Vernam, Mauborgne, Friedman:

The One-Time Pad and the Index of Coincidence

Steven M. Bellovin

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

The AT&T Online Encryptor

- Encryption concept (XOR of keying material with plaintext or ciphertext) plus hardware to do it
- Random keying material
- Non-repetition of keystream

This is the one-time pad as we know it today.

Who Invented What Parts?

Vernam Encryption mechanism (XOR of keying material with plaintext or ciphertext) plus hardware to do it

Vernam? Random keying material

Mauborgne? Non-repetition of keystream

The latter two are Kahn's conclusions.

Revisiting the Question

- Kahn was never completely happy with his answer; some evidence was contradictory, and Ralzemond Parker of AT&T disputed it.
- “The problem of who invented the unbreakable cipher…was the most difficult I faced in my research.” (Kahn, 1966)
- Kahn suggested that we visit the AT&T Archives again

☞ We were unable to find one of the folders he had consulted 50 years ago

- I obtained other important material from the William F. Friedman Collection
- I reanalyzed Kahn’s notes at the National Cryptologic Museum

Kahn's Reasoning

- Mauborgne explicitly claimed credit for non-repetition
- He was a close colleague of Hitt's; Hitt made the first explicit statement about a key needing to be as long as the plaintext
- Parker said Vernam invented the randomness requirement; there was no other evidence for or against this claim
- Neither Vernam nor anyone else at AT&T had any cryptologic background

There Were Two Machines

- The Vernam machine used a single, long tape of keying material; the bits on this tape were XORed with the plaintext to encrypt or with the ciphertext to decrypt: $C_i \leftarrow P_i \oplus K_i$
- There are about 10 characters/inch on the keying tape; 100,000 characters would require $>$800 feet of tape
- The Morehouse machine used two keying material tapes of relatively prime lengths—for example, 999 and 1,000 characters long—and XORed both tapes together with the plaintext: $C_i \leftarrow P_i \oplus K_{1,i} \oplus K_{2,i}$
- The *effective length* of the keystream is the product of the length of the two tapes

The One-Time Movie. . .

Starring: Gilbert Vernam (AT&T), Joseph Mauborgne (Signal Corps), and William Friedman (Riverbank Labs)

With: Ralzemond Parker (Vernam's boss at AT&T), Bancroft Gherardi (Chief Engineer, AT&T), and George Fabyan (founder/owner of Riverbank)

Introducing: Lyman Morehouse (AT&T engineer; colleague of Vernam's)

And with guest appearances by: Herbert Yardley (MI-8) and Parker Hitt (Army)

Gilbert Vernam

(Photo: Wikipedia)

- Engineer in the AT&T development and research group; worked on encryption devices starting in 1917
- (Probably would have been at Bell Labs, had it existed then)
- "What can I invent now?"—received more than 60 patents
- Invented XORing a keystream with plaintext, plus the teletype hardware to implement it

Joseph O. Mauborgne

(Photo: courtesy Signal Magazine)

- Head of Research and Engineering, US Army Signal Corps
- (Later became Chief Signal Officer)
- Expert cryptologist; friend and colleague of Parker Hitt
- Army liason to AT&T
- Generally credited with inventing the non-repetition part of one-time pads

William F. Friedman

(Photo: Wikipedia)

- Pioneering cryptologist
- Worked at Riverbank Labs
- His invention of the *index of coincidence* turned cryptanalysis into a mathematical discipline
- Led the attack on the AT&T cipher machines

The Case for Mauborgne

- He made an explicit statement in a letter to Kahn: “Who invented [non-repetition] you have already deduced—yes, I did it.”
- His letter cites the Chief Signal Officer’s 1919 report and his own assistance in drafting claims for the patent
- (Why an Army officer should have helped draft claims for an AT&T patent is a separate mystery.)
- He also noted that he warned of the danger of repetition in a 999,000 character key stream

There Are Problems…

- The CSO report spoke of the Hoboken/Washington/Newport News network, which used the Morehouse two-tape variant
- It also spoke of encryption per “the method of the Signal Corps”—but a number of other documents use that phrase to refer to the keying and indicator schemes for the Morehouse system
- There are no claims about non-repetition in the Vernam patent; there are such claims in the Morehouse patent
- The 999,000-character key stream is from a Morehouse system with tapes of 999 and 1,000 characters

☞ (Those sample values are in the Morehouse patent. A single tape of that length would be >8000 feet long.)

