{ii}$ the $i^{th}$ binary
decimal place of the $i^{th}$
computable real number, and
print ~$b_{ii}$}
```

This reasoning, drawn from Section 8 of Turing's paper, is almost exactly the same as was used to prove the real numbers are not countable. But there is a difference, as there must be, since the "proof" here produced a contradiction to a known fact: The computable real numbers are countable.

This line of reasoning involves a very subtle, hidden assumption—that there exists a computable enumeration of the computable real numbers. An enumeration exists, but we can never compute it. In a sense, only God knows it, while we mortal humans cannot.

I was dumbfounded. If an incorrect assumption can be that subtle, what others might have been missed in other proofs? Is mathematics itself on a firm foundation? Might Cantor's proof that the reals are uncountably infinite have a similar flaw? (I still wonder about that.)

My world was shaken in that course, but not enough for me to give up logic as the primary basis for my personal and professional life. That took 10 more years and almost ruining my marriage before I finally accepted what Gödel and Turing had been implicitly telling me: Logic is just one way of knowing about the world, and an incomplete one at that.

I learned the limits of logic in time to save my marriage. Will humanity learn the limits of its current logic in time to save the world and itself? Dorothie and I wrote our book partly to increase those odds, even if just a bit. That provides yet one more connection between the work that won me the ACM A.M. Turing Award and the book. What is the point of developing elegant algorithms (such as Diffie-Hellman-Merkle Key Exchange) if no one is around in 100 years to use them? C

**References**

1. Coppersmith, D. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development 38*, 3 (May 1994), 243–250.
2. Corrigan-Gibbs, H. Keeping secrets. *Stanford Magazine* (Nov./Dec. 2014), 58–64; http://tinyurl.com/cyptowar1, expanding to https://alumni.stanford.edu/get/page/magazine/article/?article_id=74801
3. Diffie, W. and Hellman, M. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer 10*, 6 (June 1977), 74–84; http://www-ee.stanford.edu/%7Ehellman/publications/27.pdf
4. Diffie, W. and Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory IT-22*, 6 (Nov. 1976), 644–654; http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf
5. Ellis, J. The history of non-secret encryption. *Cryptologia 23*, 3 (1999), 267–273.
6. Graham, S. *Letter to Ralph C. Merkle* (Oct. 22, 1975); http://www.merkle.com/1974/RejectionLetter.pdf
7. Hellman, D. and Hellman M. *A New Map for Relationships: Creating True Love at Home & Peace on the Planet.* New Map Publishing, Stanford, CA, 2016; http://tinyurl.com/HellmanBook, expanding to http://www-ee.stanford.edu/%7Ehellman/publications/book3.pdf
8. Hellman, M., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., Pohlig, S., and Schweitzer, P. *Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard.* Technical Report SEL 76-042 (available from NTIS). Electrical Engineering Department, Stanford University, Stanford, CA, Sept. 9, 1976 (revised Nov. 10, 1976); http://tinyurl.com/nbs-des-analysis, expanding to http://www-ee.stanford.edu/~hellman/resources/1976_sel_des_report.pdf
9. Hellman, M. Risk analysis of nuclear deterrence. *The Bent of Tau Beta Pi 99*, 2 (Spring 2008), 14–22; http://tinyurl.com/hellman74, expanding to http://www-ee.stanford.edu/%7Ehellman/publications/74.pdf
10. Hellman, M. How risky is nuclear optimism? *Bulletin of the Atomic Scientists 67*, 2 (Mar. 2011), 47–56; http://tinyurl.com/HowRisky, expanding to http://www-ee.stanford.edu/~hellman/publications/75.pdf
11. Lehmer, D. and Powers, R. On factoring large numbers. *Bulletin of the American Mathematical Society 37*, 10 (1931), 770–776.
12. Merkle, R. Secure communication over insecure channels. *Commun. 21*, 4 (Apr. 1978), 294–299.
13. Merkle, R. A digital signature based on a conventional encryption function. In *Advances in Cryptology, CRYPTO 1987, Lecture Notes in Computer Science, Vol. 293* (Santa Barbara, CA, Aug. 16–20). Springer-Verlag, Berlin, Heidelberg, Germany, 1988, 369–378.
14. Meyer, J. Letter to IEEE (July 7, 1977); https://stacks.stanford.edu/file/druid:wg115cn5068/1977%200707%20Meyer%20letter.pdf and https://purl.stanford.edu/wg115cn5068
15. Morrison, M. and Brillhart, J. A method of factoring and the factorization of F7. *Mathematics of Computation 29*, 129 (Jan. 1975), 183–205.
16. Pomerance, C. A tale of two sieves. *Notices of the AMS 43*, 12 (Dec. 1996), 1473–1485.
17. Rivest, R., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM 21*, 2 (Feb. 1978), 120–126.
18. Sanger, D. U.S. must step up capacity for cyberattacks, chief argues. *The New York Times* (Mar. 20, 2015), A4.
19. Schwartz, J. Memo to Martin Hellman (Oct. 7, 1977); https://stacks.stanford.edu/file/druid:wg115cn5068/1977%201007%20Schwartz2MH.pdf
20. Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing 26*, 5 (1997), 1484–1509.
21. Turing, A. On computable real numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, Series 2 42 (1936), 230–265; https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf

**Martin E. Hellman** (martydevoe@gmail.com) is Professor Emeritus of Electrical Engineering at Stanford University, Stanford, CA.

Watch the author discuss his work in this exclusive *Communications* video. https://cacm.acm.org/videos/cybersecurity-nuclear-security-alan-turing-and-illogical-logic