100 Years Ago: Joan Clarke

One hundred years ago, in June 1917, Joan Clarke was born in London. Her outstanding mathematical talent led her to become one of the very few women cryptanalysts working at Bletchley Park during World War II. Bletchley was the nerve center of a mammoth operation, carried out in utmost secrecy, to decode German and other enemy military communications. Decades later, as the secrecy surrounding Bletchley Park has lifted, the impact of the work of codebreakers like Clarke has become clear.

Clarke's story echoes that of the women in *Hidden Figures: The American Dream and the Untold Story of the Black Women Mathematicians Who Helped Win the Space Race*, a book by Margot Lee Shetterly that appeared last fall and was also made into a movie. The book recounts the stories of several mathematically talented women who worked as data analysts for NASA from the 1940s to the 1960s. Like the "hidden figures" in Shetterly's book, Clarke has also become better known through a movie, when her character was portrayed by Keira Knightley in the 2014 film *The Imitation Game*.

> *Her equality with the men was never in question, even in those unenlightened days.*

Clarke entered Cambridge University in 1936 and the following year obtained a first in Part I of the university's legendary Mathematics Tripos. It had not been very long since women were even permitted to take the Mathematical Tripos; the first was Charlotte Angas Scott in 1881. In 1939, Clarke received a first in Part II, under the supervision of W. Gordon Welchman, and that same year she earned her BA degree. It was actually called a "title of degree"; Cambridge began awarding full-fledged degrees to women only after the end of World War II.

Clarke started at Bletchley in 1940. By 1942, the number of people working there reached over 7,000, and two-thirds of them were women. They worked in a multitude of roles, as intercept operators, transcribers, typists, encoders, linguists, punched card machine operators, administrators, secretaries—and as codebreakers. A week after joining the staff of Hut 8 at Bletchley, Clarke was moved to a room where she worked directly with Alan Turing and two other cryptanalysts, Tony Kendrick and Peter Twinn. In an essay about her work at Bletchley,

Women working on Enigma ciphers in Hut 6 at Bletchley Park. An Enigma machine is on the table in the foreground. By 1942, 7,000 people worked at Bletchley, two-thirds of them women.

which appeared in the 1993 book *Codebreakers*, Clarke modestly noted that her quick rise from the ranks of "the girls," as the female staff was universally called, "was obviously because of my degree, and before I had had any chance of proving myself."

Clarke earned less than her male counterparts but worked with them as an equal. Her talent, ingenuity, and perseverence earned her great respect among her coworkers. After the war she went to work at Bletchley's successor organization, the Government Communications Headquarters (GCHQ). In his essay "Hut 8 from the Inside," which appeared in *The Bletchley Park Codebreakers* (2011), Rolf Noskwith writes of Clarke: "It was a tribute to her ability that her equality with the men was never in question, even in those unenlightened days."

What follows is a condensed and slightly edited version of an obituary for Clarke that appeared in *IEEE Annals of the History of Computing*, January-March 2001[1]. The obituary was written by Ralph Erskine, I. J. (Jack) Good, and Eric A. Weiss. Erskine is a leading historian of cryptography specializing in the history of World War II cryptography and was co-editor (with Michael Smith) of the *The Bletchley Park Codebreakers*. In 2002, Erskine gave the Gauss Lecture of the Deutsche Mathematiker Vereinigung. Good, who died in 2009, worked as a cryptanalyst at

[1] *The original obituary is copyrighted by the IEEE Computer Society, which has kindly given permission for the Notices to publish the version appearing here. The Notices also thanks Ralph Erskine for his permission.*

Bletchley Park in Hut 8, together with Clarke, and later became a professor of statistics at Virginia Tech. Weiss, who died last year at the age of 99, was a writer, editor, and electrical engineer who served as the biographies editor for *IEEE Annals of the History of Computing*.

— Allyn Jackson

Obituary: Joan Elisabeth Lowther Clarke Murray

Joan Elisabeth Lowther Clarke Murray was born June 24, 1917 in London, England, and died September 4, 1996 in Headington, Oxfordshire, England. She was a cryptanalyst while at the Government Code and Cypher School (GCCS) at Bletchley Park, Buckinghamshire, England, from 1940 to 1945 and worked at the Government Communications Headquarters, England (1945 to 1952 and 1962 to 1977).