The Case for Vernam

- Vernam left behind no explicit statement; we have to rely on statements by Parker
- (Parker seems to have appointed himself the protector of Vernam's and AT&T's reputation and priority)
- In 1942, Parker told Friedman that AT&T originally proposed the one-tape system as more secure
- Friedman disagreed with the notion that the security difference was understood; Parker maintained his position
- In a 1967 internal AT&T memo, he insisted that it was obvious that a random, non-repeating key was secure.

Friedman

- Friedman was asked to attack the Vernam and Morehouse machines
- At the time, he worked for neither the Army nor AT&T
- (He was later lured to Washington by Mauborgne, and much later became friends with Parker)
- His is the nearest we have to an unbiased opinion

Friedmans's View

- In 1943, Friedman did not dispute Parker's assertion that AT&T invented non-repetition
- In 1966, he wrote "not true" on a *Scientific American* article that gave part-credit to Mauborgne
- In 1967, he demurred from Parker's suggestion that he write the Chairman of the Board of AT&T to give all credit to Vernam—but he demurred soley because NSA wanted to stay out of the question. He apparently agreed with the content of the letter, and suggested sending it later.

Conclusion

Mauborgne did not invent true non-repetition. Rather, he insisted on non-repetition of the *effective keystream*, which he felt was adequately achieved by the Morehouse machine. That was the patent he worked on; that was the system mentioned in the CSO report and which was alluded to in the citation for Mauborgne’s Distinguished Service Medal. Parker was right that Vernam invented non-repetition.

Randomness

- Parker claimed that AT&T understood the need for randomness; for lack of other evidence, Kahn accepted this
- The Vernam patent (page 3, column 1, line 18) says that key characters are “preferably selected at random”.
- A June 7, 1918 descriptive memo that accompanied Gherardi’s “challenge letter” to Fabyan mentioned that the key characters were selected at random
- In other words, the need for randomness was appreciated by AT&T very early—but where did it come from?

