Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

HOW STATISTICS LED THE GERMANS TO BELIEVE ENIGMA SECURE AND WHY THEY WERE WRONG: NEGLECTING THE PRACTICAL MATHEMATICS OF CIPHER MACHINES

R. A. Ratcliff [a]

[a] 1046 Eden Bower Lane, Redwood City CA 94061 USA. cliffrat@hotmail.com

Available online: 04 Jun 2010

To cite this article: R. A. Ratcliff (2003): HOW STATISTICS LED THE GERMANS TO BELIEVE ENIGMA SECURE AND WHY THEY WERE WRONG: NEGLECTING THE PRACTICAL MATHEMATICS OF CIPHER MACHINES, Cryptologia, 27:2, 119-131

To link to this article: http://dx.doi.org/10.1080/0161-110391891801

HOW STATISTICS LED THE GERMANS TO BELIEVE ENIGMA SECURE AND WHY THEY WERE WRONG: NEGLECTING THE PRACTICAL MATHEMATICS OF CIPHER MACHINES

R. A. Ratcliff

ADDRESS: 1046 Eden Bower Lane, Redwood City CA 94061 USA. cliffrat@hotmail.com.

ABSTRACT: Only in 1974 did German intelligence and cryptologists admit that the Enigma cipher machine was not, and had not been, a secure system. Throughout World War II, German experts relied on a theoretical statistical security that took neither wartime operational reality nor their opponents' years of attention and attack into account. They ignored the far more important operational weaknesses and human errors that actually provided enemy cryptanalysts with their most valuable entries into the cipher system.

KEYWORDS: World War II, Enigma, Ultra, signal intelligence, signal security, operational security, stastistics, German military intelligence, *Wehrmacht*, machine ciphers, cryptanalysis, cribs, key repeats, re-encodements.

> "[W]e believe that the enigma cannot be solved... Enigma when used according to instructions is unbreakable. It might be broken if a vast Hollerith [punch card machine] complex is used but this is only slightly possible."
>
> Dr. Erich Hüttenhain, cryptologist, Cipher Bureau of the German High Command (Chi/OKW), in post-war interrogations.[1]

German intelligence officers ended World War II certain of one thing: Enigma machine ciphers had kept their communications secure. After the war, Allied officers interrogated German cipher machine operators, cipher experts and military officers in countless conversations and written homework. Over and over German intelligence officers and cryptologic experts repeated their confidence in

[1]National Archives and Record Agency: Record Group 457 Historic Cryptographic Collection Box 1006 NR 3142 - Statements by POWs re: Work on American and British Systems, p. 5.

the Enigma machine's security. They had, after all, conducted numerous investigations of their cipher systems' security. A quarter century later, Heinz Bonatz, wartime head of the *Kreigsmarine* [German navy] intelligence division, wrote

> ... the Enigma Cipher Machine M was secure against break-in and the German naval radio signals could not be read.[2]

Then in 1974, F. W. Winterbotham's book, *The Ultra Secret*, revealed that the Allies had read Enigma ciphers throughout the war. Bonatz and other intelligence officers had to admit, finally, that Enigma was not, and had not been, a secure system. In the rush of works that followed, the Germans learned that Enigma had been compromised almost from its adoption by the *Heer* [Army] in 1928 - the Polish mathematician Marian Rejewski had made the first break into the machine in 1932.

Gradually a remarkable - and now familiar - story emerged, revealing the Allied development and use of intelligence based on decrypts of Enigma material. The success of this Allied decryption effort raises questions about German intelligence and security. Why did the Germans believe Enigma secure? Why did they not realize - through the course of the war and in the following decades - that their entire system had been compromised and inadequate?

In fact, the Enigma machine itself was neither inadequate nor insecure. Used correctly and judiciously, an Enigma will challenge even today's computers. Allied cryptanalysts themselves said during the war "that the Enigma machine, if properly handled, is unbreakable by any known methods."[3] The Germans were right - in theory.

The theoretical mathematical possibilities[4] made the cryptologic system formidable indeed, although the physical development of Enigma created many restrictive mechanical elements that reduced the actual number of possible permutations. Even this mechanical hardwiring did not prove the undoing of the Enigma machine's security. In the end, Enigma succumbed because of the humans who operated the machine.

