Alice and Bob: A History Of The World's Most Famous Couple

Alice and Bob are the world's most famous cryptographic couple. Since their invention in 1978, they have at once been called "inseparable," and have been the subject of numerous divorces, travels, and torments. In the ensuing years, other characters have joined their cryptographic family. There's Eve, the passive and submissive eavesdropper, Mallory the malicious attacker, and Trent, trusted by all, just to name a few.

While Alice, Bob, and their extended family were originally used to explain how public key cryptography works, they have since become widely used across other science and engineering domains. Their influence continues to grow outside of academia as well: Alice and Bob are now a part of geek lore, and subject to narratives and visual depictions that combine pedagogy with in-jokes, often reflecting of the sexist and heteronormative environments in which they were born and continue to be used. More than just the world's most famous cryptographic couple, Alice and Bob have become an archetype of digital exchange, and a lens through which to view broader digital culture.

This website details the major events in the "lives" of Alice and Bob, from their birth in 1978 onwards. It is also the public, multimedia component for a related academic research project by Quinn DuPont and Alana Cattapan.

Synopsis

Alice and Bob are fictional characters originally invented to make research in cryptology easier to understand. In a now-famous paper ("A method for obtaining digital signatures and public-key cryptosystems"), authors Ron Rivest, Adi Shamir, and Leonard Adleman described exchanges between a sender and receiver of information as follows: "For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem." In that instant, Alice and Bob were born.

Within a few years, references to Alice and Bob—often in the opening sentence to an academic article—were *de rigeur* for academic cryptology research. And as cryptology became a standard part of computer science and engineering curricula, faculty began to portray Alice and Bob in a classroom setting using clip art and other images that personified Alice and Bob (usually in white, heteronormative, and gendered ways), which also made these abstract characters visible to the world. By the 1990s, mentions of Alice and Bob could be found in a wide range of fields—from game theory, to quantum cryptography, to physics, to economics, and beyond. As other characters were added, they too were given typical definitions, personalities, and life stories.

The ubiquity of Alice and Bob in the university led to winking references in digital and popular culture, including jokes, t-shirts, music, and comics. Noting their importance, in cryptology research if not digital culture, the security company that created Alice and Bob, RSA Security, chose them as their theme for their 2011 annual security conference.

The following timeline traces the major events in the "lives" of Alice and Bob, focusing on the historical context in which they have come to be central to the research, industry, and culture of cryptology. This timeline aims to create an accurate record of the history of Alice and Bob, as well as to identify the cultural and gendered contexts in which they emerged.

Public-Key Cryptography Invented in Secret (1970-73)

In the early 1970s, public key cryptography was invented in secret by the GCHQ. This is the technology that would later lead to the birth of Alice and Bob.

In December 1997, the British intelligence organization GCHQ revealed that the techniques of public-key cryptography were first invented by members of the UK's Communication-Electronics Security Group (CESG) in the 1970s. The individuals responsible for what was then known as "non-secret" encryption were James H. Ellis, Clifford Cocks, and Malcolm Williamson.

In the late 1960s, searching for a solution to key management, knowing that such a technique was critical to the new digital (and increasingly, networked) information environments, James Ellis read a classified document on the Bell C43 Project from 1943-44, a "Type II Ciphony" device, or vocoder. This secure telephone device was developed in after SIGSALY, developed by Bell Labs in 1941-42 and used during World War II. Like SIGSALY, the Type II device was unusual in that its "encryption" (technically, scrambling) was made possible by the direct involvement of the receiving party, and without the need for pre-arranged exchange of information.

It was this idea of involving the receiver in the process of secure information exchange that spurred Ellis to contemplate if such an arrangement might be possible with "ordinary encipherment," instead of audio scrambling. This line of thinking led Ellis to publish an internal report in 1970 on the possibility of "secure non-secret digital encryption." While Ellis had proved with this report that such an arrangement was possible, he still lacked a good implementation.

