Dabbling in the Cryptographic World--A Story

This note tells the story of some work that I was involved with, but to which I was not a primary contributor. For reasons that should become clear, the people most involved have not gone public with their results. Still, it is one of the more interesting things I've done and seen. The central events occurred around 1977. Jim Reeds reminds me that the incident was already babbled to John Markoff and recorded in the book by Markoff and Katie Hafner (*Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon and Schuster, 1991). This note doesn't differ materially from that account, but might be a bit more complete.

Background

Bob (Robert H) Morris was an important contributor to early Unix during the 1970s; he did the first and several subsequent versions of the math library, a variety of interesting text-processing applications like typo and other things, and with Thompson was responsible for the password encryption scheme that is still used today, together with its predecessors. (If you can handle Postscript, a 31KB paper describing the history of this password mechanism is available.) He was also the author of the series of crypt programs that came with early Unix, including the final one distributed with the Seventh Edition (the one based on a rotor machine, which was broken by Reeds and Weinberger). Because Bob privately referred to his crypt commands as a sequence of graded exercises, it's evident that he liked both making ciphers and breaking them.

At some point, I suppose around 1970, Bob acquired one of the Hagelin cipher machines usually referred to by its US Army Signal Corps designation M-209 (in other versions also known as CSP-1500 and C-38); they have a history of use that dates from the 1930s at least through the 1950s. Kahn's *The Codebreakers* has a good account and pictures. On the web, there is a page describing it from the National Maritime Museum, including pictures and the operations instruction manual. The accounts I've seen of the particular machine (and the versions closely related to it) describe it as a low-level "field cipher" and not one used for strategically or politically interesting material.

Bob's story of how he obtained the machine is interesting to hear, but not particularly mysterious (he haunted the small strange junk stores in lower Manhattan).

One of the crypt commands in early Unix (Sixth Edition, 1974) was based on an exact implementation of this machine; a variant on it, with different parameters, served as our password-encryption scheme before the current one.

On the cryptanalysis side, Bob had already crafted a hand-computed approach to recovering the key settings of the machine given ciphertext and known plaintext. His approach required about 75 characters of corresponding text. He wrote an internal memo on his approach; I understand that it was published in *Cryptologia* in July, 1978.

Over the same years (say 1969-76) Jim Reeds was, unknown to us, working sporadically but creatively on a new and quite different approach to a ciphertext-only attack on the M-209. It was statistical in nature, and described mathematically. Jim recalls that he had worked on the method since he was an undergraduate and had done some computer testing even by 1969-70. He wrote an extensive manuscript on the machine, mostly while he was at Harvard around 1971-73; he retains his notes from the whole period.

Evidently both Reeds and Morris communicated their separate work to a central collector of amateur M-209 and other crypto work: Louis Kruh. Both Reeds and Morris understand, especially in retrospect, that their work had some wider private circulation.

The Events

At some point, Morris, through contact with Kruh, obtained Reeds's manuscript. Around this time (say 1975) I became involved. I had seen and helped a bit with the editing of Bob's internal version of the M-209 key-recovery paper, but had nothing to do with his technical work. By then I had a chance to admire and play a bit with the actual machine, which is a mechanical wonder. (Unlike the Enigma machine, which I've also had a chance to play with, one has the sense that it really continues to work in the mud of the field.) I borrowed it a couple of times just to admire the construction. When Reeds's work arrived, Bob showed it to me, and I wrote a program to carry out the attack Reeds described.

The attack needs two parts: Reeds's new idea, the statistical part, finds the pins on the wheels of the machine. The second part finds the lugs on the bars of the cage. This task is more combinatorial than statistical, and the ideas in this part, as well as some of the program, owe much to Morris as well as to Reeds.

I also wrote most of the text of a paper describing the whole method. It followed Reeds's math slavishly but tried to condense the presentation and also exhibited some results.