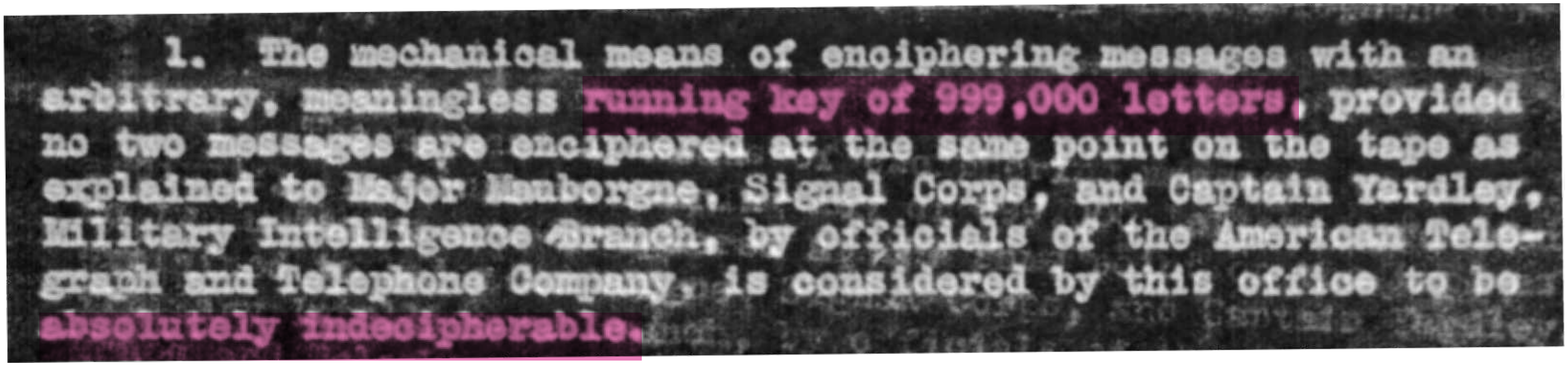
Running Key Ciphers

- In 1917, the US Army used Vigenère ciphers with coherent running keys
- Friedman and Yardley independently solved this cipher; Yardley told Mauborgne in December 1917
- Mauborgne visited AT&T only a few months later, and *before* the Gherardi letter
- Did Mauborgne tell Vernam and Parker?
- I suspect so; the need for randomness was not only non-obvious, it violated Kerckhoff's third principle ("Its key must be communicable and retainable without the help of written notes")
- (Kahn had the same data; I weight it differently.)

Who Understood Non-Repetition's Importance?

- Not AT&T in 1918—the memo with the challenge letter does not distinguish between the security of the one-tape and the two-tape systems. (The memo was likely prepared by Vernam or Parker.)
- Not Yardley in 1918
- Not Mauborgne in late 1919
- Possibly Hitt
- Friedman understood

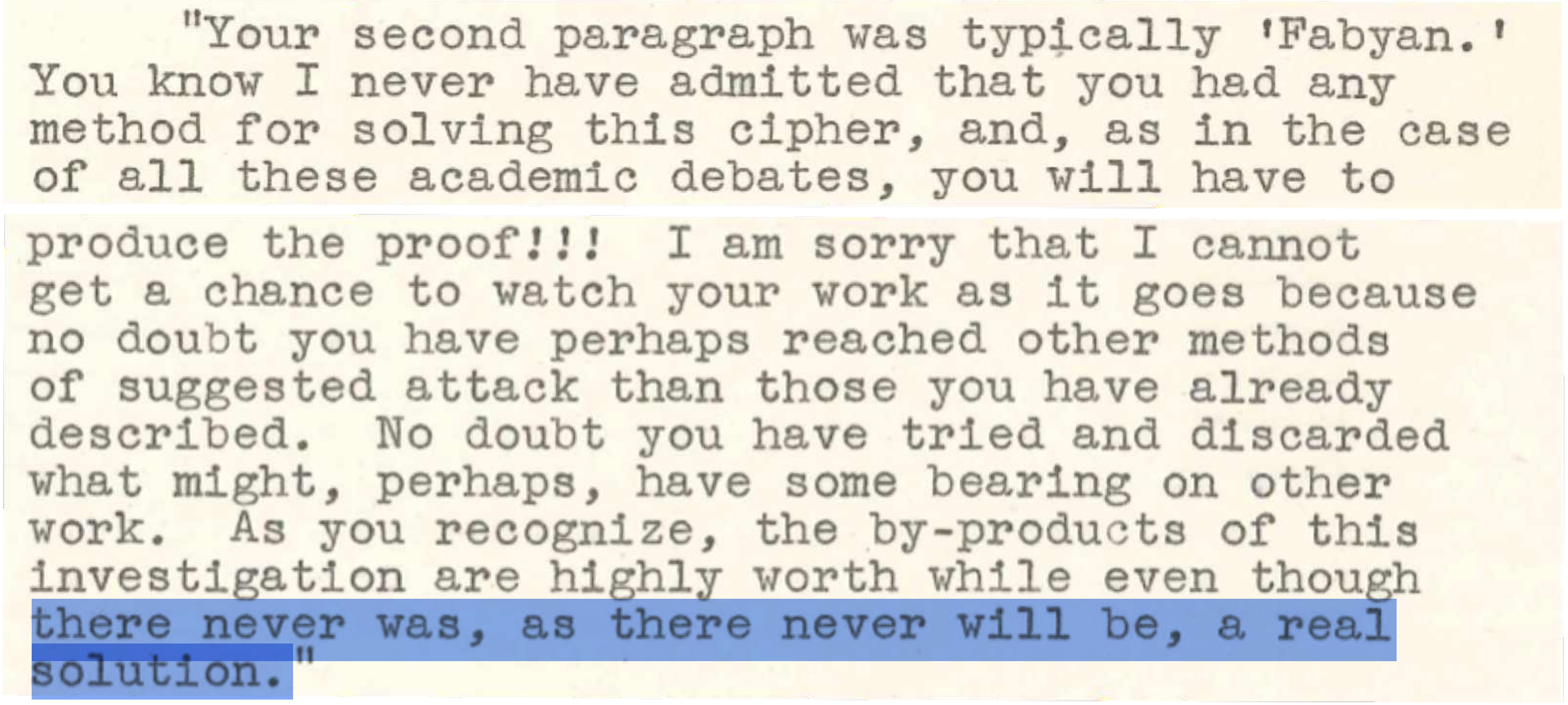
Yardley's View



1. 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.