On his own admission, Ellis' number theory was weak and so he was unable to find a suitable method for the encryption process—a process that would require some technique that would be easy to solve in the one direction, but hard to reverse. This task of finding what would become known as a mathematical one-way function was left to his colleague Clifford Cocks. So, in November 1973, Cocks published an internal report detailing a "possible implementation" of Ellis' non-secret encryption. Cocks'

implementation, it would later turn out, was basically a version of the 1978 RSA algorithm. In January 1974, Malcolm Williamson published an internal report detailing another possible implementation of Ellis' non-secret encryption; this time, Williamson's algorithm was basically a version of the one later identified by Diffie and Hellman, in their famous "New Directions" paper, which was the first unclassified description of public-key cryptography.

Public-Key Cryptography is Re-Invented (November, 1976)

In November 1976, Whitfield "Whit" Diffie and Martin Hellman published a paper entitled "New Directions in Cryptography" in *IEEE Transactions in Information Theory*. The paper demonstrated that it was possible to securely exchange information over non-secure channels, which they called public key cryptography.

Since Ellis, Cocks, and Williamson's work on "non-secret" encryption was kept secret by the GCHQ, prior to Diffie and Hellman's publication it was believed that encrypted communication was only possible by exchanging a cryptographic key in advance. Because of this limitation, cryptography was limited to important communications—diplomatic, military—and outside of the reach of civilians.

Prior to 1976, secure communication required setting cryptographic technologies with identical cryptographic keys (such as with the famous Enigma, Purple, and SIGABA machines). This was an onerous and risky process that needed to be repeated often (it is critical to change cryptographic keys frequently to maintain security). This process was complicated and labour intensive, requiring trusted personnel to transport codes on sheets of paper or electro-mechanical "fill" devices. Even the state-of-the-art Arpanet, which later became the Internet, encrypted communication required the careful coordination of cryptographic keys across distant "Private Line Interfaces." As the number of nodes in the secure network increased, so too did the labour of exchanging keys.

Diffie and Hellman had invented, for the second time (unbeknownst to them), a way to encrypt communication over insecure channels without the prior exchange of keys. This process required generating a special "split" key that contained mathematically-linked parts. The "public" part could be freely exchanged on insecure channels, and when combined with the "private" part in a complicated back and forth exchange (later known as the Diffie-Hellman key exchange), ad hoc encrypted communication over insecure channels was possible. In short, their invention provided the basis for secure transactions on the Internet, and set in motion a fundamentally new way to communicate, to organize, and to socialize.

While Ellis, Cocks, and Williamson were inventing "non-secret" encryption at GCHQ, Diffie had become inspired by John McCarthy's investigation of cryptography for large

computer networks (at the behest of Larry Roberts at IPTO). This spark of inspiration led Diffie to spend the next few years traveling across the US in search of a solution. Diffie moved between archives, universities, and colleagues to discover everything he could about cryptography. He read David Khan's famous survey of cryptography, *The Codebreakers*, met the famous computer scientist Donald Knuth, and finally, in 1974 travelled to Stanford to meet with Martin "Marty" Hellman, a professor of electronic engineering (and former employee of IBM) on the referral of friend and colleague Alan Konheim.

Diffie and Hellman started working together immediately, and drafted an early version of "New Directions in Cryptography." Some of this early work was presented to an information theory workshop in 1975, and was then revised to substantively address similar work on cryptography also being developed by Ralph Merkle. It was submitted to *IEEE Transactions in Information Theory* in June, 1976.

On the eve of the Arpanet that would soon become the Internet, this idea was a revolution in cryptography and soon became the backbone of digital communication. They called their invention "public key" cryptography, and it would soon enable ecommerce, global banking and finance, private personal communication, and—now that it had escaped the confines of the intelligence community—all of the ills associated with the dark corners of today's digital world.

Diffie and Hellman had developed public key cryptography, for the second time, in the complex context of military projects, academic associates, and government funding. This time, however, the idea was in the wild, and would soon be pursued by young computer scientists, Ronald Rivest, Adi Shamir, and Leonard Adleman, who were quick to see the commercial possibilities for public key cryptography on the emerging Internet.

At this point, Alice and Bob did not yet exist. In their paper, as was the tradition in cryptology research, Diffie and Hellman referred to the communicating parties as "A" and "B." A and B were largely featureless—presumptively male, symbolic, and abstract.

Diffie and Hellman later won the 2015 Turing Award (the "Nobel prize" of computer science) for their work in the field. Their pioneering work has stood the test of time, and has been capable of adapting to and resisting challenges.

