

**Mathematics,
Communication
and Secrecy**

a history of the development of digital cryptography

Richard W. Beveridge

“If the theory of numbers could be employed for any practical and obviously honourable purpose, if it could be turned directly to the furtherance of human happiness or the relief of human suffering, as physiology and even chemistry can, then surely neither Gauss nor any other mathematician would have been so foolish as to decry or reject such applications. But science works for evil as well as good (and particularly, of course, in time of war); and both Gauss and lesser mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

G.H. Hardy

Communication & Secrecy

Definitions of communication vary so widely that Frank Dance and Carl Larson list over 120 different definitions as an appendix to their 1976 book *The Functions of Human Communication*. They provide a working definition of their own by identifying what they consider to be the essential attributes of human interpersonal communication. They state that communication is (1) symbolic content (2) produced by an individual (3) according to a code, (4) with anticipated consumption by others (5) according to the same code. Because of the wide variety of definitions, many different types of phenomena can be classified as communication. Many of these phenomena are amenable to mathematical analysis.

In the natural world, communication may take many forms. At the cellular and multi-cellular level, communication is often accomplished through chemical secretion. Slime molds and bacteria use chemical secretion to encourage surrounding cells to aggregate in certain situations. Both the chemical signaling and the subsequent aggregation can be modeled through the techniques of mathematical biology.

In order to communicate the location of nectar and pollen, honeybees perform intricate dances that convey both the distance and direction of the food source. Professor Barbara Shipman of the University of Texas at Arlington has found that the patterns of the honeybees' dance are modeled in the geometry of a six dimensional space known as a flag manifold. This mathematical model also predicts the two types of dances the bees do - the "round dance" for nearby food and the "waggle dance" for more distant food.

In human civilizations, there exist a wide range of phenomena that can be classified as communication. In addition to spoken and written communication, these include drumming, whistling, and dance,. Human speech is a particularly important form of communication that also employs many non-verbal aspects such as inflection, volume, posture, and gesture. Each of these various forms of communication employs a particular code with the anticipation that those intended to receive the message will be able to comprehend it.

In certain situations, however, individuals may generate symbolic content with the anticipation that others may not be able to comprehend it. In this situation, what is desired is a restriction of the audience for the communication, or privacy regarding the content of the message. Parents often spell words in front of young children if they wish to discuss a topic without the children's understanding. *Pour quelqu'un qui ne parle pas une langue étrangère, cette langue est un code effectif.* If you are able to read the previous sentence, then it is obvious that communication in French is not a particularly effective form of code. However, there are other languages that, historically, have been proven to be very effective forms of code. This was apparent in the great success that the Native American code talkers experienced in the U.S. military during the First and Second World Wars.*

Alan Westin, in his 1967 book, *Privacy and Freedom*, defines privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Senator Edward V. Long of Missouri, who headed a U.S. Senate Subcommittee's investigation on the Invasion of Privacy in 1966, said that privacy is "exercising control over the number of participants in our communications." Hence, we see immediately that in the consideration of any form of communication there exists a corresponding consideration of privacy.

In the absence of personal privacy, an individual's behavior has a tendency to become false and deceptive. Allowing for privacy is a society's acknowledgement of the importance of the individual. One of the hallmarks of a totalitarian society is a lack of privacy. Just as communication and privacy seem common to all human cultures, so too is the tendency of individuals to invade the privacy of others. Human beings of all cultures typically feel a natural sense of curiosity about the behavior of others, although there exist a variety of cautionary tales about the dangers of too much curiosity (e.g. Pandora's box).

* Cheyenne, Comanche, Cherokee, Choctaw, Osage, and Yankton Sioux in WW I. Chippewa, Choctaw, Comanche, Creek, Hopi, Kiowa, Menominee, Muscogee/Creek-Seminole, Navajo, Oneida, Pawnee, Sac & Fox, and Sioux (both Lakota and Dakota dialects) in WW II.