The program was able to perform a readable decryption of English-language but otherwise arbitrary messages on about half of the texts longer than 2000 characters, and most of those above 2500 characters. It used no *a priori* knowledge except for a letter frequency table for English and a preference for at most two lugs per bar on the cage. There is no use of guessed plaintext. Any real use in practice would surely take advantage of guessable "cribs" and incorporate feedback/retry from partial solutions, but the intent was just to see what could be done by taking ordinary English, handing it to the M-209 (keyed according to usual standards), and letting the program munch on the resulting ciphertext.

At some point during the work, Bob telephoned Jim; later Jim, by then in Philadelphia, visited us at the Labs (probably autumn 1976). My own memory of the sequence of events is uncertain, but Jim recalls that by his visit the program was demonstrable, and he was

impressed by it; Bob and I were equally happy to meet the creator of this neat idea.

Once the paper was written, the question arose: what next? It was submitted to *Cryptologia*, and also, by agreement among the contributors, it was sent to NSA. We asked the agency: should we publish this, or would you rather that we not? I can't recall the exact timing here, but the internal version of the paper is dated July, 1978. At any rate this was before NSA established a formal (though voluntary) mechanism for checking out papers.

The result of the NSA query was that Bob and I--the arrangements were made by him--received a visit from a man whom Bob called "a retired gentleman from Virginia." He was quite a charmer. What he said, over lunch, was: there was no statutory reason why the paper should not be published. It was true that there were some who thought that crypto methodology should be "born classified" as some atomic energy research is, but it was not. (Bills to this effect were later proposed in Congress but never passed).

Furthermore, the RG said, there were many in the agency who thought that publishing such papers was inevitable and harmless; he himself held this view. There were also some who believed that this kind of publication might cause them real problems. He recalled the good old days when public and academic interest in cryptography was confined to newspaper puzzles. He got a bit more specific about two things: the agency didn't particularly care about the M-209. What they did care about was that the method that Reeds had discovered was applicable to systems that were in current use by particular governments, and that even though it was hard to imagine that these people would find the paper and relate it to their own operations (which used commercially-available crypto machines), still... perhaps we should exercise discretion? It was certainly legal to publish, but publication might cause difficulties for some people in the agency.

From what he said I was able to form an opinion about what countries he was talking about. As I said, he was a charmer, and he never talked about difficulties for us. No explicit threat.

The other specific thing he mentioned (since Morris had also been playing with Enigma and other rotor machines) was that NSA didn't particularly care about these and wouldn't object if we published papers about cryptanalysis of them. And indeed, I can't recall hearing of difficulty about getting a release for the Reeds and Weinberger paper about Unix crypt ("File Security and the UNIX System Crypt Command", AT&T BLTJ **63** #8 part 2, Oct 1984; 110KB Postscript version available). By the time of this paper, Reeds had left UC Berkeley and joined Bell Labs.

And of course there was one final part of that day's and subsequent discussion. The Retired Gentleman said that our results were pretty good, but (though he didn't say it quite this way) theirs were better. Would anyone like to consider entering into a consulting contract? Once you've gotten clearance, you can learn about the true state of the art (again this wasn't said in quite this bald way). In talking about the meeting afterwards, Bob described this approach as "he's bringing out the Dancing Girls" and observed that making such an arrangement implied a serious commitment about the course of one's future work.

It was Bob who pursued things further by talking both to higher Bell Labs management and higher people in the agency. (Indeed, some of the details described above might conflate what we heard over lunch and what was learned in the subsequent discussions). At any rate, what was learned from the discussions was that

- Bell Labs management strongly supported open publication of research results and would resist artificial constraints on our research, but cautioned that the national interest, as communicated in consultation with NSA, was important as well.
- NSA cautioned that some in the agency believed that the national interest could be affected by this particular work, though this faction did not necessarily reflect the consensus advice of the agency. They too supported open publication of independent research results. Nevertheless, they were not ready to write a letter advising either for or against publication.

In other words, the signals, even from those qualified to give them, were utterly ambivalent in any terms that anyone was willing to write or even say. They were also unmistakable.

In the event, the paper was "postponed" from publication in *Cryptologia*. The decision was reached by mutual agreement among the authors. No promises were made by any of the parties, nor explicit advice received. And, years after, none of us regret this choice.