RSA Algorithm Developed (1977-78)

Diffie and Hellman's proposal for public key cryptography set the course for future research, but their analysis still lacked the all-important one-way function, needed to generate the public and private key parts. Moreover, there was no working implementation of the cryptosystem. In 1977, young MIT computer scientists Ronald Rivest, Adi Shamir, and Leonard Adleman found a suitable one-way function and then developed a working implementation of public key cryptography.

In the year following the publication of “New Directions,” Rivest and Shamir made many attempts to develop a new workable algorithm for key generation—trying countless options with little success. As they were working to develop prospective algorithms, Rivest and Shamir also consulted with Leonard Adleman (also at MIT), to exploit his skill in torture testing algorithms and finding weaknesses in their design.

One night following Passover Seder in April 1977, Rivest drank “a disproportionate amount of the wine” and had a spark of insight for a one-way function, which later became the accepted solution. Late that same night, Rivest called Adleman and talked him through the key points of the algorithm—“something about prime numbers, exponentiation, and on like that,” Adleman recalled. Unlike Diffie and Hellman’s design (using the difficulty of computing discrete logarithms, later formalized by Ralph Merkle in his 1978 article, “Secure Communications Over Insecure Channels”), Rivest, Shamir, and Adleman’s design for the one-way function used the difficulty of factoring large prime numbers.

Rivest stayed up through the night, drafting a first version of the paper that described their algorithm. The first publication of their design was received by the Office of Naval Research in April 1977, entitled “On Digital Signatures and Public-Key Cryptosystems.” Rivest also sent a copy to Martin Gardner at Scientific American, who in August 1977 published the first widely-read account of their cryptosystem. Recognizing the commercial possibilities, in December of that year, they filed a patent for their invention (granted September 20, 1983). In February, 1978, Rivest, Shamir, and Adleman published their findings in an article in *Communications of the ACM*, now referred to widely as the “RSA paper.” It is in the “RSA paper” that Alice and Bob were born.

Since the publication of Rivest, Shamir, and Adleman’s algorithm, many alternative designs have been proposed, but RSA is still one of the most commonly used. Moreover, in the decades since, many attacks have been waged against the RSA cryptosystem, but none have yet to be successful and the design is still considered secure.

The RSA cryptosystem soon became a key part of digital information infrastructure, and helped define the massive changes that the Internet later brought about. In this history, Alice and Bob play a small role. Nonetheless, Alice and Bob were critical for how Rivest, Shamir, and Adleman understood and later communicated their complex algorithm.

Rivest, Shamir, and Adleman won the 2002 Turing Award for their role in designing, implementing, and commercializing public key cryptography.

RSA Algorithm Publicized in Scientific American (August, 1977)

As soon as Ron Rivest, Adi Shamir, and Leonard Adleman discovered what they believed to be a suitable one-way function for their version of public key cryptography, Rivest sent a copy of the draft paper outlining their cryptosystem to Martin Gardner, a mathematics columnist at *Scientific American.* The subsequent publication popularized the RSA algorithm and brought it under scrutiny.

Gardner's column, "Mathematical Games" was published monthly from the 1950s to the 1980s and is widely recognized for its impact on the popularization of "recreational" mathematics. Gardner's column was also read by serious mathematicians, so it was a perfect way to put the prospective one way function and RSA algorithm in front of a broad and serious audience to see if it would stand up to public scrutiny.

Gardner quickly replied to Rivest—within a week—and the two set to work to develop a column that would explain the algorithm and to offer a cryptanalysis challenge to readers. The article offered a cash prize of $100 to anyone who could decrypt a secret message. Stephen Levy described the challenge in his book *Crypto* as follows:
Rivest would generate a public key of 129 digits and use it to encode a secret message. If the system worked as promised, no one in the world would be able to read the message, with two exceptions. One would be someone who had both a powerful computer set to break the message with brute force and a very large amount of time on his hands. […]. The other exception, of course, was the person holding the private key match to that particular 129-digit public key (p. 103-104).

The secret message was not revealed until 1994, when a team led by Derek Atkins, Michael Graff, Arjen Lenstra, and Paul Leyland, in collaboration with hundreds of volunteers online, took the "brute force" approach to decrypting it. The message read: THE MAGIC WORKS ARE SQUEAMISH OSSIFRAGE.