Enigma's Theoretical Strength

Enigma's strength comes in part from the "astounding number" of possible encipherments for each letter. The three-rotor Enigma used by the *Heer* [Army] and

[2]Captain Heinz Bonatz, *Die Deutsche Marine Funkaufklärung* (Darmstadt: Wehr & Wissen, 1970), 86-87.

[3]NARA: RG 457 HCC Box 880 NR 2612 - Captain Walter J. Fried Reports, Hut 6 weekly report 14 October 44, p. 2, quoting British cryptanalyst Stuart Milner-Barry.

[4]For the following mathematical formulae, I, a nonmathematician, am indebted to Ray Miller of the NSA and his pamphlet, "The Cryptographic Mathematics of Enigma" (Fort Meade, MD: NSA, n.d.).

Luftwaffe [Air Force] theoretically had approximately 3×10^{114} possible configurations for each day's setting. Mathematicians derived this number for possible settings from the Enigma's five primary variables. The variables include the rotors' internal wiring, their *Ringstellungen* (ring settings), their initial positions, the *Steckerboard* (or plugboard) and the reflector rotor. The equations for each of these variables can be found in the National Security Agency pamphlet on Enigma.[5] Even today 3×10^{114} is an unbelievable number, a number beyond comprehension. For comparison, some scientists estimate that there are only about 10^{80} atoms in the entire observable universe. Such a truly astronomical number lends credence to the confidence that German cryptographers had in their machine.[6]

THE ENIGMA REALITY

Theory, however, rarely translates directly to practice. As with other cipher machines (notably the Japanese "Purple"), or indeed any crypto-system, practical use limited the theoretical security of the original design.

Enigma's physical manifestation lowered the theoretical numbers primarily in two ways: by the hardwiring of some possibilities into the machine and by operational limits.

The Hardwiring Limitations

The three-rotor Enigma originally had only three rotors, but by the time the war began it had five to choose from. This hardwiring of the rotors and limiting of the number of rotors available dramatically reduced the number of possible wirings.

In fact the Poles had reconstructed the wiring of the original three rotors shortly after their first break into the machine, and eventually the Allies learned the wiring of all the later rotors. Since they knew the wirings of all five existing rotors for the basic machine, the Allies and their equipment did not have to search for each one of the 26! possible wirings for each rotor. They had only to consider five possible rotors.

Moreover, since each Enigma came with a single set of five rotors (numbered I through V), the operator could use only one of each rotor at a time (eliminating settings such as "II II II"). So the Allies had only to check which three of the five possible rotors were being used, and in which order. $(5 \times 4 \times 3 = 60)$. (Note that when the Polish team tackled Enigma between 1930 and 1932, the machine

[5]See Miller, passim, and also the description of and the calculations for such substitution alphabets in David Kahn's *The Codebreakers* (New York: Scribner, 1996), 136ff, 145.

[6]Miller, 11.

had only 3 rotors, which meant only ($3 \times 2 \times 1 = 6$) possible positions for the three rotors.) Nor could either the rotors or their notches be reversed. They fit into the machine in one direction only.

In addition to these five interchangeable rotors, all Enigmas had the *Umkehrwalze* [reflector rotor]. Although the *Umkehrwalze* could be removed from the machine and replaced as the other rotors were, in practice most machines held the same rotor all the time. The number of these rotors remained very small through the war. Only the pluggable *Umkehrwalze*, nicknamed *Umkehrwalze* Dora or Uncle D, began to exploit the full potential of reflector rotors. Uncle D could literally be re-plugged on the spot. It could have had the effect of creating multiple reflector rotors and so increased the machine's possible combinations well over 100 million-fold.[7]

The "pluggable" reflector rotor terrified the Allied cryptanalysts working against Enigma at Bletchley Park. It appeared in *Heer* and *Luftwaffe* Enigma nets late in the war. However, the military commands did not introduce the new rotor uniformly. Several units did not receive the rotor on time, so virtually identical messages went out in both the Uncle D and the regular settings, allowing Bletchley Park to figure out methods for reconstructing Uncle D's changing wiring. Eventually enough Enigma operators had difficulty with the pluggable rotors that the military virtually halted its adoption of the new versatile reflector.

Enigma had one more flaw in the design of its rotors, which does not play a role in these statistical figures, but nonetheless made the machine easier to break: the regular stepping of all the rotors. Enigma's rotors all had a metric or quasi-metric stepping - i.e. they stepped in one direction, one step at a time, the way an automobile odometer does. Enigma rotors only moved forward, they did not move backward. This regularity assisted the Allies when they turned to regular reading of German messages. Once in possession of the setting for one section, a cryptanalyst had only to count the letters and he knew the rotors had moved that same number of steps. This highly regular progression meant that a break into any one part of a message almost inevitably led the cryptanalyst to a successful reading of the entire message.