I regarded the entire effort then as an amusing bit of work and as an instructive interchange (a peek behind a curtain) not strongly related to my professional career. I still do.

Morris seemed at the time to regard it much as I did, but as things worked out both the technical work and the connections he made were doubtless important to his subsequent career.

Reeds, by then an assistant professor of statistics at UCB, and also the one who had the idea that NSA regarded as possibly undesirable to propagate, was just at the time most centrally on the hook. If he didn't publish it, how would it help him professionally? Still, the paper was read by at least one well-regarded mathematician, who pronounced his work worthy in a letter to UCB.

The Outcome

Letter notwithstanding, Reeds left Berkeley and came to Bell Labs for a long stay, and then joined AT&T Research Labs. Most lately, he has moved to IDA. He has, by now, a strong professional career that includes a broad publication record, providing sage advice about crypto issues to AT&T, and also what one might call advanced amateur cryptography. Neither Bell Labs nor AT&T Research Labs actually paid him just to work on the Voynich Manuscript or Trithemius, but his various employers have been very happy to have him on staff.

Morris, like Reeds, was quite alert about the deal that NSA was offering and also about the forces that might be brought into play in

spite of the studied ambivalence of both NSA and Bell Labs management. I suspect we all had the feeling that we'd shaken a velvet-gloved hand on friendly terms and sensed that there was steel underneath.

Of course, as it later turned out, Bob became chief scientist at NCSC, where he presumably learned all the secrets. And not too long ago, about the time he retired, I asked Bob whether the paper's publication would still not be advised. He said that it would indeed still not be advised.

And I didn't do anything substantive thereafter in the area. But it was certainly an enlightening and memorable encounter.

I think we could just have gone ahead and published the paper without getting into bad trouble.

Still, I have the feeling that all of us are, on balance, more than content to have a suppressed paper to slip into the bibliography.

Thus the current citation for it is
J. Reeds, D. Ritchie, R. Morris, "The Hagelin Cipher Machine (M-209): Cryptanalysis from Ciphertext Alone", unpublished technical memorandum, Bell Laboratories, 1978. Submitted to *Cryptologia.*

> *This note represents my own recollection of an encounter. It was read by both Reeds and Morris, who both helped correct my failing memory about dates and names. They each have their own version of the story, and have sent a lot more details that I've chosen to skip. Thanks to their attention, this version is not wildly discordant with a consensus account. Many thanks to both for checking it, and more importantly for the experience itself.*
>
> *--Dennis*

Final note: so far as I know the main published work on the M-209 is the monograph by Wayne Barker, *Cryptanalysis of the Hagelin Cryptograph*, Aegean Park Press, document C-17, 1977. It appears to be currently available from there, but I bought my copy on the used-book market.

Interestingly, Barker's publication was nearly contemporaneous with the RRM manuscript.

Barker probably had access to Reeds's notes, but he missed their main point. Barker's monograph includes three appendices containing material evidently not by him, although he fails to supply any attribution.

Appendix I is touchingly naive: it spends several pages telling how even a very fast computer (a "giant brain") must take a very long time to exhaustively search all the possible settings. Reeds observes that Appendix I is almost certainly a retyping of Hagelin advertising material; he points to the end of paragraph 2, which says "... of course assumed that our machine type C-52 is used in accordance with our advice as contained in our brochure 3153". Reeds also suspects that its ultimate origin owes to Yves Gyldén; see Kahn's book for references to Gyldén's sanguine view of the security of such machines.

It appears that Appendix II, which is entitled "Operating Instructions," is probably a reprint of some edition of the (US) War Department Technical Manual TM 11-380; it resembles a version of which Reeds has a copy. Its content remains interesting for its description of actual use of the machine (recovery from garbles, security and keying procedures).

Appendix III is clearly a direct reproduction of material from Crypto AG in Zug, Switzerland, including its logo boasting "Hagelin-Cryptos". It is about the CD-57 machine, which differs from the M-209, though it operates on the same underlying principles, but with more wheels, more pins per wheel, and hand-carried--sort of the Palm Pilot version.

Slightly updated 5 May 2000