The publication served two important purposes. First, it made the RSA algorithm accessible to a wide audience, which generated a great deal of interest and excitement (they received many requests for the full technical paper, and ended up sending some 4000 copies of it across the globe). With this public interest also came interest by the intelligence community. Rivest, Shamir, and Adleman found themselves in the same situation that Diffie had rebelled against years earlier in his search for public discussions of cryptography—if Rivest, Shamir, and Adleman were not careful, they risked having their invention retrospectively classified or blocked by the US National Security Agency, since at the time cryptographic materials were considered munitions (later, in the 1990s, this issue would be resolved).

Second, the publication allowed for the algorithm to be tested by a broad population, with many different ideas and approaches. So far, the RSA algorithm has proven robust (given sufficiently long key bit lengths).

In Gardner's column there is still no mention of Alice and Bob. Instead, Gardner described the sender and receiver as "A" and "Z" respectively, and as was the custom, referred to each as a featureless "he."

Alice and Bob are Born (February, 1978)

Five years after public key cryptography was invented at GCHQ, two years after public key cryptography was re-invented by Diffie and Hellman, and a year and two articles after a practical cryptosystem was developed by Ron Rivest, Adi Shamir, and Leonard Adleman, **Alice and Bob are finally born.**

In February 1978, Rivest, Shamir, and Adleman published their paper "A Method for Obtaining Digital Signatures and Public-key Cryptosystems" in *Communications of the ACM,* (the paper is now typically called the "RSA paper" given its stature in the field). In this paper (largely identical to their MIT technical report published a year earlier), Rivest, Shamir, and Adleman need to describe the complex secure communication scenarios possible with their version of public key cryptography. To do so, they write: "For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem" — making reference, for the first ever time in cryptology, to Alice and Bob.

Inventing Alice and Bob was an unusual approach to scientific and technical communication. Previously, it had been standard practice to identify the sender of information as "A" and the recipient as "B." Diffie and Hellman, for instance, wrote "If user A wishes to send a message M to user B…" in their "New Directions" paper. In the "RSA paper," "A" and "B" were renamed Alice and Bob. Rivest later remarked that he invented the names in order to maintain the traditional use of "A" and "B," but to make the users easier to trace in the paper by using the pronouns "he" and "she."

This is the first ever mention of Alice and Bob in any connection to cryptography, and the start of a long and storied history.

(Some people have suggested that the 1969 movie Bob & Carol & Ted & Alice was the origin of Alice and Bob. While it is possible—even likely—that Rivest, Shamir, and Adleman might have been familiar with the movie, there is no evidence to indicate that the movie influenced their naming decision. More likely, since Alice and Bob are common English names that start with A and B, the names were chosen without much forethought.)

RSA Data Security Founded (1982)

Ron Rivest, Adi Shamir, and Leonard Adleman realized that their public key cryptography algorithm was commercially valuable, and in December 1978 they filed for

a patent (through MIT) and began assembling a commercial enterprise, RSA Data Security.

Despite being more comfortable in the halls of academia, and with little business experience to guide them, Rivest, Shamir, and Adleman received outside investment ($150,000) to purchase the rights to their algorithm from MIT (MIT still held the patent) (Yost, 2007 p.614). The first investor was Jack Kelly, but soon he was joined by others, making modest investments despite not having any real product to sell. The first years of RSA Data Security were financially troublesome, and in 1986 RSA Data Security brought on Jim Bidzos to help run the company. Bidzos landed several large contracts (notably, Lotus Development bought a license in 1987), initiated the RSA Security conference, and soon the company was on more secure financial footing. Rivest, Shamir, and Adleman thereafter played a smaller role in the business of RSA Data Security.

