

Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence

Steven M. Bellovin

<https://www.cs.columbia.edu/~smb>

CUCS-014-14

Abstract

The conventional narrative for the invention of the AT&T one-time pad was related by David Kahn. Based on the evidence available in the AT&T patent files and from interviews and correspondence, he concluded that Gilbert Vernam came up with the need for randomness, while Joseph Mauborgne realized the need for a non-repeating key. Examination of other documents suggests a different narrative. It is most likely that Vernam came up with the need for non-repetition; Mauborgne, though, apparently contributed materially to the invention of the two-tape variant. Furthermore, there is reason to suspect that he suggested the need for randomness to Vernam. However, neither Mauborgne, Herbert Yardley, nor anyone at AT&T really understood the security advantages of the true one-time tape. Col. Parker Hitt may have; William Friedman definitely did. Finally, we show that Friedman's attacks on the two-tape variant likely led to his invention of the index of coincidence, arguably the single most important publication in the history of cryptanalysis.

1 Introduction

The one-time pad as we know it today is generally credited to Gilbert Vernam and Joseph O. Mauborgne [22]. (I omit any discussion of whether or not the earlier work by Miller had some influence [2]; it is not relevant to this analysis.) There were several essential components to the invention:

- Online encryption, under control of a paper tape containing the key.
- The requirement that the key be random.
- The requirement that the key be non-repeating, across not just a single message but across all messages.

It has always been clear that Vernam invented the first element, though some of his colleagues made notable contributions; in particular, Lyman Morehouse devised the variant that used two looped tapes with relatively prime lengths. This is well-attested by contemporary memos, Vernam's patent (US 1,310,719), etc.

The origin of the other two elements, though, has always been rather murkier. Drawing on letters, interviews, and documents, David Kahn concluded that Vernam came up with the randomness requirement, albeit without full understanding of the cryptologic requirement (he noted—incorrectly, as it transpires—that the word “random” did not occur in the patent and in fact was not mentioned until Vernam's much-later paper [35]), and that Mauborgne—possibly drawing on earlier work with Parker Hitt—realized that absolute security could only be obtained if no portion of the key was ever repeated. Ralzemond Parker, Vernam's manager, strongly disagreed; he has long claimed that Vernam alone invented the one-time pad; see, e.g., [25], [1, Parker to Kahn, 21 Nov 1962], [1, Parker to Kahn, 3 Apr 1963], and [1, Parker to *Scientific American*, 26 Jul 1966].

To try to resolve a problem he himself called “the most difficult [he] faced in [his] research” [1, Kahn to *Scientific American*, 6 Aug 1966], Kahn suggested to me that we reexamine the relevant files in the AT&T archives. Unfortunately, despite diligent efforts by AT&T archivist George Kupczak, we could not locate them all; the folder numbers have been changed in the 50 or so years since Kahn's original efforts, and many keyword searches across three visits

were futile. We did find one crucial folder; I also relied on papers in the William Friedman Collection at the George C. Marshall Foundation Library and in the Dr. David Kahn Collection at the National Cryptologic Museum. Those papers include Kahn's own notes on the missing AT&T folder; I re-analyzed them.

My conclusions are different than Kahn's. I believe that Vernam (possibly alone, possibly with the help of his AT&T colleagues) was primarily responsible for the idea of a non-repeating tape. Furthermore, he and/or his colleagues at AT&T did indeed know that the key needed to be random, though it is unclear when and how they concluded this. Mauborgne was likely the person who codified the non-repetition requirement, but his conclusion was rather later in coming, and was based on not just his own work, but also that of Parker Hitt and William F. Friedman. He may also have had the original insight behind Morehouse's two-tape variant. Friedman (and possibly Hitt) were the first to realize the true security of the non-repeating, random tape. Finally, I believe that attacking the Morehouse scheme is what led Friedman to invent the index of coincidence.

1.1 The Morehouse Scheme

Per [22] and numerous other sources in the various archives, the original AT&T proposal was for a true one-time tape system: a character from a key tape was XORed with a plaintext character to encrypt, or with a ciphertext character to decrypt. Mauborgne doubted its feasibility for production use. For example (and using the paper tape specifications given in [33]), a key tape that held 1,000,000 characters would require a reel over two meters in diameter. Even 100,000 characters—the bare minimum for a day's traffic—would require a reel about .6 meters across. On top of that, the problems of secure key tape manufacturing, distribution, destruction, and accounting were daunting.

The solution was Morehouse's two-tape system. Two tape loops, of relatively prime lengths, were used; a character from each tape was XORed to produce a key character. The effective length of the key stream is the product of the length of the two tapes. Using the notional lengths of 999 and 1,000 characters, the loops would be about 2.5 meters in circumference; this is easy to handle. The tapes could even droop onto the floor.

2 The Problem

2.1 Kahn's Reasoning

Kahn's reasoning, based on an analysis of the sometimes-conflicting information from different sources, is presented in a long endnote to the section of his book discussing Vernam's invention. A somewhat longer version is in [1, Kahn to *Scientific American*, 6 Aug 1966]. Unless otherwise noted, information in this section is taken from the footnote.

The attribution of the invention of randomness to Vernam is, according to Kahn, due to the lack of any other claims. Kahn does assert that AT&T never mentioned randomness until Vernam's 1926 paper [35] and notes that Mauborgne was the one who was aware of the dangers of coherent running keys [1, Kahn to *Scientific American*, 6 Aug 1966]; however, since Mauborgne never claimed credit for randomness of the key, he is content to let the AT&T claim stand.

The difficult question has always been about non-repetition. The strongest evidence Kahn has for his conclusion is a categorical statement by Mauborgne [1, Mauborgne to Kahn, 5 Mar 1963]:

The answer to the question contained in the third paragraph of your letter "who invented this"? (referring to the non-repetitive cipher key tape) you have already deduced—yes, I did it.

When Kahn questioned him further, after Parker's continued disagreement, Mauborgne seemed rather miffed that Kahn did not consider the question settled [1, Mauborgne to Kahn, 25 Oct 1964]: "So far as I am concerned the case is closed. Many thanks."

Kahn also relied on a letter from Donald Perry [1, Perry to Kahn, 1 Jul 1963], which states that the Army didn't like AT&T's two-tape system, so AT&T came up with the one-time system. This sequence—the two-tape version coming first—is at variance with all other claims; furthermore, it is contradicted by the patent history and various memos in the AT&T archives. Accordingly, I do not attach much weight to it.

Finally, Kahn cites Hitt's statement that keys for the Larrabee must be as long as the plaintext. Hitt was a friend and colleague of Mauborgne's; Kahn speculates that Mauborgne helped Hitt develop the notion, and hence was long aware of the notion of very long keys.

2.2 Organizational Structures

It is impossible to follow this without understanding the organizations each party represented and perhaps spoke for. Most obviously, when a request was sent to George Fabyan or a result was announced by him, it was really Friedman who was doing the work. Fabyan was egotistical and apparently wanted his name on any publications [3]. However, he was not a cryptanalyst; he was a businessman. It is likely that the more bombastic (and, on occasion, apparently ignorant) comments were by Fabyan, while the technical meat was supplied by Friedman. Friedman himself had disclaimed some of Fabyan's more outlandish claims [17, Friedman to Parker, 16 May 1944], such as the assertion that any enciphered message could be broken [4, Fabyan to Gherardi, 31 Mar 1919].

Mauborgne was in the Office of the Chief Signal Officer in the Signal Corps. As such, and despite his abilities as a cryptanalyst, his responsibility was what today would be called "information assurance": he was responsible for keeping U.S. communications secure. He was *not* charged with reading other countries' traffic, and thus was not "officially" a cryptanalyst. He was, however, the only senior cryptologist in the Signal Corps; when the Chief Signal Officer, Gen. George Squier, opined on the security of a scheme, it was almost certainly Mauborgne's technical opinion that was being cited.

Herbert Yardley, on the other hand, headed the Military Intelligence Division's (MID) Cipher Bureau, i.e., what we would call the COMINT function. His superior, Gen. Marlborough Churchill, had great confidence in Yardley's abilities; cryptologic statements from Churchill should be understood as Yardley's statements. Friedman certainly thought that Yardley was responsible for MID's opinion of the two-tape solution [17, Friedman to Parker, 16 May 1944].