Electronic Communication

The development of the telegraph during the first half of the 19th century created a new medium for human communication – electrical impulses sent over wires. By the end of the 19th century, the wireless electronic communication of radio would further revolutionize communication. Almost as soon as electronic communication existed in a feasible manner, the human impulse to eavesdrop appeared with it. David Kahn, in his seminal work on cryptology, *The Codebreakers*, states the telegraph created modern cryptography; the radio, modern cryptanalysis.*

In 1862, the state of California passed legislation prohibiting the interception of telegraph messages. In 1864, a stockbroker in California was prosecuted for attempting to intercept news of stock operations coming from the East in order to sell this information to his clients. During the Civil War, both the Union and Confederate armies employed wiretappers to intercept opposing side's messages. A former Civil War wiretapper who found employment with a Boston newspaper after the war was exposed as a fraud when it was discovered that his reporting was simply lifted from the wire dispatches of other newspapers. California extended its wiretapping legislation to include telephones in 1905, after the *San Francisco Call* accused its rival, the *San Francisco Examiner* of tapping the phones of the *Call*'s reporters to steal the newspaper's exclusives.

The New York City Police Department was discovered to have engaged in widespread wiretapping between the 1892 and 1938, although wiretapping was prohibited by New York State law. The NYPD felt that this law applied only to private citizens. Although the legislature passed a law in 1918 prohibiting law enforcement wiretapping without court authorization, the governor vetoed this legislation. It was speculated that he feared that the new law would inhibit the federal secret service during a time of war. Finally, in 1938, the New York State constitution search and seizure clause was amended to prohibit police wiretapping without court approval.

* Cryptography refers to the encipherment of messages into code, whereas cryptanalysis refers to the attempts to break a code. Cryptology is the study of these two competing endeavors.

Wiretapping was widespread during the prohibition years and was the primary means of enforcement and prosecution under the 18th amendment and the Volstead Act. The prevalence of wiretapping during the 1920's eventually led to the *Olmstead v. U.S.* Supreme Court decision of 1928. Roy Olmstead was a Seattle bootlegger who had been arrested due primarily to information gained over wiretaps installed by federal agents without court approval. Because the agents had not entered any private homes and thus had not technically violated the provisions of the Fourth Amendment, the Supreme Court upheld Olmstead's prosecution. However, in the dissenting opinion, Justice Louis Brandeis stated that the makers of the Constitution had conferred the "right to be let alone" to all Americans and that the extension of communications technology required a parallel extension in the interpretation of the Fourth Amendment.

Signals Intelligence and the World Wars

At the outset of World War I, Britain hauled Germany's transatlantic cables out of the North Sea and severed them, forcing the Germans to communicate using radio or over cables that were controlled by unfriendly nations. It was due to this action that several years later the British were able to intercept and decode the infamous Zimmerman telegram which proposed a German-Mexican alliance in the event that the United States entered the conflict.

While wiretapping was an important method to intercept messages, the public nature of radio communications resulted in a far greater number of intercepted messages. The amount of coded text that is available for analysis greatly affects the chances of breaking the code. A great deal of code-breaking activity is based on repetition and the appearance of certain key words. One of the first steps in breaking a code is often a frequency analysis. A frequency analysis can help determine what language a message is in if the letters have simply been rearranged. It can also help to break a code that is based on a substitution alphabet. The more coded text that becomes available, the more accurate and more helpful a frequency analysis is likely to be.

During World War II, American war planes began carrying Identification Friend or Foe (IFF) devices in order to reduce the incidence of planes being shot down by friendly fire. These early devices were somewhat primitive and not secure against replication by the enemy. After the war, the Air Force worked to improve this device through the use of cryptography. A prototype was built at the Air Force Cambridge Research Center (AFCRC) during the early 1950's. While it was an improvement over the devices used during the war, there were still weaknesses.

Horst Feistel began working at the AFCRC in 1944, shortly after he became a citizen of the U.S. Feistel was a naturalized American citizen who had emigrated from Germany in 1934. During the war, he was required to report his movements to the government if he left the Boston area. Feistel was concerned that the new IFF device had not been adequately tested and set a team of mathematicians to work to analyze the system. This group discovered the weaknesses in the system and suggested improvements. In the process, they also made some major advancements in mathematical cryptography.

After the creation of the NSA in 1952, the AFCRC was shut down and work on cryptography was discouraged anywhere but the NSA. Feistel then worked for MIT's Lincoln Laboratory and its spin-off the Mitre Corporation during the late '50's and early '60's. He attempted to set up a cryptography group at Mitre, but due to the control exerted by the NSA, Feistel was unsuccessful in these efforts and moved on to the IBM T.J. Watson Research Laboratories in Yorktown Heights, New York.