By the 1990s, the Internet boom was beginning and RSA Data Security was positioned to be a key player, since their security software was essential for emerging opportunities like ecommerce. RSA Data Security continued to win lucrative contracts and was tapped by an emerging Internet technical committee to share the responsibility with Digital Equipment Corp. to certify encryption keys (later, in 1995, spun-off to become Verisign). Given their potential position as the security provider for the Internet, RSA Data Security drew the ire of the US National Security Agency, which had begun to protest the expansion of their strong cryptography products. RSA Data Security soon became a key player in the fight to control cryptography, which they won in 1996 when cryptography technology was removed from the munitions list and permitted to be sold globally. Through the rest of the 1990s, RSA Data Security was courted by companies wishing to purchase it. In the ramp-up to the dot.com boom, RSA Data Security was sold to Security Dynamics in April 1996. Over the next decade, the company would be sold several more times (as RSA Security Inc.), notably, to EMC Corporation for $2.1b in 2006, which then moved it under the banner of Dell EMC Infrastructure Solutions Group when EMC was acquired by Dell Technologies (now RSA Security LLC).

Alice and Bob Become Tropes of Cryptology Research (1980-)

After their birth in 1978, Alice and Bob soon became tropes of cryptology research. Over the next decade of academic research in cryptology, Alice and Bob would become ubiquitous and a key epistemic tool.

Shamir, Rivest, and Adleman again soon mention Alice and Bob, in their chapter “Mental Poker,” for the edited volume Mathematical Gardner. This volume was published in 1981 to celebrate Martin Gardner’s 65th birthday, on October 21, 1979 (Gardner, himself, was extremely important to the success of the RSA algorithm). In this work, just a year or two after their birth, we already see evidence of the epistemological

centrality and stereotypical depictions of Alice and Bob. The couple is thus re-introduced: “Perhaps it will make the ground rules clearer if we imagine two players, Bob and Alice… .”

In the same year, two more academic publications make mention of Alice and Bob. On May 20, 1981 Michael O. Rabin wrote a technical report for the Aiken Computation Lab at Harvard University, entitled “How to Exchange Secrets with Oblivious Transfer.” In this report, Alice and Bob are again the central epistemological frame, opening the very first sentence: “Bob and Alice each have a secret…” Next, Manuel Blum’s report from November 10, 1981 is published, entitled “Coin Flipping by Telephone: A Protocol for Solving Impossible Problems.” Here again, Alice and Bob are the key epistemological frame, opening the report: “Alice and Bob want to flip a coin by telephone.”

Up to this point, however, all references to Alice and Bob referred to them as featureless symbols—little more than named abstractions. Blum’s report is the first in what would become a tradition: literature that invents their situational context and backstory. Blum writes: “They have just divorced, live in different cities, want to decide who gets the car.” From this point on, Alice and Bob have a history and, soon, will start to acquire personalities, and eventually friends.

In the cryptology literature that follows, most but not all publications make reference to Alice and Bob, often in their first line. Alice and Bob are mentioned in DeMillo and Merritt (1983), Blum (1983), Rabin (1983), and Gordon (1984). Some authors, however, continue to use the traditional A and B nomenclature (inherited from Diffie and Hellman’s New Directions paper). For instance, the famous article from CRYPTO 84 by Taher ElGamal, entitled “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms” makes no mention of Alice and Bob. In 1986 (published 1988), Silvio Micali, Charles Rackoff, and Bob Sloan hedge their use of Alice and Bob, writing: “the goal is that A(lice)… becomes able to securely send a message m to B(ob).” Increasingly, however, not making reference to Alice and Bob would be unusual, and by the end of the decade their presence would be nearly total.

Alice and Bob After Dinner Speech (April, 1984)

In 1984, a year after Ron Rivest, Adi Shamir, and Leonard Adleman received the patent for the RSA algorithm—and still early days for Alice and Bob—the cryptologist John Gordon gave an “after-dinner speech” about Alice and Bob at an April conference in Zurich.

The precise context of this meeting is unknown (it was likely the Zurich Seminar on Digital Communications: “Applications of Source Coding, Channel Coding and Secrecy Coding”); Gordon’s speech was at the invitation of Professor James Massey (see IEEE Spectrum, November 1983).

The speech is legendary in the field of cryptography, and for good reason. Gordon took a lighthearted approach to chronicling the many lives of Alice and Bob—from their hypothetical experiences playing poker by mail or telephone (as described in Shamir, Rivest, and Adleman's "Mental Poker" (1981) and Richard DeMillo and Michael Merritt's "Protocols for Data Security" (1983)), to similarly hypothetical experiences playing the stock market.