A memo from Gen. Churchill, Yardley's superior. It speaks of "999,000 letters", showing that the two-tape system is being described.

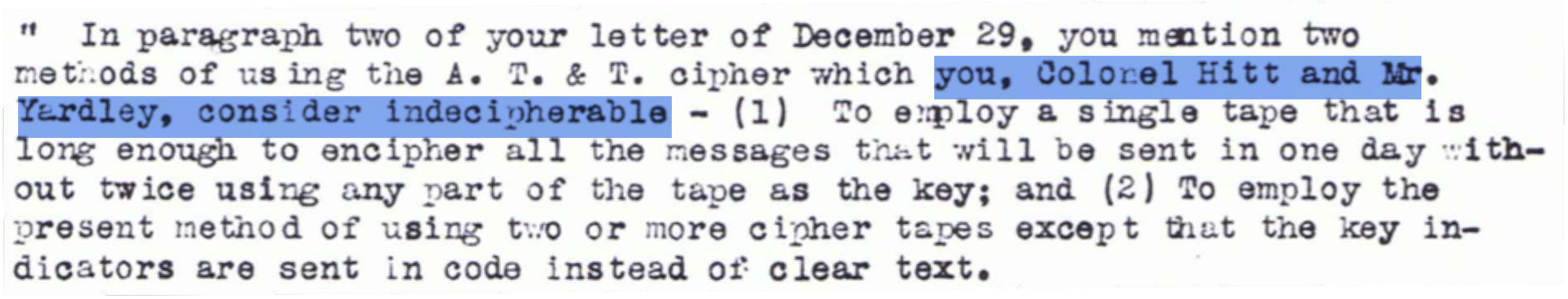
Mauborgne, November 1919



"Your second paragraph was typically 'Fabyan.' You know I never have 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 even though there never was, as there never will be, a real solution."

Ten days later, Friedman had solved it.

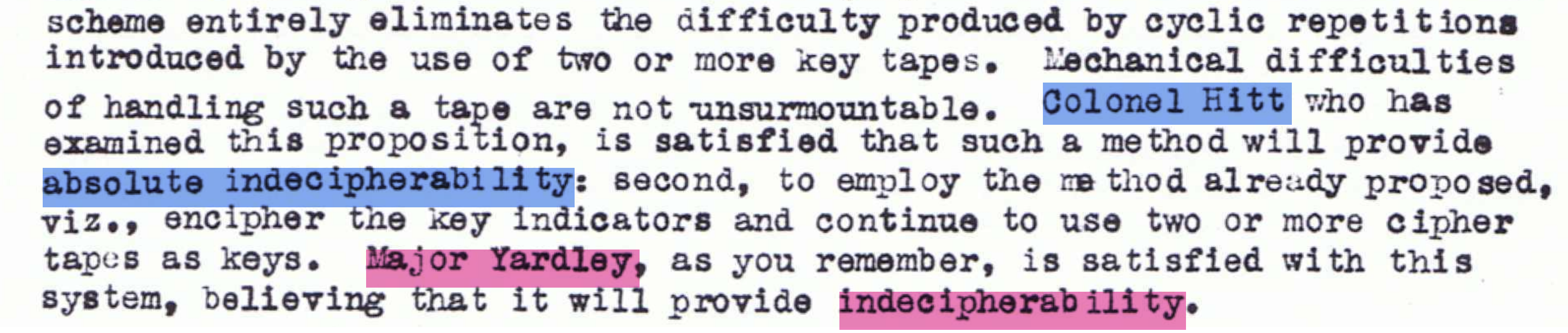
The Army’s View, December 1919



" In paragraph two of your letter of December 29, you mention two methods of using the A. T. & T. cipher which you, Colonel Hitt and Mr. Yardley, consider indecipherable - (1) To employ a single tape that is long enough to encipher all the messages that will be sent in one day without twice using any part of the tape as the key; and (2) To employ the present method of using two or more cipher tapes except that the key indicators are sent in code instead of clear text.