Whitefield Diffie

In 1961, Whitfield Diffie enrolled at the Massachusetts Institute of Technology. He had grown up in New York City, where his father was a history professor at the City College of New York (CCNY). Stories of Diffie's eccentricity are numerous and seemingly cover every period of his life. From his learning to read at age ten to the menagerie of exotic pets that he kept while a student in Cambridge, it is safe to say that

Whitfield Diffie was an uncommon young man when he graduated from MIT in 1965 with a Bachelor's degree in Mathematics.

After graduation, Diffie began working at the M.I.T. Artificial Intelligence Lab writing LISP code for the Mitre Corporation's mathematical software project. It was there that he became interested in the more philosophical aspects of computer science in general and the idea of proofs of the correctness of programs in particular. In June of 1969 Diffie met John McCarthy, who was working on the same ideas at Stanford. Diffie and McCarthy began talking about their work, and McCarthy ended up offering Diffie a job at the Stanford University Artificial Intelligence Lab. Diffie accepted and moved to Palo Alto in 1969.

During his time at the Stanford Artificial Intelligence Lab, Diffie often talked with John McCarthy about many of the concepts that lay at the heart of the rising need for data security. If electronic documents were to replace paper documents, then digital authentication would be of paramount importance. In particular, the problem of a "digital signature" became a focus of their conversations.

All this remained a sideline for Diffie until 1972, when Larry Roberts approached John McCarthy, asking him about ways to develop cryptographic protection for a project he was working on. At the time, Roberts was the director of information-processing techniques for the Department of Defense's Advanced Research Projects Agency (ARPA) and his project was the ARPAnet, which would link major computer systems for universities, research centers, and government agencies.

McCarthy and the other researchers at the lab then began to work on the problem. Diffie eventually became engulfed in the cryptography work to the exclusion of all other projects and, in the spring of 1973, he took a leave of absence from the Lab to focus on cryptography. Understanding of cryptography was very closely guarded at the time, and there were no generally available resources on the subject. Most of the people who knew anything about cryptography worked for the National Security Agency (or NSA), the famously secretive government agency created by President Truman in 1952 to deal with communications security and intelligence.

Diffie left Palo Alto that spring and took to the road in a black Datsun 510 automobile on a crusade to learn all that he could about cryptography. He had saved most of his salary from the Mitre Corporation and used this to fund his cryptographic odyssey. Diffie crisscrossed the country for nearly two years hunting down dusty tomes in various libraries and visiting universities and think tanks to interview experts, all in an effort to increase his understanding of cryptography. Finally, in late 1974, he found Martin Hellman, a man who would become Diffie's partner and collaborator. Together, using the ideas of Gauss and Euler, they would help change the face of computer science, cryptography and American society.

The need for data security

One of the major problems confronting computer scientists of the 1960's and 70's was data security. Computers had incredible potential in facilitating communication and in data storage and transmission, but the data had to be secure, otherwise the computer's utility would be severely limited. During the 1960's, a concerted effort was made to develop secure cryptosystems to protect electronic data.

In 1965, the National Bureau of Standards (today called the National Institute of Standards and Technology) was authorized to develop standards governing the purchase and use of computers by the federal government. As a result of this mandate, the NSB began a study in 1968 to determine the data security requirements of the federal government. By the early 70's, the NSB had begun soliciting submissions for a government-wide encryption standard that would be applicable to non-classified government data and to proprietary commercial data as well.

Also in the late 1960's, Horst Feistel was working on a cryptosystem for electronic data at the IBM research lab. By 1971, Feistel and IBM began patenting their system, which was quickly implemented by Lloyds Bank in their Cashpoint ATM system. Large commercial banks were particularly hungry for secure electronic transmissions due the nature of their business. The ability to transact banking

electronically would save banks enormous amounts of money once they could ensure the security of the electronic transmissions.

Diffie and Hellman search for a solution

In the summer of 1974, Diffie was living temporarily in Cambridge again in order to attend a seminar on cryptography. He also made time that summer to drive to the New York suburbs to visit the researchers at the T.J. Watson Research Center in Yorktown Heights, N.Y. Although Horst Feistel was based at Yorktown Heights, he was away when Diffie visited. It was at the Watson Research Center that one of the researchers told Diffie about someone who had worked there a few years before and was also interested in cryptography - Martin Hellman.

Hellman was now an assistant professor of Electrical Engineering at Stanford University, back in Palo Alto, where Diffie had begun his quest the previous year. As it turned out, Diffie had agreed to house-sit for his former boss at Stanford, John McCarthy. So, in late 1974, Diffie returned to the Bay Area and got in touch with Martin Hellman. An initial half-hour meeting stretched into dinner and then late into the evening. Finally, Diffie and Hellman agreed to meet again later to continue their discussion.