Before Bletchley Park

Clarke was the youngest daughter of William Kemp Lowther Clarke (a London clergyman) and Dorothy Elisabeth Clarke. She matriculated to Cambridge University in 1936. She chose Newnham College, half a mile from the university's heart, and not Girton, then Cambridge's only other women's college.

Early in 1940, Gordon Welchman, who joined the GCCS, recruited Clarke to join the codebreakers. Without telling her what the job was, he said that it did not really need mathematics but that mathematicians tended to be good at the job. Cryptanalysis requires imagination and accurate thinking. Some mathematics is often used, especially probability and statistics, but at that time the mathematics needed was usually not very advanced.

She was to start work in June 1940 after she had completed Part III of her studies and was to be paid 2 pounds (then about US$8) a week. Men with her qualifications were getting paid much more.

Summer 1940

On June 17, 1940, the day before France capitulated, and after receiving a "pass" in Part III at Cambridge, Clarke arrived at Bletchley Park. Alan Turing, six years her senior, whom she had previously met as a friend of her older brother Martin, recruited her to work in his Hut 8 instead of with Welchman in Hut

> *Clarke fully held her own in the male-dominated world of codebreaking.*

6. The grounds of the big estate of Bletchley Plark were gradually being covered with hastily constructed, barn-like huts—one-story, non-uniform, and wooden—usually about 18 by 48 feet in size, internally partitioned into rooms of various shapes. A hut number designated a building and also indicated the work being done in it. Hut 8 was attacking the Enigma signals of the German Navy, while Hut 6 was working on those of the German Air Force and Army.

Decoding Enigma-coded Messages

The German military believed that the signal contents were secret since they had been encrypted on the Enigma machines before being transmitted by radio. The electro-mechanical Enigma machine—which had been available in commercial form since 1919—changed each letter in a complex manner depending on a daily changing key. The German military knew that the commercial Enigma could be broken, but believed that the military machine, which had a plugboard (*Stecker* board), was unbreakable in practice. The plugboard interchanged letters in pairs, which added 150 trillion possible settings to a key (for the ten letter pairs that were generally used).

Joan Clarke in 1936.

Even Alastair Denniston (head of GCCS at Bletchley at the time) shared the German belief that the military Enigma was invincible, telling his codebreakers that "all German codes were unbreakable." But the new codebreakers at Bletchley Park, Clarke among them, were determined to prove him wrong by reading German Enigma signals. However, German confidence in the machine was not wholly misplaced. Some Enigma cipher versions, such as Aegir (code-named Pike by Bletchley Park and used by merchant raiders) and TGD (used by the Gestapo), were never broken during the war.

Matched plaintext and Enigma ciphertext for April 23-26, 1940, captured from the German patrol boat *Schiff 26* off the Norwegian coast, had become available in early May and were being used to test a new key-finding aid called the Bombe. Clarke started checking the output of the first Bombe—optimistically named Victory—on the data from *Schiff 26*. The Bombe had entered service on March 18, 1940. The plugboard connections for one day were then apparently found to be already available on a piece of paper from *Schiff 26*, enabling the solution of that day to be completed manually.

More Decoding and Banburismus

Early in July 1940, Turing figured out how to make the Bombes test 26 hypotheses at once, using a process known as "simultaneous scanning," rather than one at a time. He explained his brainstorm to Clarke and discovered that he first had to tell her how electrical relays worked. Later

that summer, when Turing wrote his account of Enigma theory for the use of new recruits to Huts 6 and 8, locally called the "Prof's book," Clarke was the guinea pig who had to read it to test whether it was understandable to lesser mortals.