Hitt had no official role in the goings-on; he was, however, a skilled cryptanalyst and had served as Chief Signal Officer for the U.S. 1st Army during World War I. He was a friend of Mauborgne's, and knew Friedman and Yardley; most likely, his opinion was sought by all concerned.

At AT&T, Bancroft Gherardi and John Carty, as high-level managers, had the primary communications responsibility; the technical work was done by Vernam, Razemond, D. Parker (his manager), and Morehouse, among others.

AT&T knew that Vernam's online encryptor was an interesting invention, and notified the military [22]. Mauborgne worked with them, and suggested that they contact Fabyan, who had a lab that did research in many fields including cryptology. Friedman led a team that did the technical analysis and tried to crack the system. Mauborgne probably could not adopt a cryptographic device without buy-in from the Cipher Bureau, the official cryptanalysts. Most likely, he was the one to bring Col. Hitt in, though this was apparently done with Fabyan's knowledge and consent. Fabyan, in turn, seemed to value Hitt's role as a neutral party; he was not formally charged with either attacking the AT&T machine or defending it.

3 The Opposing Viewpoints

Vernam, who died in 1960, did not leave any known documents with his side of the story. Instead, we must rely on Parker as Vernam's advocate, as opposed to Mauborgne. Friedman, who was the independent evaluator of the scheme, worked for Mauborgne shortly thereafter, and became good friends with Parker in later years, is the nearest we have to a neutral observer who nevertheless was intimately familiar with the technology and the organizations concerned.

3.1 The Case for Mauborgne

Kahn's strongest evidence is Mauborgne's letter to him. It is unambiguous and apparently definitive; to question it is apparently to doubt the word of a decorated, highly respected senior officer. However, a close reading of his letter and comparison with other documents suggest that his memory, more than 40 years after the event, was somewhat faulty. He made major contributions, but probably not to the meat of Vernam's invention.

Mauborgne's letter explicitly cites as evidence the "Report of the Chief Signal Officer to the Secretary of War for the year 1919":

The operativeness and speed and reliability was thoroughly tested during the War over lines carrying messages of the most confidential character from Hoboken to Washington and from Washington to Newport

News. The cipher produced by this apparatus *when used in accordance with the method of the Signal Corps* has thus far successfully resisted all the efforts of cipher experts to break it.

(Emphasis by Mauborgne in his letter to Kahn.)

There are two problems here. First, the three-station network mentioned in that paragraph used the two-tape system [22] [17, Friedman to Parker, 12 Oct 1943] [4, Squier to Fabyan, 19 Sept 1919], not the non-repeating tapes. Second, and perhaps more important, the text that Mauborgne himself emphasized speaks of “the method of the Signal Corps”. That method, however, appears to refer to encrypted indicators (see Section 5.1) for the two-tape system. One letter, from Mauborgne to John Carty of AT&T, is somewhat ambiguous [4, Mauborgne to Carty, 20 Dec 1919]:

Herewith are forwarded copies of recent correspondence on the subject of the decipherment of the batch of cipher tapes sent to Colonel Fabyan in which the cipher indicators were not coded, as done in accordance with the policy of the War Department regarding official cipher messages.

A later letter from Mauborgne to Carty [4, Mauborgne to Carty, 22 Jan 1920] clarifies the situation. Quoting from a memo Mauborgne had sent to Churchill, he noted that Fabyan’s group had exploited unencrypted indicators, a weakness that Mauborgne and Yardley had not previously perceived. Marlborough then asked the Chief Signal Officer to insist on encrypted indicators. The letter to Carty goes on to note that either the true one-time tape or dual tapes with encrypted indicators were acceptable to the Chief Signal Officer. The two clearest statements are in the August 16, 1919 entry in [17, Extracts from Correspondence Relating to Solution of A.T. and T. Printing Telegraph Cipher, 12 Oct 1943], which refers to the two-tape system with appropriate indicators and procedures as “the cipher as used by the Signal Corps”, and in [10, Addendum 1], which gives the actual rules.

Mauborgne’s letter to Kahn also cites

... my collaboration with the inventor Vernam and Mr. Neeve (spelling may be wrong) Chief Patent Counsel for the AT&T Co. while the patent claims for the Vernam patent were being drawn up, in my presence, in the New York offices of the Company.

The issue of the patent claims is dealt with in more detail in Section 4.1; for now, I note that Kahn’s records state that Mauborgne participated in drafting the claims of the Morehouse (two tape) patent [1, Kahn’s notes on AT&T files, 15 Jun 1964]. While this is not evidence per se of his non-participation in drafting the Vernam claims, it is very unusual for an outsider to be involved in drafting any patent claims. For it to have happened twice, with no other evidence for the other time, strains credibility. (Mauborgne also stated that he worked on the Vernam claims in a 1960 oral history interview with Dr. Thompson of the Signal Corp Historical Division [17, Interview with Mauborgne, 2 Dec 1959]; there is no further explanation given in Thompson’s memo.)

The last significant point in Mauborgne’s letter is his correct assertion that there is danger if a key stream is repeated. The text in his letter, though, warns of danger from repeated use of the 999,000 character key stream, i.e., the key stream from a two-tape system with tapes of 999 and 1,000 characters:

Using a five letter key word as a simple example I demonstrated how a cryptanalyst would proceed to break either a single message of sufficient length or from different messages in the same key from a lot of stations. I said that the same decipherment scheme would apply if a number of Army stations used the 999,000 key tape simultaneously and the circuits could be tapped by the enemy. I urged those present to include in the Vernam patent claims one covering the use of a non-repeating cipher tape and the method of rapidly producing such tapes.

No such claims appear in the Vernam patent. However, there is a series of related claims in the Morehouse patent (U.S. Patent 1,356,546), starting with claim 5:

The method of producing a cipher key, free from cyclic repetition of the same character or sequence of characters, which consists in forming a plurality of series of ciphering characters with the number of characters different in different series, selecting characters from each series to form a continuous sequence by retraversing the sequence as it is exhausted, and combining the successively selected characters from different series.

This is consistent with the text in Kahn’s notes on Mauborgne’s participation in drafting the claims on Morehouse’s patent. I believe that this claim—a way to produce a long key stream from a “plurality” (i.e., more than one) repeating sequence—is what Mauborgne’s letter is actually referring to when he speaks of “the method of rapidly producing such tapes”.

Mauborgne says that he worked with an AT&T patent attorney named “Neeve”. This adds little. Both the Vernam and Morehouse patents were filed by a different attorney, G.E. Folk, but multiple attorneys might work on preparing an application. In fact, we know from [1, Kahn’s notes on AT&T files, 15 Jun 1964] that one William R. Ballard, apparently a patent attorney, also worked with Mauborgne.

One item perhaps supporting Mauborgne’s claim is not in the letter. Kahn’s notes of his visit to the AT&T archives [1, Kahn’s notes on AT&T files, 15 Jun 1964] mention a memo with a diagram of encryption with two repeating keywords, RIFLE and THOMAS.¹ Although the notes do not say so, this diagram was apparently in Mauborgne’s handwriting [20]. Kahn’s book says that this was Mauborgne explaining the dangers of repetition to the Vernam et al.; however, it seems equally plausible that this was Mauborgne explaining how a two-tape solution might work. The only caveat here is that the same memo uses GRANT as a key, which Kahn notes was also used in Hitt’s manual [12, pp. 51]; however, Hitt used it to demonstrate encryption with Vigenère’s cipher, and not to show cryptanalysis. (There is a later example of a recovery of GRANT as a key, but for Playfair.) There is no further context in Kahn’s notes; while I cannot conclude from them that it was Mauborgne explaining the two-tape system, I also think it unclear that it was Mauborgne showing the dangers of that scheme.

There is one more piece of evidence that Kahn cites as supporting his analysis: he speculates that Mauborgne helped Hitt come up with the notion that the key in the Larrabee cipher needed to be as long as the plaintext. However, Hitt himself categorically denied this [1, Hitt to Kahn, 9 Apr 1966]:

I can assure you that Mauborgne had nothing to do with the reference to the Larrabee cipher albeit in a letter that Kahn received very late in the manuscript preparation process.