Eventually, Hellman would formally hire Diffie as a research assistant, although they worked together as equals. Hellman and Diffie began running a seminar on cryptography and trying to work out the problems involved in creating a secure cryptographic system. The problem on which Diffie and Hellman focused their attention in creating this system was that of finding what is known as a "one-way" function. This is a function whose computation would be trivial for a computer to execute, but would be extremely difficult to reverse.

In their famous 1976 paper "New Directions in Cryptography," Diffie and Hellman describe their search for a one-way function:

Polynomials offer an elementary example of one-way functions. It is much harder to find a root x_0 of the polynomial equation $p(x) = y$ than it is to evaluate the polynomial $p(x)$ at $x = x_0$.

For example, it is easy enough to find $x^5 + 5x^2 - 2x + 3$ when $x = 2$, but trying to determine what value of x will make $x^5 + 5x^2 - 2x + 3 = 51$ is somewhat more difficult.

Even this does not fully convey the type of problem Diffie and Hellman were working on because roots in our conventional number system may be found by successive approximation. In the number systems first conceived of by Euler and Gauss, both 5^8 and 6^8 may be 16, while 8^8 and 9^8 are both 1. This is the one-way function known as the Discrete Logarithm Problem. Because of the unpredictable nature of Discrete Logarithms, in order to attempt to break a code that uses Diffie and Hellman's applications of Gauss and Euler's ideas, a computer is forced into a brute-force search of an entire number system.

The Discrete Logarithm Problem

The Discrete Logarithm Problem involves modular number systems, which are finite number systems that operate in much the same way as our standard number system, with one important difference. Modular systems use only a finite group of numbers. Whenever a calculation results in a number greater than the modulus that defines the system, this answer may be reduced to an equivalent number that is less than the modulus. Two numbers are said to be equivalent, or congruent, if their difference is divisible by the modulus. This system generates a finite series of congruence classes that include all the integers.

For example, if the modulus is 5, then the congruence classes will be

- {...-15, -10, -5, 0, 5, 10, 15.....}
- {...-14, -9, -4, 1, 6, 11, 16.....}
- {...-13, -8, -3, 2, 7, 12, 17.....}
- {...-12, -7, -2, 3, 8, 13, 18.....}

{...-11, -6, -1, 4, 9, 14, 19.....}

Notice that all of the numbers in the congruence class for 2 will leave a remainder of 2 when divided by 5.* Any integer not in the set of numbers {0,1,2,3,4} may be reduced to what is called its least positive residue in this number system. As a result, calculations in a modular system may produce somewhat unexpected results. As noted earlier, in mod 17, 5^8 and 6^8 are both 16, while 8^8 and 9^8 are both 1.

The unpredictable nature of the arithmetic of modular systems is what allowed Diffie and Hellman to create a one-way function that is trivial for a computer to calculate, but incredibly time-consuming for a computer to reverse. For example, given that $5^x \equiv 10 \pmod{17}$, there is no standard algorithm for computing x other than calculating all the powers of 5 to discover that $5^7 \equiv 10 \pmod{17}$. This particular problem would not be very time-consuming (even if done by hand). However, in implementing these ideas, a modulus whose decimal representation has over 200 digits is generally used. This creates a situation that would occupy an unreasonably large amount of computational time.

Bringing crypto to the masses

Once Diffie and Hellman had settled on their cryptographic system, a long period of testing and refining followed in order to ensure that the system was secure. As their results were made public, other researchers began to work from their ideas and create further applications of Discrete Logarithms. Inspired by Diffie and Hellman's 1976 paper, three M.I.T. professors, Ron Rivest, Leonard Adleman, and Adi Shamir, developed what became known as the RSA cryptosystem. In April of 1977, the three researchers finished their paper on the system and sent copies to a number of mathematicians and computer scientists, including Diffie and Hellman. They also sent a copy to Martin Gardner, who wrote a column for Scientific American called "Mathematical Recreations." Gardner devoted his August 1977 column to the work of

* The remainder is defined as a positive integer, so that, for example $-13 = (-3 \cdot 5) + 2$

Diffie and Hellman and Rivest, Shamir and Adleman. The resulting publicity created an avalanche of attention for cryptographic researchers and the possibility for mathematicians to turn their ideas into a business.