Gordon's speech collected the nerdy lore of Alice and Bob: Bob was a stockbroker while Alice was a stock speculator, Alice and Bob tried to defraud insurance companies, Alice and Bob played poker over the phone, Alice tried to hide her financial dealings with Bob from her husband, Alice and Bob are wanted by both the Tax Authority and the Secret Police, and Alice doesn't trust Bob because of some unknown past experience. Gordon remarks, "Bob is a subversive stockbroker and Alice is a two-timing speculator."

Ultimately, Gordon uses Alice and Bob for their typical purpose: as means to an explanatory end. Gordon's speech explains coding theory in relation to secret communication. He remarks, "a coding theorist is someone who doesn't think Alice is crazy."

In a retrospective article in Network World (2005), Gordon describes the long-term impact of his speech, "Today, nobody remembers I invented Strong Primes, but everyone knows me as the guy who wrote the story of Alice and Bob." Indeed, Gordon's speech marks an important fact about the history of Alice and Bob—Alice and Bob are key elements of the conceptual and discursive frameworks of contemporary cryptography.

Alice and Bob Move (1980-)

While Alice and Bob were born in the academic field of cryptology, they were soon being used in many other disciplines, domains, and contexts.

In Shamir, Rivest and Adleman's 1981 chapter for *Mathematical Gardner*, Alice and Bob were the players of "mental poker" over a telephone line, as also in Blum's 1981 article. In these articles, Alice and Bob already straddle the line between public key cryptography, rational choice theory, and logic. In 1983 (revised and re-published in 1987), Joseph Y. Halpern and Michael O. Rabin use Alice and Bob in a paper on modal logic (however, Alice and Bob were already familiar to the authors—especially Rabin, who makes reference to his "oblivious transfer" report from 1981). As quantum computing and quantum cryptography begins to get discussed in the literature, Alice and Bob are again referenced (for example, in Bennett et al. 1990).

From these origins and their cross-pollinations through rational choice theory, logic, and quantum computing, Alice and Bob have slowly become common characters in economics, physics, and other engineering domains. In fact, it is not unusual to find

reference to Alice and Bob in domains well outside of science and technology, often with no recognition of their origins.

Similarly, Alice and Bob have become critical for university teaching of cryptology and cybersecurity. Today, it is common to see reference to Alice and Bob in slide decks explaining the basic concepts of cryptographic key exchange for undergraduate audiences. Because of the multi-media format, in these pedagogical contexts Alice and Bob are often visually depicted, especially as stereotypical clip-art images of men and women (on the other hand, they are often depicted abstractly, as blocks, lines, animals, computer chips, and so on).

Eve is Born (1985-88)

As was customary for cryptology literature by this point, Charles Bennett, Giles Brassard, and Jean-Marc Roberts opened their 1985 abstract "How to Reduce Your Enemy's Information" with a story about Alice and Bob. This time, however, a new character was introduced: Eve.

The problem facing Alice and Bob in Bennett, Brassard, and Roberts' narrative is that a seemingly secure channel for communication is rendered "imperfect in various ways: transmission errors can occur, and partial information can leak to Eve, the eavesdropper, who also can modify the transmissions arbitrarily." This is the first known appearance of Eve—a disruptive force in the history of Alice and Bob—and is the basis of their more widely cited paper "Privacy Amplification by Public Discussion," published in the *SIAM Journal on Computing* in April 1988.

Between Bennett, Brassard, and Roberts' 1985 abstract and the publication their longer 1988 article, Eve had become a well-known and accepted third party in cryptographic communications. She was a central figure in Steven Rudich's dissertation on one-way functions (1988), in Rudich and Impagliazzo's conference paper on a similar topic (i.e. Limits on the Provable Consequences of One-Way Permutations) (1989), Fischer, Paterson, and Rackoff's article on secret bit transmission (1990), and in Bennett et. al.'s later work on experimental quantum cryptography (1990). Eve's growing status as a central character in the history of Alice and Bob was cemented with her inclusion in the *dramatis personae* of cryptography published in Bruce Schneier's *Applied Cryptography.*

Early depictions of Eve are rather indifferent about Eve's moral status. She is an eavesdropper, to be sure, and she may or may not engage in tampering with the relevant information exchange. She is not malevolent (usually wishing no ill will to Alice and Bob), rather, she is simply an eavesdropper who potentially alters the communications in which Alice and Bob are engaged by infiltrating a private channel. But over time, popular depictions of Alice, Bob, and Eve paint the three in a sordid heteronormative affair of one kind or another–Eve as a jilted wife listening into her

husband's conversations with Alice, or alternatively with Eve as the "cheating adversary".