Multiple notches in a rotor, however, did change the pattern of the next rotor to the left. With the extra notches, the slower rotors moved more frequently than every 26 clicks of the fast rotor. However, these extra notches would not turn out to be much of an advantage because of another idiosyncrasy of the physical implementation. The actual Enigma turns out to have had a limitation that cryptologists would not have calculated. After 26 rotations of the second or medium rotor, all the rotors were lined up to rotate over on the next letter - the

[7]Miller, 10-11, 15.

notch on the first rotor to turn the second, the notch on the second (middle) rotor to turn the third. On the next letter all three rotors rotated together, a movement nicknamed "lobster" by the British.[8] With this triple rollover, however, the fast rotor did a two-step, moving two positions instead of one. Cryptanalysts nicknamed this two-step the "Click process".

This double progression of the fast rotor reduces the rotors' period by one rotation, from the theoretical number of 17,576 to 16,900. When the *Heer* and *Luftwaffe* introduced double notched rotors, the click process occurred more frequently. In the worst-case scenario - both fast and medium rotors having two notches - the period for the rotors to return to their initial setting dropped to 16,224.

Finally, Enigma included an anomaly that completely undermined the goal of randomness in encipherment: no letter could ever be enciphered as itself. Originally the Germans had included this impossibility of self-encipherment to simplify the machine's reciprocity; that is, its ability to turn enciphered messages back into plain text. However, this restriction opened the door to standard codebreaking techniques. Once the Allies learned that self-encipherment could be ruled out, they realized that wherever 'e' appeared in a signal, the plain text would *not* contain an 'e'.[9] This detail allowed the Allies to use letter frequency rules in reverse and exploit mechanical means of eliminating possible rotor settings that produced self-encipherment for any one letter. Once again the restrictions of the physical Enigma had produced unintended openings for its compromise.

These hardwiring and mechanical limitations of the physical machine reduced the theoretical security of Enigma somewhat. Yet these realities did not prove the ultimate downfall of the machine. The numbers of possible combinations remained daunting in the precomputer age and the Germans were content with numbers far smaller than the 3×10^{114} theory. Although the limitations of the physical Enigma - particularly the earliest machines - did assist the Poles and the British in their successful attack, they did not ensure Enigma's compromise. Far more limiting than the physical factors was the way in which the Germans operated Enigma. In the end, the weakness of Enigma came not from the machine's limitations, but from its operation.

[8]See David Kahn's description of the 'crab' and the 'lobster', *Seizing the Enigma* (Boston: Houghton Mifflin, 1991), 112.

[9]See one story of how this characteristic led to a complete reconstruction of an Italian Enigma key. Kahn, *Seizing the Enigma*, 139.

The Operational Limitations[10]

The types of limitation that German operating procedures created varied. Several of the restrictions simply made the lives of Bletchley Park's cryptanalysts slightly easier, whereas others doomed the security of the machine completely. For example, the restrictions placed on the *Steckerboard* diminished its complication. First, as the calculations show, the *Steckers* substituted letters only in pairs. Secondly, the Enigma variations did not use *Stecker* pairs randomly, but according to precise rules. In the *Heer*, the cryptologic staff's theoretical examination of the Enigma determined that 10 pairings of *Steckers* produced the optimal number of variations.[11] So 10 and only 10, neither more nor fewer, were used every day. (Here, in fact, the Germans made an additional mistake. The number of *Stecker* pairings that created the greatest number of variations was not 10, but 11. With 11 pairs of *Steckers*, the number of combinations rose to 205,552,193,096,250, whereas 10 pairs created 150,738,274,937,250.[12])

Many nets took the additional step of eliminating any *Stecker* combinations that connected sequential letters, such as a *Stecker* linking a to b or x to y. The Allies took advantage of this rule and created the CSKO - Consecutive *Stecker* Knock Out jack - which ruled out any Enigma setting that included *Steckers* in consecutive letters.[13] Thus the formidable *Steckerboard* lost some of its complexity and the number of *Stecker* combinations fell to one-third of the possible theoretical combinations.