I conclude that Mauborgne’s memory was faulty. The available evidence is much more consistent with him coming up with the two-tape solution instead; furthermore, his very late attachment to it, and his view of it as equally secure as the true one-time system (see Section 4.3), suggests that he had no clear understanding of the security advantage of the true one-time tape, even as late as early 1920.

3.2 Parker and Friedman

Ralzemond Parker apparently appointed himself the guardian of Vernam’s—and by extension, AT&T’s—reputation with respect to the one-time tape. He must have understood the importance of the invention, because he played this role long before there was any public discussion of credit. There was an exchange of letters with Friedman during World War II, an internal AT&T memo to preserve the tapes and plaintext of the challenge messages sent to Fabyan [4, Parker, Memorandum, 4 Dec 1946], a 1956 internal NSA article, a 1960 letter to AT&T informing them of Vernam’s death [15, Parker to Kappel, 30 Aug 1960], and of course his sometimes heated discussions with Kahn. His primary point—that Vernam invented non-repetition—does appear to be correct; that said, there are apparent errors in other of Parker’s claims.

The exchange with Friedman started with a chance meeting in 1942 [25]. Following it, Parker sent Friedman a note in which he wrote [15, Parker to Friedman, 30 Jan 1942]:²

The printing telegraph cipher system, as originally proposed, contemplated the use of a scrambled non-repeating key tape. The double key system was suggested to overcome the practical difficulty of replacing key tapes which are used only once and then destroyed. In the early days we argued that a single non-repeating key of random characters could, with our machine, give absolute secrecy as well as rapid encipherment and decipherment. We were disappointed at the emphasis given to the problem of preparing and distributing such key tapes.

¹ Betsy Rohaly Smoot suggests that these two keywords might be a reference to Parker Hitt [32]. Hitt was an expert on riflery and had just coauthored a book on it with Thomas Brown [13].

² There is some ambiguity about the year of the letter. There is a note on it, apparently by Parker, concluding that it was 1942; Friedman’s October 1943 response [17, Friedman to Parker, 12 Oct 1943], which refers to Parker’s letter as being from “a number of months ago”, makes one suspect that 1943 is more likely. However, since it is Parker’s letter and he concluded that it was 1942, I have used that date.

Friedman disputed part of this [17, Friedman to Parker, 12 Oct 1943]:

There also can be no question but that everybody except ourselves at Riverbank believed the double tape system absolutely secure. Certainly the A.T. & T. people, including Mr. Gherardi, were positive about the matter; and as far as concerned Washington, note what the 2d item in the “extracts” says. Incidentally, that is not an extract from that letter but the whole letter and you will note that the description of the system very clearly demonstrates that what was contemplated therein was a tape 1000 characters in length interacting with another 999 in length.

The “extracts” refers to Churchill’s note in [4, Churchill to Mauborgne, 8 Aug 1918]. Parker’s hand-written comment on Friedman’s letter reads “I shall to [sic] dispute this as it was not true of Vernam and myself.”

The two exchanged another pair of letters on the topic during the war. Parker stressed that “the engineers of the A.T.&T. Co. never believed that [the two-tape system was absolutely secure] but they did believe that the use of a non-repeating single key tape could give such security”. He also claimed, recounting a meeting where (presumably) Mauborgne said that the single tape system was impractical, that [17, Parker to Friedman, 16 Mar 1944]:

I argued with him a bit at that time on the value of the secrecy obtained by the single key system. It is remembered that this argumentative attitude was out-of-line with the feelings of my bosses.

Friedman again disagreed [17, Friedman to Parker, 16 May 1944], noting that the Gherardi letter [4, Gherardi to Fabyan, 11 Jun 1918] did not distinguish between the security of the two schemes:

I am, I regret to say, not quite prepared to accept at its full value your assurance that *all* the engineers of the A.T.&T. Company never believed the duplicate tape system to be absolutely secure. My own recollection of the manner in which Mr. Gherardi handled the matter is too clear to permit me to do so.

He went on to note his opinion that a single-tape system likely was impractical in 1918, though “the problem has been solved in a practical fashion but I much doubt whether it could have been in those days.”

There are two other important documents showing Parker’s and Friedman’s attitudes; both concern a Scientific American article by Kahn [19]. Friedman himself annotated a copy of the article with “not true” by the discussion of Mauborgne’s role ; there is also a suggestion that he write Kahn. (See [18, *Scientific American* article, Jul 1966]; also see [28, p. 237].) Parker, for his part, drafted a letter to be sent to AT&T management under Friedman’s signature urging them to respond to Kahn; this letter cited the 1956 article and stated that it had been reviewed by Vernam [17, Parker to Friedman, 4 Jan 1967]. An annotation by Friedman says that he called Parker to explain that he wouldn’t send it because the NSA wished to stay out of the controversy. Significantly, he did not challenge the substance of the letter: that Vernam, not Mauborgne invented non-repetition.

It is likely that Mauborgne in 1918 and Friedman in 1943 were right that distribution and control of one-time tapes was infeasible during wartime. They were military and cryptologic professionals, well aware of the chaos and fog of war; Vernam and Parker were not. By the time of Friedman’s second letter to Parker, he was undoubtedly aware of just how much the Japanese Navy’s trouble distributing revised copies of JN-25 had helped the Allies [22]; it would have been no stretch to extend that to the more difficult problem of one-time tapes. In fact, it is less clear why he felt it had become manageable by 1944, though perhaps he was talking more about the problem of generating so many random characters.

Parker’s opinions have long been known. What is new here is that as long ago as 1942, he was concerned that the true story be told. His assertions that he and Vernam understood the security difference are not entirely credible. For one thing, Friedman’s successful attacks on the two-tape system sank the entire project; one would think that there would have been an attempt to push the stronger version, but there is no evidence for such an effort. Indeed, a 1933 diagram [5, Teletypewriter ciphering set, 8 Nov 1933] shows a Morehouse machine. Perhaps more significantly, Gherardi’s letter shows no sign of awareness of any difference (though admittedly Gherardi was by then a member of management and was perhaps not cognizant of all of the technical details). However, Parker’s version of the history, long before Kahn had suggested that Mauborgne had a role, had always stated that AT&T suggested the single-tape solution but that the Army—Mauborgne—didn’t want it.

The most detailed exposition of Parker’s reasoning is in a 1967 memorandum [17, Parker, memorandum, 1 Mar 1967], apparently intended for AT&T management. Some of his arguments are less than convincing. For example, in

Part III he claims that “simple reasoning” leads to the notion of a non-repeating, random key. That this was obvious would surely be a surprise to the generations of cryptologists who preceded Vernam. He also claims that it is obvious that a loop is insecure, and that cryptanalysis, though “difficult”, can be done. Other quotes from early memoranda by Vernam and others do suggest an awareness of non-repeating keys, but also discuss other variations. The multiplicity of suggestions does tend to confirm the notion that though Vernam and company may have invented non-repetition, they did not have a clear understanding of its theoretical properties.

Most significantly, Friedman appears to agree that Vernam first came up with the crucial concepts, even if he didn’t quite understand them all. While Friedman’s relations with Kahn were prickly (see, e.g., [28, p. 10]) and while he became good friends with Parker later on, in the 1940s neither of these were true. As the external tester, he was extremely familiar with the AT&T machine, and visited there. Shortly thereafter, he left Fabyan’s lab and went to work for Mauborgne. He was thus ideally positioned to have heard the entire story, from all concerned. His acceptance of the story in the 1940s, and his refusal to disagree in the 1960s, thus strongly suggest that he was already familiar with and therefore agreed with Parker’s version. This is perhaps the strongest evidence that Vernam did indeed invent non-repetition.

4 Behavioral Indications

There are a number of clues from the behavior of various parties that are useful as well.

4.1 Patent Issues

There are a number of oddities in some of the AT&T patents on the project that tend to support the notion that Mauborgne played a major role. To explain, though, it is necessary to give a brief tutorial on patents.