The Culture of Alice and Bob (1990-)

As Alice and Bob became common features of the academic landscape, and as the 1990s and 2000s saw a rise of nerd and geek culture, Alice and Bob were soon found across digital culture broadly. Their depiction in popular media is usually a winking subcultural reference, signaling awareness of geek lore.

References to Alice and Bob in geek culture have added to their imagined lives. Jokes and comics are a common way of further depicting their lives.

Similarly, in the in the tradition of John Gordon's "After Dinner Speech," narratives and stories about Alice and Bob have expanded and updated Alice and Bob (even including a Prius-driving, kombucha-drinking Eve).

There are now t-shirts, mugs, and even a rap song about Alice and Bob.

Applied Cryptography is Published (1994)

In 1994, Bruce Schneier published the first edition of the now-classic *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. In this book, Schneier expanded the cast of characters beyond Alice, Bob, and Eve. In doing so, Schneier created the canon of characters accepted today.

Schneier has a long record as a cryptographer, computer scientist, and writer and was well-positioned to write a comprehensive and practical account of the field of cryptography. The book was highly influential, credited for popularizing cryptography by making its key problems and history accessible to a broader public. Further, it aimed to be an "indispensable source" to working cryptographers (Highland, 1996). According to Whitfield Diffie, Schneier achieved this goal, as Diffie expressed in his foreword: "[s]itting on the shelf, this volume may do no better than the books and papers that preceded it, but sitting next to a workstation, where a programmer is writing cryptographic code, it just may."

The publication of *Applied Cryptography* was an important landmark in the history of Alice and Bob, largely because it identified the rest of their social circle. As was by-then customary, Schneier used Alice and Bob as stand-ins for senders and receivers in the examples provided throughout the book. However, given the scale and scope of the book, his examples required many other participants. And so, Schneier created a list of his cast of characters and their intended uses—his dramatis personae—who would each engage in communications with Alice and Bob throughout his examples.

Schneier's list refers to Alice as the "first participant in all the protocols," with Bob as the second, with eight more characters and their roles laid out (second edition, 1996).

The "Adventures of Alice and Bob" (2011)

In 2011, RSA Security LLC made Alice and Bob the theme for their annual security industry conference.

In 1991, under the helm of Jim Bidzos, RSA Data Security started holding annual security industry conferences. The first conference was as a small, one-panel event and has since become the premier industry conference. Today, there are several events a year, addressing a range of issues in security and information technology, with an annual attendance of approximately 45,000. The theme of the 20th anniversary conference (in 2011) was Alice and Bob, and the event included a series of short videos entitled *The Adventures of Alice and Bob* explaining the history and key ideas in cryptography through a dramatic narrative featuring the characters.

The narrator of *The Adventures of Alice and Bob* describes the origin story of Alice and Bob, "when Alice saw Bob, she fell head over heels…and squashed the algorithm." In the story that unfolds, Eve ("a rogue intercept") lies to the police about Alice's identity, which results in Alice's detention, where cunningly "she languished for years" far away from Bob. Once Alice frees herself with a public key (a nod to the public and private keypair used in public key cryptography), and after Mallory ("a malevolent force") steals Bob's unencrypted identity, Alice and Bob are finally reunited.

That same year, RSA Security produced another series of short videos for the conference entitled "The Giants Among Us," which saw key figures including Whit Diffie, Martin Hellman, Adir Shamir, Leonard Adleman, Ron Rivest, and others speaking about their various contributions to cryptography and the RSA algorithm. As part of this series, Bruce Schneier (security expert and author of *Applied Cryptography*) appeared in a video called *Who are Alice and Bob?*. Schneier describes the roles of Alice, Bob, and Eve, and highlights their ubiquity in writing on cryptography: *"Alice and Bob have a storied history. They send each other secrets, they get locked in jail, they get married, they get divorced, they're trying to date each other. I mean, anything two people might want to do securely, Alice and Bob have done it, somewhere in the cryptographic literature."*

Cultural Interpretations of Alice and Bob (2012)

In 2012, the computer scientist Srini Parthasarathy wrote a document entitled "Alice and Bob can go on a holiday!". Rearticulting the deeper culture in which Alice and Bob lived, Parthasarathy proposed that Alice and Bob might be usefully replaced by Sita and Rama, characters central to Hindu mythology.