In its operational form, the reflector rotor completely lost its potential. German nets, with few exceptions, used only one reflector rotor, so it became a constant, rather than an additional daily variable, for Allied cryptanalysts. Since the Allies knew the wiring of the reflector rotor by 1940, its contribution to Enigma's overall equation reduces to 1.

With these operational restrictions, the number of possible configurations for the three-rotor Enigma machine decreased significantly. By restricting the *Stecker* pairings, not changing reflector rotors, and creating only a very limited number of rotors, the Germans eased the enemy cryptanalyst's task. In particular, once the Allies reconstructed the rotor wirings, the number of possible combinations became far less formidable.

[10]For many of the following points I am indebted to conversations with Steve Kelly and Steve Budiansky. See Stephen J. Kelly, *Big Machines* (Laguna Hills, CA: Aegean Park Press, 2001).

[11]NARA: RG 457 HCC Box 1407 NR 4541 - Codes and Ciphers: Germany German Cryptanalytic Documents - "*Aktennotiz 6 zum Chiffrierverfahren mit der Enigmamaschine.*" 30 July 1940, p. 4; and Ibid., "*Aktennotiz 5 . . .*" passim.

[12]See the calculations in Miller, 9.

[13]NARA: RG 457 HCC Box 1283 NR 3814 - Decoding German Enigma Machine Messages, p. 34.

Possible wiring of the rotors (known to the Allies, so simply the choice and position of 3 of 5 rotors) (when naval operators could choose from 8 rotors, this number grew to 366)	60
Possible settings for the *Ringstellungen* (again, with a possible 3 of 8 rotors, the number rose to 476,976)	676
Possible initial positions for the rotors	17,576
Steckerboard possibilities	150,738,274,937,250
Reflector wiring possibility (known and generally unchanging)	1
The product of these numbers is:	1×10^{23}

Enigma 3-Rotor Reality

Although by no means the astronomical number of the theoretical version, this number meant the Allies were still faced with a daunting prospect.[14] Indeed, the Germans would still have considered 1×10^{23} a formidable wall against cryptanalytic attack.

Before the war, cryptanalysis had little in the way of mechanization and most of the German mechanization consisted of punch card cataloguing and sorting. Under these circumstances, even the reduced number of Enigma permutations seemed close enough to infinity in those pre-digital computer days. Even with IBM or Hollerith machine sorting capabilities, sifting through raw messages looking for repeats among these numbers of possibilities would have taken an enormous amount of time. Had the Allies been forced to try all of these possible combinations every day, they would have rarely, if ever, read any Enigma messages in time to influence the war. The Germans were correct in their belief that the hardwired version of the Enigma could stymie a cryptanalyst using the latest in punch card and similar mechanical sorting assistance.

They failed, however, to consider electromechanical capabilities. Although their own Enigma encryption system used electromechanics, they did not apply the same level of technology to cryptanalysis. They did not actively investigate how machines could be used in cryptanalysis beyond statistical counting and sorting. In particular, they apparently never considered using Enigma against itself. Yet the Polish mathematicians did so, successfully, in the early 1930s. German experts found mechanized solving only a remote possibility, "even though the fancy of some analysts had been occupied with this idea."[15] In a formerly

[14]Miller, 13.

[15]NSA Museum collection: DF 187A (*Wehrmacht* cryptanalyst chief Wilhelm Fenner), 27.

top secret, post war list comparing Allied and German rapid analytic machinery in cryptanalysis, numerous Allied machines have no German equivalent. German cryptologists imbued their mechanical ciphers with great prowess, yet they did not much consider the potential of mechanical decipherment. They did not expect Enigma to face machines of its own caliber.

The Human Factor

Most important of all, the Germans did not fully reckon with that most vital factor of cryptology: human error. The greatest damage to Enigma's security came from the humans operating the machines, particularly those in the *Heer* and *Luftwaffe*. Lazy cipher clerks and tired, bored or homesick Enigma operators kept producing vulnerabilities for the Allies to break into the daily keys. These entry points arose from three major types of errors: key repeats, re-encipherments (called re-encodements at Bletchley Park), and stereotyped phrases.