A patent may be granted for an invention that is novel, useful, not previously published, and non-obvious.³ Prior publication of an idea bars someone else from seeking a patent on it. Crucially, a patent does not confer the right to manufacture something; rather, it is the right to prevent someone else from doing so.

Philosophically, a patent is a contract between an inventor and society. In exchange for teaching people about the invention, the inventor is granted a limited-term monopoly on the invention. The teaching is done in what is called the “specification”; the scope of the invention—that is, the outer boundary of the inventor’s monopoly—is set forth in a series of “claims”. The specification is more or less an ordinary technical paper, albeit written in a somewhat stylized fashion; drafting a good set of claims, though, is how patent attorneys earn their keep. Such a set of claims can be really hard to construct, because of the desirability of claiming as many variants of the invention as possible while not claiming more than can be defended. Broad claims prevent people from inventing their way around the patent by coming up with a trivial variant not covered by the claims.

An example (taken from [29]) will help. Suppose someone has invented the stool and wants to patent it. An obvious claim would describe a device comprising a “flat surface and four legs descending from it to the ground.” That, however, would let someone build a non-infringing stool with three legs; this patent requires four. On the other hand, a five-legged stool does infringe; that device has the four legs that the invention requires, and thus contains the invention. It has something else as well, but that doesn’t matter; it could also have a back, decorations, a drink holder, and more, all without affecting whether or not it infringes the patent. The proper claim language is probably something like “a seat and one or more elongated support members for supporting the seat above an underlying surface”.

Patents typically include language in the specification to show that the inventor is aware of trivial or obvious variants. For this stool, it might say something like “it is obvious that the legs need not be wood, but may instead be metal, plastic, or any other suitably strong substance”. That will protect the inventor, even if all of the rest of the language in the specification speaks of wood.

One issue in the AT&T patents is the question of randomness. Given that they knew of it in June, 1918, why did Vernam’s September 1918 patent application not make it part of the claims? Randomness is mentioned in the specification section of the patent:⁴

³ See §101–103 of Title 35 of the U.S. Code.

⁴ U.S. Patent 1,310,719, page 3, column 1, line 18.

The ciphering devices at the opposite ends of the line are provided with identical sections of tape upon which are recorded a series of code signals which are preferably selected at random but if desired may themselves represent a predetermined series of letters or words.

There is similar text in Morehouse's patent: "Each of the transmitters X and Y is provided with a separate perforated tape or equivalent record having a series of characters represented thereon preferably selected at random."⁵ If Mauborgne indeed had a hand in coming up with the concept, for Vernam to have claimed it would have been improper. U.S. patent law at the time required that "the applicant shall make oath or affirmation that he does verily believe himself to be the original and first inventor or discoverer of the art, machine, manufacture, composition, or improvement for which he solicits a patent."⁶ False statements here constitute perjury; omission of an inventor can render the patent unenforceable. The sworn declaration, though, applies only to the claims section of the patent; other people's work can be included in the specification section. In other words, if Mauborgne had had a hand in the invention of anything covered in the claims, his name had to be listed as an inventor; however, if he only invented something mentioned in the specification but not the claims, his name could be omitted.

It is also unclear if including the randomness requirement in the claims would have been possible. Under the case law of the time, and in particular a Supreme Court ruling in *O'Reilly v. Morse* (56 U.S. 62, 1854), abstract ideas could not be patented. The notion of a random versus a comprehensible key would not change the hardware; to have included the requirement might have rendered that part of the invention unpatentable. Strongly linking the encryption system to a randomness requirement might have risked invalidating the entire patent. It is quite likely that a cautious attorney would have counseled omitting any such claim.

Finally, including a randomness claim might not have provided AT&T any benefit. No one else could build the encryptor without licensing the AT&T patent; mentioning that keys should be random discloses the concept and as noted thus prevents anyone else from patenting it and barring AT&T from using it.

If the Vernam patent has an anomaly—no mention of Mauborgne—Morehouse's patent on the two-tape variant (U.S. 1,356,546) is downright strange. For all that *O'Reilly v. Morse* barred patenting abstract idea, this patent does just that.⁷ The specification says "It is not important in the use of the invention that the effect of combining the two or more characters from different series should be actually manifested in a discernible form." While mentioning alternative embodiments is conventional, saying that it could be done without a physical mechanism was decidedly odd for the time. The claims make this even more explicit; most are written without any reference at all to hardware. Here is the first claim:

The method of enciphering or deciphering messages which consists in forming a plurality of series of ciphering characters different in each series, selecting characters from each series in a fixed order to form a continuous sequence by retraversing the series as it is exhausted, and altering the message characters in accordance with a predetermined rule whose effect upon successive message characters is dependent upon the concurrent use of characters so selected from different cipher series.

There is no mention of relays, currents, contacts, paper tapes, grounds, batteries, etc. The description is purely algorithmic. The patent claims don't even mention paper tape loops until claim 12. Electrical contacts are not mentioned until the last claim. Such language would not be unusual today, when the actions could be carried out by software; in 1919, it may be unprecedented. However, examination of the file history—the record of correspondence between the patent examiner and the inventor—shows that the examiner did not object to the language.

The anomaly that bears on the priority question, though, is in a letter from William R. Ballard to Mauborgne on November 21, 1918 [1, Kahn's notes on AT&T files, 15 Jun 1964].⁸

In accordance with your request, I am enclosing a copy of a claim drawn for use in the double key ciphering case, which we discussed last Tuesday. The object, as you will recall, was to supplement the method claim already prepared to be sure that the protection would extend to such uses of the double key system as you explained to me.

⁵ U.S. Patent 1,356,546, page 2, column 1, line 30.

⁶ This is from Section 30 of the Patent Act of 1870, which was in effect at the time.

⁷ The two patents were drafted by the same attorney, G.E. Folk.

⁸ This text is taken from Kahn's notes. I was unable to locate Ballard's letter.

The part of the specification this is referring to begins on page 3, column 2, line 67:

To practice the invention it is only necessary that there shall be [a] plurality of series of ciphering characters, differing in length, so that they may be used repeatedly for combining with another series without producing a cyclic repetition of the same character or sequence of characters in the resulting series, and that each character be assigned a definite form, position, value or other characteristic (the electrical symbols, such as + + - - - for A, in the embodiment above described) such that those for characters of different series may be combined, in accordance with some predetermined rule, to produce definite effects, indications or symbols, which in turn are similarly combinable with characteristics assigned to the characters of the message.

It is extremely hard to explain why Mauborgne should have requested new claim language to cover what Ballard describes as “such uses . . . as you explained to me” (emphasis added). That text seems to imply that Mauborgne came up with some uses for the system. If that is the case, Mauborgne should have been listed as a coinventor. If his contribution was somehow not sufficient to qualify him as a coinventor, why did he suggest or approve new claim language? Such an activity protects AT&T’s interests; it does nothing to advance the interests of the U.S. Army. Mauborgne certainly wanted AT&T to manufacture these devices to protect American communications, which it could not do if someone else were to patent this feature; as noted, simply publishing the idea would accomplish that goal. The most likely answer is that Mauborgne had worked closely enough on the invention that he saw some uses for it that needed to be protected. Note that this contradicts Parker’s assertion that “Col. Mauborgne was a stranger to us; one who represented authority . . . [who] failed to grasp the significance of what he had seen” [1, Parker to Kahn, 17 Mar 1963]. The most likely subject of this concern was the the ability to use two tapes to generate a single long—and, he thought, secure—single tape.

4.2 Random Keys

Examination of the AT&T archives shows that the randomness requirement was set forth explicitly in a memo accompanying a letter from Bancroft Gherardi, assistant chief engineer of AT&T, to George Fabyan, the founder and director of Riverbank Laboratories [4, Gherardi to Fabyan, 11 Jun 1918]. (It is unclear who prepared the memo. The copy in [15, Gherardi to Fabyan, 11 Jun 1918] has the hand-written notation “Return to R.D. Parker”; this notation is not on the copy in the AT&T archive [4].) This is the famous challenge letter, where Gherardi gave seven ciphertext messages to Fabyan and William F. Friedman (an employee of Fabyan’s) to solve. In this letter, Gherardi gave the following description of the encryption process:

Our standard printer alphabet was used in preparing these messages. This alphabet consists of thirty-two characters.