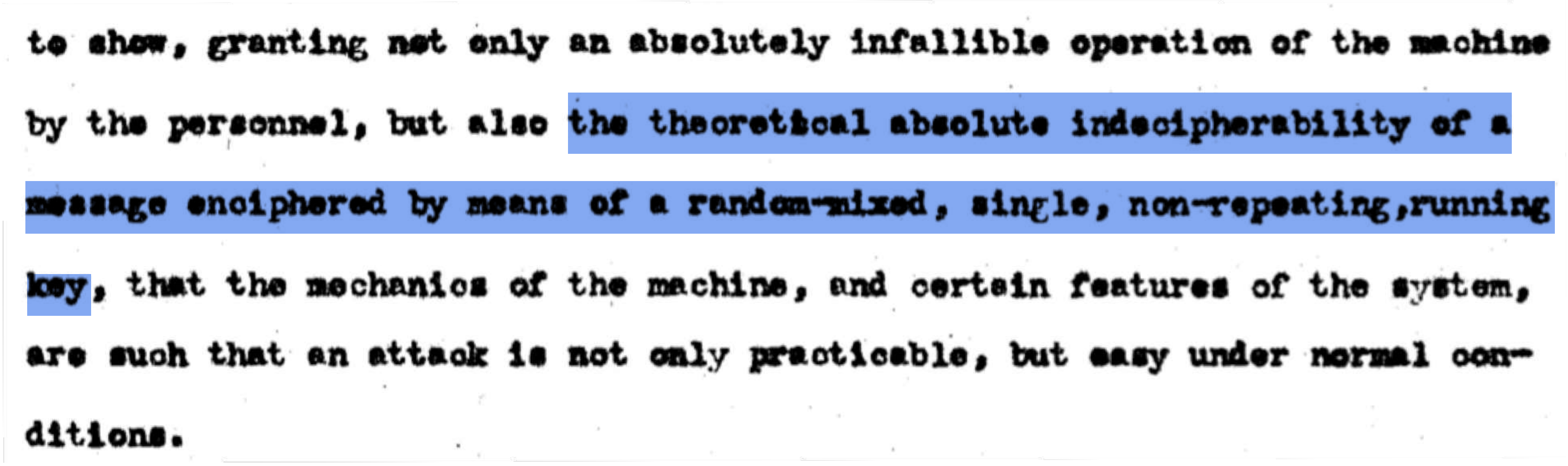
A memo from Churchill to Mauborgne.

Hitt v. Yardley?


scheme entirely eliminates the difficulty produced by cyclic repetitions introduced by the 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, believing that it will provide indecipherability.

Is there a difference between Hitt's "absolute indecipherability" and Yardley's "indecipherability"? Note the reference to the "difficulty produced by cyclic repetition".

Friedman Understood the True One-Time Tape



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 the mechanics of the machine, and certain features of the system, are such that an attack is not only practicable, but easy under normal conditions.

However, he warned of the likelihood of operator errors.

Friedman’s Attack on the Morehouse System

- Friedman used plaintext indicators of tape starting positions to find overlaps of keytape (December 1920)
- He was then able to use probable plaintext and the reciprocity of the cipher square to recover the key tapes
- Yardley produced a codebook plus cipher to encrypt the indicators
- Friedman cryptanalyzed that system, and was able to use his previous attack to recover the key tapes

Strengthening the Attack

- Yardley's encryption scheme was pretty bad, and hence was easily solved
- Did Friedman wonder how to find overlaps if he couldn't read the indicators?

☞ Almost certainly!

- Did this lead to the index of coincidence?