Code clerks created key repeats by reusing part or all of a daily key. The basic daily key had four elements: 1) the choice and order of the rotors, 2) the *Ringstellung* or position of the rotor notches, 3) the placement of the *Steckers*, and 4) the discriminants, that is, the letters telling the cipher clerk which net or type of Enigma traffic the message was.[16] Clerks creating a net's monthly books of daily settings often reused one or two of the pieces from another net's codebook. The Allies soon found that patterns in the Enigma key's daily setup traveled from net to net predictably. The month's worth of discriminants and rotor orders from one net would appear the next month in a different net, while the *Ringstellungen* and *Stecker* settings surfaced on a third net. The next month the same pieces of the daily key would be shuffled again and redistributed through the same signal nets, giving the cryptanalysts at Bletchley Park an easier entry into all of the connected nets.

One example (see Figure 1) had pieces traveling through four nets in what the British nicknamed a "quadrilateral."[17]

Portions of the Primrose net's monthly setting would appear the next month in each of the other three nets. The third month each piece would move to yet

[16]Each cipher key connected a specific group of planes, U-boats, or units in a network. Each network had two names, one German and one British; thus the U-boat key in the North Atlantic was known as 'Triton' to the Germans and 'Shark' to Bletchley Park. [see NARA: Microcopy T-1022 (German Navy records 1850-1945) Roll 2310.]

[17]NARA: RG 457 HCC Box 1126 NR 3620 - E Operations of the GC&CS at Bletchley Park, p. 40. BP grouped code names in categories: main *Luftwaffe* codes were colors (Red, Blue, etc); Weather codes were vegetables, such as Leek, Garlic; *Heer* codes were birds (Sparrow, Falcon), the S. S. fruit (Orange, Quince), and the Baudot ciphers were "Fish" (Tunney and Sturgeon). See one list of names in Box 1009 NR 3175 - Cryptanalytic Report on Yellow Machine, p. 10.

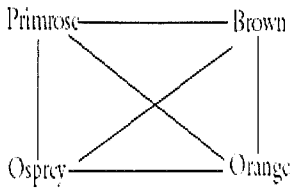

Figure 1. The "quadrilateral" of four nets.

another net in the square. This constant shifting meant that each piece of the daily key would be used four times over four months, so the clerk charged with creating months of daily settings could save himself considerable mental effort.

This quadrilateral of shared key pieces was not unique. In an unrelated *Luftwaffe* arena, Bletchley's cryptanalysts found that a clerk had fallen into a similar habit of repeating pieces of the daily setting among a set of four signal groups (Bletchley had named them Mosquito, Leek, Cockroach and Cabbage). As such repeats rotated, Bletchley cryptanalysts could break into all four networks. Once they recognized a pattern, the cryptanalysts would know at least a portion of the daily key by the time the day's messages began to arrive.

Such key repeats proved blatantly disastrous to Enigma because they reduced or even eliminated the cryptanalytic work that the Allies and their machines did to read a day's messages. If the cryptanalysts at Bletchley Park knew the day's setting, they simply set up their own Enigma machines,[18] and began typing in the cipher text; the machines produced plain text just as they would have for the German cipher clerk intended as the recipient.

Two other major errors - re-encipherments and stereotyped phrases - gave the Allies another way to break into the day's signals: cribs. Cribs occur when a cryptanalyst either knows or can guess the wording of the message's plaintext. With that wording, the cryptanalyst can work backwards to uncover the daily key and - daily key in hand - can begin reading all the other messages sent that day on that same net.

The Allies generally discovered such cribs by following the habits of cipher clerks and their superiors. The re-encipherments occurred when clerks made the serious mistake of repeating the same message virtually verbatim in more than one cipher. As in any military, the Germans needed to send the same information to different sections of its forces. Many clerks found the routine messages tedious and the cryptographic regulations unimportant, so they enciphered them without

[18]The first Enigmas the Allies had were reconstructions built by the Polish team before the war. Later the British modified their own cipher machine, the Typex, to mimic the Enigma. See Wladyslaw Kozaczuk, *Enigma* (Frederick, MD: University Publications of America, Inc., 1984) and Peter Calvocoressi, *Top Secret ULTRA* (New York: Pantheon Books, 1980).

changing the wording significantly. Sometimes they did not paraphrase at all and the message was repeated from one net to the next without a single change except the address. These repeated messages opened a door from the more easily broken net to a more difficult one.