...

In preparing these messages the message to be enciphered was first put in perforated tape form, and then enciphered by combining this tape with one or more others having the characters of the printer alphabet, chosen at random.

The memo goes on to describe the seven messages. #1 was encrypted with a true one-time pad. #2, #3, and part of #4 reused the same portion of the key tape. #5, #6, and #7 were encrypted with Morehouse’s two-tape system, using loops of 1,000 and 999 characters.

Note that Gherardi explicitly specified “chosen at random”, though he did not use the phrase “key”. It is likely, though not certain, that all 32 possible values for each key character were used, since Gherardi used the phrase “printer alphabet” both here and when describing the 5-bit Baudot code. I have not found anything to indicate how they derived this requirement, nor any explicit requirement for a uniform distribution of key values.

Parker claimed in 1942 that “in the early days we argued that a single non-repeating key of random characters could, with our machine, give absolute secrecy as well as rapid encipherment and decipherment” [15, Parker to Friedman, 30 Jan 1942]. This is the earliest explicit assertion available that AT&T had invented the idea by itself. In 1967, Parker wrote that key characters were selected by pulling slips of paper from a container [17, Parker, memorandum, 1

Mar 1967]: “This was the inventor’s idea of a random key.” This, however, was after the controversy over credit had started.

There is one more item to consider, though. Very shortly before Vernam’s invention, Friedman [6] and Yardley [27, Yardley to Churchill, 15 Sept 1919] independently devised a solution for running key ciphers, i.e., coherent long keys taken from, say, a book.⁹ Mauborgne knew of this; indeed, Yardley’s attempt sprang from a conversation with Mauborgne in October 1917. He showed his results to Mauborgne in December. It seems very unlikely that Vernam could have learned of this from anyone but Mauborgne; the discovery was very recent and not likely to be bandied about casually during wartime since the U.S. Army was relying on such ciphers in France. It couldn’t have come from Friedman; no one at AT&T knew him until Mauborgne sent a letter introducing Gherardi to Fabyan [4, Mauborgne to Gherardi, 22 May 1918]. This strongly suggests that Mauborgne told Vernam about the need for randomness. AT&T certainly knew of it when Gherardi sent his letter, but that was several months after Mauborgne’s visit. This reasoning is certainly not definitive but does leave Kahn’s conclusion (or rather, lack of a conclusion) open to question. Note that Kahn was aware of the running keys issue [1, Kahn to *Scientific American*, 6 Aug 1966]; however, I attach greater weight than he did to how recent that solution was. Of course, it could have been an independent realization; indeed, I showed in [2] that Miller had conceived of the need for randomness in 1882. Still that seems less likely to me.

4.3 Key Length

The key length issue is more complex and more interesting. The Gherardi letter says “I have no doubt that you can decipher Nos. 2, 3, and perhaps 4. These, however, as you understand are not the arrangement which we propose.” Message 2 and 3 used the same portion of a single key tape; message 4 used part of that tape but went beyond it. Message 1 used a true one-time tape; 5, 6, and 7 were produced by overlapping portions of a two-tape system. In other words, by June 1918 AT&T understood the danger of reuse of the effective key stream, or Gherardi would not have expected Friedman to be able to solve #2, #3, and the part of #4 that overlapped the prior two. Note that 1, 5, 6, and 7 are lumped together as secure and as what AT&T proposed. To be sure, Mauborgne had joined the project by then [22]; the insight about the one-time tape could have come from him. However, other documents make it clear that even he did not yet realize the full importance of non-repetition.

A brief memo from Churchill to Mauborgne, given in full below, makes this clear [4, Churchill to Mauborgne, 8 Aug 1918]. Undoubtedly, Yardley wrote this note.

The mechanical means of enciphering messages with an arbitrary, meaningless running key of 999,000 letters, provided no two messages are enciphered at the same point on the tape as explained to Major Mauborgne, Signal Corps, and Captain Yardley, Military Intelligence Branch, by officials of the American Telegraph and Telephone Company, is considered by this office to be absolutely indecipherable.

There are a number of very important points in this note.

First, Churchill explicitly references a key of “999,000” letters. That is the length of the keystream provided by Morehouse’s dual looped-tape system, rather than the length of any single tape. In other words, Herbert Yardley was endorsing a stream cipher, rather than a one-time pad. The considerable length of each constituent tape was important, as was the requirement for an “arbitrary, meaningless” key; this differentiates the design from the toy encryption using “ARMOR” and “THOMAS” that that Mauborgne perhaps showed the weaknesses of [22]. Still, this is not a one-time pad.

The mention of Yardley is itself interesting. No prior source mentions his involvement in evaluating Vernam’s invention. Churchill’s memo appears to have been sent just around the time that Yardley left for Europe [23].

Mauborgne himself continued to believe in the two-tape solution for quite some time. In a letter more than a year later from him to Fabyan, he explicitly asked for an evaluation of both it and the true one-time pad [4, Mauborgne to Fabyan, 10 Dec 1919]. This by itself does not mean that he did not appreciate the difference; however, the description of the two-tape shows his concern with one aspect of it:

Cipher indicators to be encoded, and the cipher is to be used for the body of the message alone: two cipher tapes to be used as in former practice.

⁹ Yardley accused Friedman of stealing his solution; Friedman strongly disputed this and noted that his manuscript had been finished in September 1917, before Yardley had even tackled the problem.

He also says:

The dangers, of course, in not encoding the cipher indicators were clearly demonstrated by you some time ago with the result that it was decided that anything further in the way of official business sent over the cipher printer would have these indicators encoded.

(Red, hand-drawn underline in the AT&T copy.)

This and his later note to John Carty [4, Mauborgne to Carty, 22 Jan 1920] make clear what the problem was: if the indicators were readable by the enemy, they could find the overlaps in each key tape, and thus recover both tapes and read messages.

The copy of the 10 December letter in the AT&T archives is an onion skin carbon copy, so it was presumably sent by Mauborgne himself to AT&T. The underlining was apparently done by Mauborgne, to ensure that Fabyan realized the need to encrypt the indicators.

The 22 January letter to Carty contains a typed addendum from an AT&T “equipment development engineer” (the signature is illegible, though it appears to begin with the letter “F”) mentioning the need to develop an encryption scheme for the indicators.

Mauborgne’s letter to Fabyan also notes a possible role for both Parker and Genevieve Hitt. He asks Fabyan for:

All statements, if any, or suggestions forwarded by Colonel or Mrs. Hitt in connection with the decipherment of these messages as a result of their intimate connection with this office, which you received during the course of this experiment and which may have led you to its solution.

The context was an inquiry asking for what other information Fabyan (and Friedman) may have had. At the time Colonel Hitt was assigned to the War College, not the Chief Signal Office [31]. His wife was no longer working as a cryptanalyst by 1919, nor is there any record of her having any contact with Fabyan’s lab after 1917 [30]. The answer seems to lie in letters from Fabyan to Colonel Hitt, seeking cribs to some of the messages [24, Fabyan to Hitt, 25 Oct 1919][24, Fabyan to Hitt, 27 Oct 1919]. (This is not, of course, cheating; cribs are a venerable technique in cryptanalysis, and assessing the susceptibility of a new cipher machine in the face of some known or probable plaintext is certainly legitimate [21].) Most likely, Mauborgne—being a close friend of Colonel Hitt’s and knowing of Genevieve’s cryptanalytic abilities—added her name to be sure.

The clearest statement of Mauborgne’s confidence in the two-tape system is contained in a letter he apparently sent to Fabyan on November 28, 1919:¹⁰

You know I have never admitted that you had any method for solving this cipher, and, as in the case of all these academic debates, you will have to produce the proof!!! I am sorry that I cannot get a chance to watch your work as it goes because no doubt you have perhaps reached other methods of suggested attack than those you have already described. No doubt you have tried and discarded what might, perhaps, have some bearing on other work. As you recognize, the by-products of this investigation are highly worth while [sic] even though there never was, as there never will be, a real solution.