One of the first companies to use the RSA cryptosystem was a software developer called Iris Associates. In the early 1980's, Iris Associates was working on the software for the Lotus Development Corporation's Lotus Notes program. Many other businesses soon saw the benefits of the applications of RSA and other, similar cryptosystems. As time went on, the proliferation of strong commercial cryptographic resources allowed businesses to exploit the full communication potential of computers. Once the WorldWideWeb became established, businesses were also able to buy and sell their products over the web with an acceptable level of assurance that information like credit card numbers would not be intercepted.

The National Security Agency has always had a difficult relationship with cryptography for public use. Anyone interested in the NSA and their part in the story of cryptography will find information regarding this in Bruce Schneier's *The Electronic Privacy Papers* and Stephen Levy's *crypto* as well as James Bamford's books *The Puzzle Palace* and *Body of Secrets*, and David Kahn's *The Codebreakers*.

Mathematically speaking, the most wonderful aspect of modern cryptography is the application of 200-year-old ideas that were first considered purely for the logical connections that existed in the arithmetic operations. To the question of whether or not the work of pure mathematicians is of practical value to our society, the answer must be emphatically yes. While mathematical ideas do not always find immediate application, sometimes the most esoteric mathematical concepts can find their way into the most commonplace aspects of our society.

References

- Dallon, J.C., Othmer, H.G., "A discrete cell model with adaptive signaling for aggregation of *Dictyostelium discoideum*," *Philosophical Transactions of the Royal Society: Biological Sciences*, London B 352 (1997), 391-417.
http://www.pubs.royalsoc.ac.uk/phil_trans_bio_homepage.shtml
- Dance, Frank E. X., Larson, Carl E., *The Functions of Human Communication: a theoretical approach*, Holt, Rinehart and Winston, 1976.
- Dash, Samuel, Knowlton, Robert E., Schwartz, Richard F., *The Eavesdroppers*, Da Capo Press, New York, 1971.
- Diffie, Whitfield and Hellman, Martin E., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, v. IT-22, n. 6, Nov. 1976, pp. 644-54.
- Diffie, Whitfield and Landau, Susan, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 1998.
- Gauss, Carl Friedrich, *Disquisitiones Arithmeticae*, Yale University Press, 1966. (Translation from the 1870 Latin 2nd ed. by Arthur A. Clarke, S.J.)
- Hellman, Martin E., "The Mathematics of Public-Key Cryptography," *Scientific American*, v. 241, n. 8, Aug. 1979, pp. 146-157.
- Kleiner, Israel, "The Evolution of Group Theory: A Brief Survey," *Mathematics Magazine*, vol. 59, n. 4, Oct. 1986.
- Leech, David P., Chinworth, Michael W., "The Economic Impacts of NIST's Data Encryption Standard (DES) Program," Planning Report 01-2, National Institute of Standards and Technology, Program Office, Strategic Planning and Economic Analysis Group, October 2001.
(<http://www.nist.gov/director/prog-ofc/report01-2.pdf>)
- Liska, Jo, Cronkhite, Gary, *An Ecological Perspective on Human Communication Theory*, Harcourt, Brace & Co., 1995.
- Levy, Steven, *crypto*, Penguin Books, 2002.
- Long, Senator Edward V., *The Intruders: The Invasion of Privacy by Government and Industry*, Frederick A. Praeger Publishers, New York, 1966.
- Meadows, William C., *The Comanche Code Talkers of World War II*, University of Texas Press, Austin, 2002.

Schoeman, Ferdinand D. ed., *Philosophical Dimensions of Privacy*, Cambridge University Press, 1984.

Schoeman, Ferdinand D., *Privacy and Social Freedom*, Cambridge University Press, 1992.

Shipman, Barbara, "The Geometry of the Honeybee's Dance," Presentation at the MAA/Texas Section Spring meeting 2002, Eastfield College, Mesquite, Texas.

Westin, Alan F., *Privacy and Freedom*, Atheneum, New York, 1967.

In 1890, future U.S. Supreme Court justice Louis Brandeis and his Harvard Law School classmate and law partner Samuel D. Warren wrote a famous Harvard Law Review article titled "The Right to Privacy." In this article, Brandeis and Warren saw the possibilities inherent in the new communication technologies of the late 19th century. At the time, the newest technologies were telegraphy and still photography. In these new forms of communication, Brandeis and Warren saw the potential for the types of invasion of privacy that would become ubiquitous 100 years later with the rise of the paparazzi and tabloid journalism in the late 20th and early 21st century.