At times the re-encipherment came from unexpected sources. For example, the Germany military espionage division, the Abwehr, produced some useful re-encipherments. A certain Oberinspektor Menzer served as the Abwehr expert in charge of vetting ciphers and security procedures. Concerned about security lapses, he sent word of a procedural upgrade to all the Abwehr stations throughout Europe. From Bletchley's point of view, his message provided the perfect re-encipherment, and as each Enigma operator dutifully repeated Menzer's warning and upgrade from one site to the next, the cryptanalysts pried their way into "several links hitherto unbroken."[19]

Because the Allies recognized operators and stations that frequently practiced these sloppy re-encipherments, they would often break one message, see that it mirrored another message of similar length, assume the plaintext to be the same, and discover a crib. With such a clear series of re-encipherments as those of Oberinspektor Menzer, they could uncover the day's setting for one or more new ciphers and thus break into another net for the day, which might in turn lead to more breaks in the future. Although the Germans periodically issued warnings against reciphering without significant paraphrasing, their threats usually did not leave a lasting impression and the re-encipherments quickly reappeared.

These two errors - key repeats and re-encipherments - often linked different sections of the *Wehrmacht* together in regular patterns. Allied cryptanalysts soon found the many *Heer* keys of the Mediterranean intertwined so tightly that they essentially formed a single cryptologic problem. Once one key succumbed to the day's attack, the rest of the *Heer*'s Mediterranean nets usually followed quickly.[20]

The third major operational error that gave Bletchley Park's cryptanalysts considerable assistance arose from phrases that frequently appeared with precisely the same or very similar wording. These stereotyped phrases would reappear in signals traveling between the same stations on a regular, often a daily, basis. Of course, all military dispatches tend to follow a predictable pattern and the German military proved no exception. Message openings often gave cryptanalysts an excellent starting point, e. g. *An Fliegerfuehrer Afrika Korps*. Many German addresses provided cribs of so many letters that enemy cryptanalysts could break some nets simply on them.

[19]NARA: RG 457 HCC Box 880 NR 2612 - Capt. Walter J. Fried Reports/SSA Liaison with GCCS, p. 4

[20]Public Record Office (Kew, England): HW 14/62 - "Appreciation of the "E" Situation" Dec 42, p. 10.

Other breaks came from daily reports signaled by far flung stations. Reports from some operators became very predictable - to the point where British cryptanalysts wanted certain stations left intact by the advancing Allies as long as possible. The predictable patterns emerged when operators followed standard reporting formats, such as the operator in Czechoslovakia who regularly reported the number of "wine barrels on hand." Sometimes the conditions being reported simply did not vary much and the operators became accustomed to using exactly the same wording every day. An obliging operator in France, for example, always signaled the presence of enemy aircraft, telling his superiors "RAF plane over airport." A polite signaler in Norway began his daily messages with "Good morning," whereas one lone operator in the North African theatre signaled the same situation report every morning, saying "Quiet night."[21] These regular, mundane operational habits provided the British with an end run around Enigma's complex calculations. The familiar patterns of German clerks and signalers did more damage to the cipher system's security than any flaw produced by the hardwiring of the machine.

The Illusion of Statistical Security

One last limitation on the part of the German military made Enigma's vulnerability enduring: the Germans did not take a creative, nonlinear view of attacking security. When reporting on the security of Enigma or even of other ciphers, including enemy systems, they focused on the statistics of cryptology. Their security investigations and cryptanalytic reports examined either the problems of physical compromise or of possible statistical methods for breaking a system. Among the surviving wartime documents, no reports deal with the more subtle ways around and into a cryptologic problem.

The various branches of the German military had cryptanalysts attack their own Enigmas and investigate several Allied cipher machines as well. In these attacks Germany's experts seem to have stuck to statistical and straightforward approaches. They conducted statistical attacks on Enigma-enciphered traffic, both with and without the help of 'captured' documentation. They did recognize many of the statistical limitations in Enigma's design. At least two German cryptologic bureaus found methods to crack the original unsteckered versions of Enigma.[22] However, they apparently never tackled live traffic and instead

[21]NARA: RG 457 HCC Box 1283 NR 3814 - Decoding German Enigma Machine Messages, p. 3.

[22]NARA: RG 457 HCC Box 1405 through Box 1409 NR 4541 - Codes and Ciphers: German Cryptanalytic Documents Folder 3, October, November 1943 on In 7's work; Adolf Paschke. *Das Chiffrier- und Fernmeldewesen im Auswärtigen Amt: Seine Entwicklung und Organisation.* Bonn 1957. Signatur at Auswärtiges Amt: Aktengruppe VS Band 6025 (2 volumes) discusses the Pers Z work pp. 54ff.

stuck to straightforward attacks conducted under artificial conditions. Needless to say, all of these examinations concluded that the machine would defeat enemy cryptanalysts.[23] Throughout these investigations, German cryptologists seem to have never realized the true reduction of Enigma's statistical possibilities under real conditions, particularly those reductions arising from operational procedures and human error.