Ten days after this letter, Fabyan telegraphed Mauborgne announcing that a solution had been found [4, Fabyan to Mauborgne, 8 Dec 1919].

The letter to Carty makes clear that as of January 1920 Mauborgne had at most a slight preference for the true one-time pad solution compared with the two-tape option. He quotes a letter he sent to Churchill saying that the “Chief Signal Office”—himself, presumably—was:

of the opinion that there are two methods by which this cipher can be used which will insure [sic] secrecy and freedom from decipher ability: first, return to the method first proposed for this machine, viz, that only one cipher tape, consisting of a running key selected at random, be used, and that the length of this tape should be sufficient to take care of the total number of messages to be sent in one day by all stations concerned. This scheme entirely eliminates the difficulty produced by cyclic repetitions introduced by the

¹⁰I have not seen the original of this letter. This excerpt is contained in the attachment [17, Extracts from Correspondence Relating to Solution of A.T. and T. Printing Telegraph Cipher, 12 Oct 1943] to a letter from Friedman to Parker [17, Friedman to Parker, 12 Oct 1943]. The attachment also shows the extent of Yardley’s involvement in the evaluation.

use of two or more key tapes. Mechanical difficulties of handling such a tape are not unsurmountable. Colonel Hitt who has examined this proposition, is satisfied that such a method will provide absolute indecipherability; second, to employ the method already proposed, viz., encipher the key indicators and continue to use two or more cipher tapes as keys. Major Yardley, as you remember, is satisfied with this system, believe that it will provide indecipherability.

His mention of “cyclic repetitions” shows that he is aware of some potential for trouble from using two tapes, presumably as a result of Friedman’s earlier success. However, other than stressing the need for encrypted indicators he does not seem aware of any attacks, so long as the key tapes are long enough. His authority for pronouncing the one-time solution absolutely secure is Colonel Hitt; Mauborgne would not have done that had Hitt not devoted serious effort to analyzing the scheme.

The endorsement of the two-tape scheme is attributed to Yardley. At the time, Yardley was running his covert cryptanalytic shop in New York with funding from the State and War Departments [23]. No other source of which we are aware indicates that he had any role in evaluating Vernam’s scheme; still, Churchill valued his abilities. It is likely that this 1920 letter does not refer back to Yardley’s 1918 work, since it quotes Churchill (in very late 1919 or early 1920) as having received a report from him “several months ago”. History remembers Colonel Hitt as a better cryptanalyst than Yardley, especially when dealing with ciphers rather than codes, but that is retrospective; it is not clear that anyone thought that at the time. It is unclear how much weight to attach to the difference between “absolute indecipherability” and “indecipherability”; probably, he saw some difference but accepted Yardley’s opinion that the two-tape variant was very, very strong.

Churchill says that he prepared a “tentative code book to be used for the encoding of the key indicators” [4, Mauborgne to Carty, 20 Jan 1920]. The typed AT&T note at the bottom of that letter suggests that they wished to develop their own indicator encryption scheme; presumably, this is what led to Vernam developing a solution and receiving U.S. patent 1,479,846. The application was filed on June 23, 1920 and issued Jan. 8, 1924; the unusually long (for that era) processing time suggests a fair amount of give-and-take with the patent examiner.

Finally, the letter to Carty concludes by suggesting that he ask Fabyan (that is, Friedman) if the two-tape solution is secure if encrypted indicators are used. This clearly shows that Mauborgne himself did not know of any way to attack such a scheme.

The person who may have first understood the strength of the true one-time system was Friedman. In his report on the solution of the two tape system [10, Addendum 1], he wrote:

Since carelessness on the part of the personnel to be entrusted with the operation of machine ...[is] to be expected, the existence of this opening for an attack must be admitted. Secondly, we shall attempt to show, granting not only an absolutely infallible operation of the machine by the personnel, but also the theoretical absolute indecipherability of a message enciphered by means of a random-mixed, single, non-repeating, running key, ... that an attack is not only practicable but easy under normal conditions.

Did he actually realize the theoretical strength of the system at this time? It would seem so. The text at the start of the quote shows his awareness of the likelihood of human error. There is no such qualifier anywhere in the document about any way to attack the true one-time system. This is the first clear statement by anyone that the true one-time system is indeed perfectly secure if properly used. This is to some extent supported by a 1967 memo by Parker [17, Parker, memorandum, 1 Mar 1967] that states that it was outside experts—Friedman and company—who concluded that the one-time tape was secure, but that the two-tape system was not.

Probably just a bit later, Friedman made the first unambiguous statement about the requirements for and properties of true one-time pads [8, Differential Primary Keys in Cryptography]:

All popular ideas to the contrary notwithstanding, the condition termed “absolute indecipherability” is by no means purely chimerical, or impossible of production, for the existence of but one case in which it can be demonstrated that such a condition has been produced is sufficient to establish the validity of the hypothesis, as well as of the possibility of the existence of other absolutely indecipherable systems. One such case is exemplified in that type of cryptographic system known as the “running” or “continuous key” method, in which the key and its method of employment conforms to the following conditions:

(1) As to its method of employment, the key must be applied to the plaintext to be enciphered in such a manner that its successive, individual elements are employed to encipher the successive individual

elements of the plaintext; and once having been used, neither the whole key nor any part of it must be employed a second time.

(2) As to the nature the key must be:

(a) absolutely unintelligible in the cryptographic sense;

(b) as nearly absolutely nonrepeating as is mathematically possible;

(c) a primary or basic sequence, not a secondary or derived sequence such as can result from the interaction of two or more relatively short primary sequences.

He then went on to explain why the system was secure. His basic argument was that there could be no consistency check with a one-time pad. That is, a cryptanalytic attack on an older cipher in effect makes predictions: that the key and algorithm recovered for one section of the message implicitly predict that using them in some fashion on another part will yield intelligible text

When this can be done with each and every letter of the cryptogram, and each and every letter of the solution offered, *and the latter makes intelligible sense*, the proof may be regarded as being complete.

(Emphasis in the original.) Unfortunately, the date of this memo is unclear. A typed headnote says that “the material for this paper was first prepared in 1920” at Riverbank, but other text in its body speaks of a course he taught in 1924. It appears to be a replacement for the first two pages of [9], which was almost certainly written in 1920; see Section 5.1.

Conversely, one can question just how deep AT&T’s understanding of the problem was, even as late as 1925. In comments on a draft of Vernam’s paper [35], Friedman noted [5, attachment to letter from Lt. Col. Voris to Morehouse, 7 Nov 1925]:

The statement that the double-key system can be used “without appreciably reducing the secrecy of the system” considerably underestimates the degree of success that the expert cryptanalyst may have in attacking messages prepared in this way as compared with the case wherein a single non-repeating key is used.

Vernam changed the text to say that

If proper care is taken to use the system so as to avoid giving information to the enemy regarding the lengths of the two tape loops or their initial settings... this system is extremely difficult to break even by an expert cryptanalyst having a large number of messages...

The conditional clauses no doubt refer to suitably encrypted indicators.

5 Friedman’s Insights

5.1 The Two-Tape System

While a full exposition of how Friedman solved the two-tape system is beyond the scope of this paper, a brief discussion of his approach is necessary to understand the next section. His own description is in [10].

To an academic, the two-tape variant looks something like this:

$$C_i = P_i \oplus A_{i \bmod |A|} \oplus B_{i \bmod |B|} \quad (1)$$

where C_i is a ciphertext character, P_i is the corresponding plaintext character, A and B are the two sets of keying characters, and $|A|$ and $|B|$ are the lengths of A and B . It’s simple and obvious; it’s also not usable in the real world.

The major item that is missing is the “indicators”, some metadata sent with the message saying where on the tapes the encryption started and perhaps to state which key tapes should be used. That, coupled with the length of each message, was what Friedman initially exploited, along with the reciprocity of XOR encryption. His approach was simple: given the starting position of each tape and the length of each message, it is straightforward to find where two or more messages were encrypted using the same section of a key tape. By stacking messages this way, and by trying probable plaintext words such as names and addresses, he was able to strip off (and hence recover) each of

the key tapes. (The full prescribed format and procedural rules were given in Addendum 1 to his report [10].) One particularly useful piece of plaintext was the sequence carriage return-carriage return-line feed (denoted 442); this had to occur every 60 or so characters because of the limited line length of the receiving teletype. Note that he was working with 150 messages, an approximation of one day’s traffic from a busy location during wartime; this gave him many messages to stack together to find overlaps.