Parathasarathy argued that by changing Alice and Bob to Sita and Rama, the context of their meetings (often in hostile environments) would be better explained, and that the first letters of their names ("S" and "R") correspond directly to the sender and receiver in the communications channel.

The proposal itself is an interesting one (now available on Academia.edu), in part because it moves the teaching practices and discourses of cryptography outside of the context in which they were conceived. The proposal to use Sita and Rama rather than Alice and Bob draws attention to the ways that the language of cryptography continues to reflect the seemingly arbitrary and innocuous (but thoroughly Anglo-American and Western) naming practices used by Ron Rivest, Adi Shamir, and Leonard Adleman. Further, Parathasarathy's short paper reflected deeper concerns about the globalization of technology. Parathasarathy merely suggested that Alice and Bob might be more effectively named, but his proposal soon became the source of a joke characterizing the role of the Indian technology industry. For example, The Register ran an article suggesting "even their jobs are being outsourced." Once again, despite their innocuous origins, Alice and Bob reflect deeper norms and values in the history of cryptography.

On Gender

In the history of cryptology, women tend to be either systematically excluded or reduced to objects. The absence of women is both a reflection of the bias of society and historians, and a gap in the employment of women in computing fields. In the early history of computing, in fact, women were key to the development of computing, and especially cryptology (see Woodfield, 2001; Misa (ed.), 2010; Hicks, 2017). But, once computing gained status and importance, women were increasingly pushed out of the computer and cybersecurity industry. Worrisomely, in the field of cybersecurity, this trend to marginalize and exclude women has *increased* in recent years. Those women that have managed to elbow in on the male-dominated industry are important to highlight and celebrate. Uncovering the gendered context of Alice and Bob is one chapter in the larger, untold story of women in cryptology.

Women have a long history of being depicted as technical objects in computing (see also Brahnam, Karanikas, and Weaver, 2011). Consider, for example, Ivan Sutherland, the so-called "father of computer graphics." In his 1963 MIT PhD dissertation, he depicted a "winking girl" using the revolutionary Sketchpad software he developed. Lawrence Roberts, an essential figure in the creation of the ARPANET, used an image of an unnamed woman from Playboy magazine for his academic article on image processing. A decade later, Alexander Sawchuk and his team at the University of Southern California used *another* image from Playboy magazine to demonstrate image processing. This latter image, of Lena Sjööblom posed among toys and engaging in a game of dress-up, has since become the standard test image for image compression and processing software. And finally, the first "Photoshopped"

image was of a topless woman on a beach: Jennifer, the software developer John Knoll's then-girlfriend.

In the case of Alice and Bob, the presumption that Alice is a woman and Bob is a man aids in their use, since (in English), gendered pronouns enable easy reference ("he said, she said"). At the same time, gendered assumptions about the characters of Alice and Bob have been read into their fictional lives. Images of Alice, Bob, and Eve depict the three as in love triangles, with Alice and Eve alternately portrayed as disrupting one another's blissful domestic life with Bob. Visual depictions of Alice, Bob, Eve, and others used in university classrooms and elsewhere have replicated and reified the gendered assumptions read onto Alice and Bob and their cryptographic family, making it clear that Bob is the subject of communications with others, who serve as objects, and are often secondary players to his experience of information exchange. Thus, while Rivest, Shamir, and Adleman used the names "Alice" and "Bob" for a sender and receiver as a writing tool, others have adapted Alice and Bob, in predictable, culturally-specific ways that have important consequences for subsequent, gendered experiences of cryptology.

Contact

Research by Quinn DuPont and Alana Cattapan. DuPont developed the website, and received institutional and financial support through a Rutgers Digital Studies Fellowship and UVic Electonic Textual Cultures Lab Open Knowledge Practicum. Corrections, suggestions, and responses warmly welcomed:

Quinn DuPont @quinndupont
Alana Cattapan @arcattapan