German cryptanalysts had no luck breaking British and American high-grade cipher machines and this lack of success only reinforced their belief in Enigma's strength and vice versa. The British high-grade cipher machine Typex had a stepped rotor design reminiscent of Enigma's inner workings; but where Enigma had three rotors, the Typex had seven. Since Enigma had proved unbreakable, top German cryptanalysts concluded the more complex seven-rotor Typex would prove even more impervious to attack and hence they did not expend much effort on the assault.[24] Indeed, after a mere six weeks of work on Typex, the *Kreigsmarine*'s cryptanalytic experts abandoned their assault.[25] Faced with a system that they calculated as statistically unbreakable in a reasonable period of time, they simply gave up.

Relying too heavily on theoretical statistics made the Germans vulnerable. Even their cryptologic experts did not believe Enigma compromised until faced with the British government's admission of Ultra in 1974.[26] They knew the British had captured Enigma machines and material, at least by the middle of the war.[27] They knew the British had a history of successful cryptanalysis and they appreciated the ability of British intelligence. Yet they relied on a statistical security that took neither operational reality nor their opponents' years of attention and attack into account. They ignored simple factors which could have hindered, if not completely defeated, their enemies. Had the *Wehrmacht*, for example, completely replaced Enigma's rotors even once, rather than just adding to the existing set, they might have ended the Allies' success.

Both then and now, the problem for the cryptanalyst remains that numbers don't tell the whole story. A cryptologic system's theoretical complexity by

[23] *Bundesarchiv/Militärarchiv*: RM 7/108, pp. 19-21, for example.

[24] Dr. Erich Hüttenhain, chief cryptanalyst at OKW/Chi. NARA: RG 457 HCC Box 1006 NR 3142 - Statements by POWS, p. 5.

[25] *Bundesarchiv/Militärarchiv*: RM7/104 3./Skl, 29 Feb 1941, p. 40.

[26] See for example the presentations given at the conference on Ultra intelligence in Stuttgart and Bad Godesberg in 1978. E. Jäckel and J. Rohwer, *Die Funkaufklärung im Zweiten Weltkreig* (Stuttgart: Motorbuch Verlag, 1978).

[27] They did not know that a German, Hans-Thilo Schmidt, had passed documents on Enigma to the French a decade before the war began. See Gustave Bertrand's account of handling Schmidt in the 1930s in *Enigma ou la plus grande énigme de la guerre 1939-1945* (Paris: Plon, 1973).

no means assures operational security. In the end, cryptologic theory suffers the greatest reduction in security from a single element - humans. Humans gravitate towards regularity, towards habits and patterns that help us make sense of the world. This regularity undermines the randomness that cryptology tries to create. In this case Enigma's security suffered most from officers who did not replace rotors, from code clerks who tired of coming up with something new every month, and from worn out Enigma operators who used easy, repetitive openings and message phrasings.

The Germans did recognize many of these procedural problems and they frequently reprimanded Enigma operators for such insecure habits. In addition, several of the signal intelligence agencies conducted investigations into Enigma security that hinted at the system's general compromise. These theoretical and compartmentalized investigations of Enigma's security did not suffice. Throughout the nearly two decades of Enigma's operation, none of these investigations ever fully examined the machine's operational limitations or even examined live traffic. Only the examination of live traffic under real conditions could have suggested the true level of security for Enigma - or any other system.

In short, the only real security lies in realizing that nothing is truly secure in practice. Whatever the statistical security of a cryptologic system, the practical security will rely on human operations. The most complex computer cryptography collapses when humans fail to practice such basic safeguards as avoiding repetitive phrasing, changing settings frequently and randomly, and, above all, guarding their keys and passwords appropriately. Knowing one's enemy thoroughly - and never underestimating him - offers a cryptanalyst the most valuable information of all. No theoretical element plays as large a role in security as the human.

BIOGRAPHICAL SKETCH

R. A. Ratcliff, a graduate of Bryn Mawr College, has a PhD from UC Berkeley's Rhetoric Department, taught history at the University of San Francisco in San Francisco, California, worked in the high tech industry, and currently freelances in history and communications in Silicon Valley.