His solution relied heavily on the concept of “sequent cycles”—combinations of tape lengths that had favorable, small displacements of the relative positions of the two tapes. To use his own example from [9], assume that the two tapes have lengths of 24 and 25 characters. After the longer tape makes one complete loop and is back to its first character, the shorter one is on its second character; these two cycles are thus sequential or “sequent”. His scheme worked well with cycles that were not further apart than 25 or so characters.

Friedman took a few months to solve this, but that was largely because of a transcription error in recording the ciphertext. Once that was corrected—and, no doubt, using the techniques that had been worked out during those months—he solved for the key tapes quite quickly and used them to encipher his reply.

Yardley and Mauborgne were duly horrified. Mauborgne, as the representative of the Office of the Chief Signal Officer, could mandate encrypted indicators; Yardley prepared the encipherment [16, Yardley, A.T.&T. Cipher Indicator Code]. Unfortunately, it wasn’t very well done. It was a two-part code with no homonyms; each possible 3-digit indicator was mapped to a 3-letter codegroup. Each letter in turn was encrypted with a separate monoalphabetic substitution. The codebook was intended to be relatively long-lived; the substitution tables were to be changed daily. Key tapes were limited to 999 characters for mechanical reasons. A loop of that length was about 8 feet in circumference; the physical arrangements to handle it imposed *some* maximum length. (Judging from a photograph in [35], their implementation used loops that dangled beneath the machine; possibly, spring-loaded pulleys could have been used.) Friedman solved Yardley’s indicator encryption very quickly; he was then able to use his previous solution [10, Addendum 3].

There appears to have been no serious attempt to improve the indicator encryption after that. Vernam devised his own mechanism to encrypt them (US patent 1,479,846), but the military does not appear to have been interested. The Vernam design was largely retired until the the U.S. entry into World War II, when they were rushed back into service—with better keying and indicators—until enough newer devices could be produced and deployed [34].

Friedman himself took on a different issue: how could dangerous overlaps be prevented, especially in a multi-station network? In [8, The Mechanics of Differential Primary Keys], he used his attack to construct safety conditions designed to minimize the probability of the same two regions of the same two tapes would be used to encrypt different plaintexts and that no sequent cycles occur. He concluded [p. 57, 8, The Mechanics of Differential Primary Keys] that “in order to ensure to assure absolute safety, the communicating stations must use different pairs of primary keys” and that “all the primary lengths must be prime numbers.” This is arguably the first use of prime numbers in cryptography.

In devising this scheme, he also solved a crucial operational problem with one-time tapes. In an n -station network using one-time tapes, you would need n^2 tapes so that every station could send to every other. However, in a simple Morehouse/Friedman network, where every node needs the ability to talk to every other, you would need only about $\sqrt{2n}$ tapes for each station to have a unique pair to use when sending. It is likely that some variant of this scheme is what Friedman says was used during World War II [34].

5.2 The Index of Coincidence

Friedman’s solution of the two-tape systems deserves its own paper. Even the administrative aspects were complex; there was a lot of confusion and hostility, plus misunderstandings about the precise indicator format and usage rules, complaints about inadequate amounts of ciphertext supplied, and even transcription errors. The best summary of that is in a memo he compiled [17, Extracts from Correspondence Relating to Solution of A.T. and T. Printing Telegraph Cipher, 12 Oct 1943].

Through all that, he apparently stuck with the same (and ultimately successful) technical approach: using the indicators to find sections of multiple messages that used the same keying tape. It had to have been obvious to him that encrypting the indicators was the next step. This was, as noted, done; however, it was done poorly. The next obvious step would have been a strong way to protect the indicators, one he couldn’t crack. Friedman had to have wondered if there was another way to find the overlaps. Is it possible that this led him to invent the index of coincidence?

Friedman solved Yardley's indicator book in early March, 1920. The index of coincidence manuscript was given to Fabyan in the summer of that year [3, p. 77]. The timing strongly suggests that trying to crack the two-tape Vernam system led Friedman to his idea. To think otherwise, during peacetime when there was much less need for "real" cryptanalysis, would require too much of a (if you will pardon the expression) coincidence. The two-tape AT&T machine was a problem for which his invention was a solution; we know of no other such problems at this time beyond the pure academic question.

Suppose, though, that the index of coincidence had existed prior to Morehouse's conception of the two-tape scheme. Could it have been used? In theory, the answer seems to be that it could; in practice, though, it is unclear if it was feasible in 1920.

The index of coincidence works because plaintext has a non-flat distribution. The encryption equation for any plaintext character P_i in a two-tape Vernam system was given in Equation 1. We can consider this as encryption with first one tape and then superencryption with the second. Consider the encryption of a character with just the first key tape, $P_i \oplus A_i$. If the string of plaintext is shorter than the length of the key tape, the distribution of the ciphertext bytes will be flat. However, if the plaintext is longer the keytape will repeat, resulting in situations where the same position in the key tape will be used to encrypt the same letter of plaintext. The distribution of values is therefore not flat; in particular, since there are 32 values in the Baudot alphabet Vernam used, the frequency of any given letter will be $\frac{1}{32}$ of that in plaintext. This is much flatter, of course; accordingly, considerably more ciphertext will be necessary to find the overlap. Encryption with the second will reduce the frequency still more. Could sufficient text be intercepted to make recovery feasible? In wartime, this might be possible, though it may have been difficult. The real barrier might have been computational; it is necessary to do the index of coincidence computation for every possible overlap offset.

Using the index of coincidence requires calculating some value (the phi value in Friedman's day) for each possible offset, i.e., for about 1,000 different alignments of the message or messages. This would have been very time-consuming by hand, though perhaps that is what enlisted personnel are for. The same process would have been necessary for each new message intercepted, a necessity to build up a sufficient depth of ciphertext for each position to enable use of Friedman's attack. This might have been feasible with the machine-assisted cryptanalysis that came into being in the 1930s; it seems rather more dubious for 1920. (It is perhaps worth mentioning that during World War II, the military built a photoelectric machine to find overlaps via the index of coincidence [26, Memorandum to John H. Howard: Proposed cryptanalytical machines, 25 Apr 1942]; doing it by hand was too time-consuming.)

6 Conclusions

The need for randomness seems to have been appreciated very early, both by Vernam (or perhaps his colleagues at AT&T) and by Mauborgne. I found nothing to contradict Kahn's conclusion that this was likely done without real comprehension of the strong need for it; nevertheless, the Gherardi letter and the AT&T patent mention it, and the Churchill memo notes that the AT&T system was "explained to Major Mauborgne, Signal Corps, and Captain Yardley, Military Intelligence Branch." Perhaps this is a formalism of speech and reflected nothing more than acknowledgment of AT&T's role; after all, Vernam did explain it to Mauborgne at some point, even though Mauborgne started working with the device by the spring of 1918. That the AT&T patent permits use of a "predetermined series of letters or words" does not indicate lack of comprehension; patents often disclose concepts not believed to be useful to prevent someone else from subsequently discovering a use and then patenting it. The coincidence of timing between the solution of running key ciphers and the adoption of random keys for the Vernam machine may be just that, a coincidence. On balance, I think it more likely than not that Mauborgne told Vernam, but this point remains debatable.

The origin of the requirement for non-repetition seems clearer. Almost certainly, Vernam came up with the idea. Both Vernam and Mauborgne seem to have appreciated its strength compared with alternatives, but without full comprehension; Mauborgne in particular appeared to have some misgivings about the two-tape system but not enough to prevent him from endorsing it in January 1920. He understood the danger of repetition of the effective key stream; he did not clearly see that a key stream composed from two shorter, repeating streams was dangerous. It was Friedman who was the first to realize the essential weakness of the two-tape system and the theoretical strength of the true one-time tape. He understood *why* it was strong, in a way that no one else did.

There are several documents I have not been able to locate that might shed more light.