The Index of Coincidence

- The index of coincidence—Friedman's greatest single idea—can show if two sections of ciphertext were encrypted with the same key
- In December 1919, he knew that the next challenge would likely involve encrypted indicators, but that didn't happen until late January at the earliest
- He solved Yardley's indicator encryption in early March, 1920—but he couldn't have known that that would be possible
- He had a 100 page manuscript for his index of coincidence paper by summer 1920
- Timing suggests that he had to have been working on it before March
- It seems highly probable that attacking this system led him to the basic idea

My Conclusions

- Vernam, not Mauborgne, invented true non-repetition
- However, neither he nor Mauborgne really understood its importance, and in particular did not appreciate the difference between a non-repeating key and Morehouse’s two-tape variant with a long effective key stream
- Timing suggests that it was Mauborgne who suggested random keying material to Vernam
- Attacking the Morehouse variant probably led Friedman to invent the index of coincidence

☞ More details in a forthcoming paper

Thanks To. . .

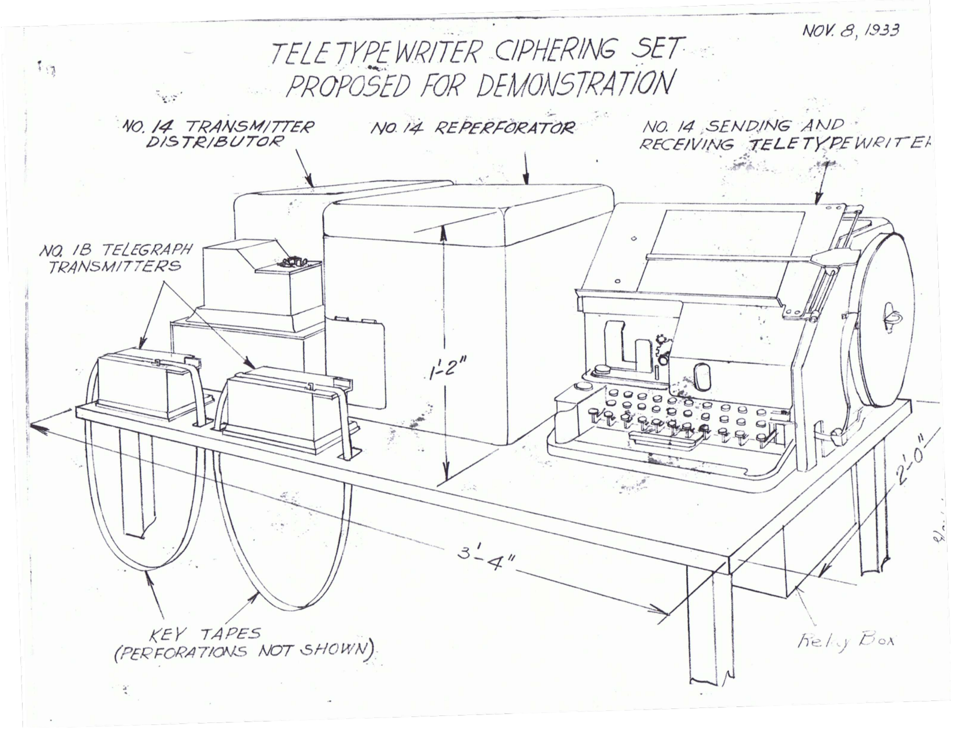

NOV. 8, 1933
TELETYPEWRITER CIPHERING SET
PROPOSED FOR DEMONSTRATION
NO. 14 TRANSMITTER DISTRIBUTOR
NO. 14 REPERFORATOR
NO. 14 SENDING AND RECEIVING TELETYPEWRITER
NO. 1B TELEGRAPH TRANSMITTERS
1'-2"
2'-0"
3'-4"
KEY TAPES (PERFORATIONS NOT SHOWN)
Relay Box

Diagram: AT&T Archives

David Kahn, Paul Barron (George C. Marshall Foundation Library), Bill Cheswick, Kathleen Kain, George Kupczak (AT&T Archivist), David Lesher, Betsy Rohaly Smoot (NSA CCH), Rene Stein (National Cryptologic Museum library).