- First, of course, are the original AT&T documents that Kahn examined 50 years ago, and in particular the RIFLE/THOMAS memo. Ballard’s letters to and from Mauborgne would also be valuable.
- Vernam kept a technical diary. The diaries for 1918–1919 and 1922–1926 are in the George C. Marshall Foundation library; however, his diary for 1917 has never been located [14, Friedman to Nielssen, 2 Mar 1969] [14, Nielssen to Friedman, 22 Jun 1969] [11].
- Friedman gave a 1948 lecture about the AT&T machines, which was later printed in an internal NSA journal [7]; as of this writing, it has not yet been declassified. It may also shed some light on the history.
- Some of Friedman’s papers have not yet been declassified. When they are released, they may shed more light, too, especially about how he used the two-tape system.

Although there is no explicit confirmation in Friedman’s papers, it seems extremely probable that attacking the two-tape system is what led him to invent the index of coincidence, a “by-product” of what was ultimately a successful attack. There is thus a linkage between some of the most important developments in classical cryptology: the first online encryptor, the first absolutely secure cipher, and the paper that turned cryptanalysis into a mathematical discipline.

The narrative of the invention of the Vernam-Mauborgne one-time pad is more complex than had been thought, with even more ramifications for the history of cryptology than had been realized.

Acknowledgments

My primary thanks must go to David Kahn. He more than suggested this project, he strongly and repeatedly urged it, even though he realized that the conclusions might disagree with what he wrote all these years ago—as indeed they have. Beyond that, his well-organized notes from 50 years ago were extremely useful.

This paper could not have been begun, let alone written, without the aid of AT&T Archivist George Kupczak. His help was invaluable, especially his work in finding the crucial file folder containing not just the cited letters but also the original paper tapes sent to Fabyan in the challenge. My long time friend and collaborator Bill Cheswick assisted in the research there.

Equally valuable was the assistance of Paul Barron, archivist at the George C. Marshall Foundation Library; he arranged for access to papers from the William Friedman Collection. Kathleen Kain, independent research assistant for the George C. Marshall Foundation, copied those documents for me.

Ben Lee provided useful guidance on patent legalisms. David Leshner assisted in research at the National Archives.

Betsy Rohaly Smoot of the NSA Center for Cryptologic History, an expert on the Parker and Genevieve Hitt, found many useful files and letters on most of the people mentioned here. Rene Stein of the National Cryptologic Museum Library helped me with access to papers from the Dr. David Kahn Collection.

References

- [1] *AT&T Machine folder*. Dr. David Kahn Collection, National Cryptologic Museum.
- [2] Steven M. Bellovin. “Frank Miller: Inventor of the One-Time Pad”. In: *Cryptologia* 35.3 (July 2011). An earlier version is available as technical report CUCS-009-11, pp. 203–222. URL: <http://dx.doi.org/10.1080/01611194.2011.583711>.
- [3] Ronald William Clark. *The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese Code in World War II*. Boston: Little, Brown, 1977.
- [4] *File 41-10-03-01*. AT&T Archives, Warren, NJ.
- [5] *File 433-06-01-02*. AT&T Archives, Warren, NJ.
- [6] W.F. Friedman. *Methods for the Solution of Running-key Ciphers*. Riverbank Publication No. 16. Geneva, IL: Riverbank Laboratories, 1918.

- [7] William F. Friedman. “Can Cryptologic History Repeat Itself?” In: *NSA Technical Journal* XVIII.3 (Summer 1973).
- [8] William F. Friedman. “Differential Primary Keys in Cryptography”. In: *Item 1056, William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA*. Although the actual manuscript was created no earlier than 1924, it contains a typed headnote saying that it was based on materials prepared at Riverbank in 1920.
- [9] William F. Friedman. “Mechanics of Differential Primary Keys”. In: *Item 1056, William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA*. 1920.
- [10] William F. Friedman. “Methods for the Solution of the A.T. & T. Machine Cipher”. In: *Item 669, William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA*. The title page has a hand-written note denouncing the March 1919 date as an example of Fabyan’s “finagling”. Friedman did not return from Europe until April 1919, and did not solve the system until December. Geneva, IL: Riverbank Laboratories, Mar. 1919.
- [11] *Gilbert Sandford Vernam Collection*. George Marshall Foundation Library, Lexington, VA. URL: http://www.marshallfoundation.org/Library/documents/Vernam_Gilbert_Sandford.pdf.
- [12] Parker Hitt. *Manual for the Solution of Military Ciphers*. Fort Leavenworth, KS: Press of the Army Service Schools, 1916. URL: <http://books.google.com/books?id=2MVBAIAAAJ>.
- [13] Parker Hitt and Thomas W. Brown. *Description and Instructions for the Use of the Fire Control Rule*. United States Infantry Association, 1917. URL: <https://encrypted.google.com/books?id=ExgxQAAMAAJ>.
- [14] *Item 669, Folder Nielssen*. William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA.
- [15] *Item 669.2*. William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA.
- [16] *Item 669.3*. William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA.
- [17] *Item 669.4*. William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA.
- [18] *Item 669.5*. William F. Frieman Collection, George Marshall Foundation Library, Lexington, VA.
- [19] David Kahn. “Modern Cryptology”. In: *Scientific American* 215.1 (1966), pp. 38–46.
- [20] David Kahn. *Private communication*. July 5, 2013.
- [21] David Kahn. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943*. Boston: Houghton Mifflin, 1991.
- [22] David Kahn. *The Codebreakers*. New York: Macmillan, 1967.
- [23] David Kahn. *The Reader of Gentlemen’s Mail: Herbert O. Yardley and the Birth of American Codebreaking*. New Haven: Yale University Press, 2004.
- [24] *Parker Hitt Papers*. David Kahn Collection, National Cryptologic Museum.
- [25] Ralzemond D. Parker. “Recollections Concerning the Birth of the One-Time Tape and Printing-Telegraph Machine Cryptography”. In: *NSA Technical Journal* I.2 (July 1956), pp. 103–114.
- [26] *RG457, E9032, Box 705*. National Archives and Records Administration.
- [27] *RG457, E9032, Box 776; also in SRM-050*. National Archives and Records Administration.
- [28] Rose Mary Sheldon. *The Friedman Collection: An Analytical Guide*. 2011. URL: <http://marshallfoundation.org/library/documents/FreidmanCollectionGuide.pdf>.
- [29] R.D. Slusky. *Invention Analysis and Claiming: A Patent Lawyer’s Guide*. American Bar Association, General Practice, Solo & Small Firm Section, 2007. ISBN: 9781590318188. URL: <http://books.google.com/books?id=WvpuGLMVg-QC>.
- [30] Betsy Rohaly Smoot. “An Accidental Cryptologist: The Brief Career of Genevieve Young Hitt”. In: *Cryptologia* 35.2 (2011). URL: <http://www.tandfonline.com/doi/abs/10.1080/01611194.2011.558982>.

- [31] Betsy Rohaly Smoot. “Pioneers of U.S. Military Cryptology: Colonel Parker Hitt and His Wife, Genevieve Young Hitt”. In: *Federal History* 4 (2012). URL: <http://shfg.org/shfg/wp-content/uploads/2012/12/6-Smoot-Web-final.pdf>.
- [32] Elizabeth Rohaly Smoot. *Private communication*. May 7, 2014.
- [33] *Standard ECMA-10 for Data Interchange on Punched Tape*. second. Geneva, Switzerland: European Computer Manufacturers Association, 1970. URL: <http://www.ecma-international.org/publications/files/ECMA-ST-WITHDRAWN/ECMA-10,%202nd%20Edition,%20July%201970.pdf>.
- [34] *The Friedman Legacy: A Tribute to William and Elizabeth Friedman*. Sources in Cryptologic History 3. Center for Cryptologic History, National Security Agency, 2006. URL: http://www.nsa.gov/about/_files/cryptologic_heritage/publications/prewii/friedman_legacy.pdf.
- [35] Gilbert S. Vernam. “Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications”. In: *Journal of the American Institute of Electrical Engineers* XLV (Feb. 1926), pp. 109–115. URL: <https://www.cs.columbia.edu/~smb/vernam.pdf>.