Hut 8 made little progress against the Naval Enigma until the capture, in February and May 1941, of the keys and special bigram (digraph) substitution tables used to encipher Naval Enigma message keys, which were the starting positions for Enigma's rotors in specific signals. Hut 8 cryptanalysts were therefore sometimes deployed against other versions of Enigma and other cryptographic machines. Following Lieutenant-Colonel John Tiltman's recovery of the plaintext of signals enciphered on the Railway Enigma in July 1940, Clarke helped to find the wiring of its specially wired rotors and worked on breaking traffic using it. Based on the commercial Enigma, the Railway Enigma-cipher—named Rocket by Bletchley Park—lacked a plugboard, making the traffic relatively easy to solve.

In August 1941, following another series of codebook captures, Hut 8 started to use the codebreaking technique called Banburismus that Turing had developed in mid-1940. It had been impossible to employ it earlier, since it depended on Bletchley Park having the bigram tables. Banburismus was a Bayesian sequential procedure for producing and handling a probability network consisting of thousands of weights of evidence. It used paper sheets that were punched with representations of the messages under attack and then moved across each other to find both single-letter and multi-letter repeats of coincident holes to obtain a probabilistic piece of information about the two messages.

Banburismus was invaluable in breaking the main Naval Enigma cipher, *Heimisch*—later called Hydra and code-named Dolphin by Bletchley Park. Without Banburismus, breaking the Naval Enigma would have been greatly slowed down, since Bombes were in short supply until the US Navy's four-rotor Bombes came into service in August 1943.

Clarke was good at Banburismus and was so enthusiastic and enthralled that she would sometimes not hand over her work to the next shift but would stay to see if a few more tests would give a result. One of Clarke's important contributions to the work of Hut 8 accelerated the solution of Naval Enigma *Offizier* signals, which were often extremely difficult to break. Some were never solved, since they were reenciphered with a second set of plugboard settings. Leslie Yoxall devised the first stage of an ingenious statistical method for recovering *Stecker* settings from messages of about two hundred letters or more. It involved a graphical procedure and was called a *dottery*, because the cryptanalyst penciled dots into the cells of a square matrix to represent letter correspondences.

A day or two after Yoxall's invention, Clarke invented a method for greatly speeding up the "routine method," the first stage of the dottery procedure. Clarke's contribution was the second stage of the procedure. It took the *Stecker* of the letter E, as determined in the first stage, assumed that all the plaintext consisted of the letter E, and proceeded with this through a triangular dottery. Her name was not attached to the invention, so the entire *Stecker*-recovery procedure was named Yoxallismus, although Yoxall now disclaims all memory of inventing the second stage.

At the time, Clarke was told that she had merely rediscovered "pure Dillyismus," a reference to the highly talented Dillwyn (Dilly) Knox, a founding member of GCCS and a former member of Room 40, the Royal Navy's highly successful codebreaking unit during World War I.

> *Her work on the Naval Enigma helped to shorten the war and saved many lives on both sides of the conflict.*

Engagement on and off

In the spring of 1941, Alan Turing and Joan Clarke got engaged. He gave her a ring, and they arranged for formal introductions to both families. However, they kept the engagement secret, and Clarke did not wear her ring in the Hut. After taking their holiday together at the end of August, they broke off the engagement by mutual agreement. Turing believed the marriage would be a failure owing to his homosexuality. Clarke and Turing continued to be friends and corresponded during Turing's trip to the United States in the winter of 1942-1943. Clarke said that they had a special friendship, and her warm feelings for Turing lasted throughout her life.

End of the War

The labor-intensive Banburismus attack was discontinued in mid-September 1943 when three-rotor Bombes became more freely available following the entry into service of the US Navy's four-rotor Bombes. By the end of 1943, the US Navy codebreaking unit (Op-20-G) had assumed responsibility for breaking the four-rotor cipher, Triton (Shark to Bletchley Park), that the Atlantic U-boats used. This led to many of the Hut 8 staff being transferred to other work, but Clarke remained in Hut 8 as a highly capable member of a small team that broke Naval Enigma ciphers until the end of the war.

Postwar Period

After the war, Clarke transferred to the successor of both Bletchley Park and GCCS, the Government Communications Headquarters (GCHQ) at Eastcote, where she met a colleague named Lieutenant-Colonel J. (Jock) K.R. Murray, whom she married in 1952. She was appointed a Member of the British Empire in 1947 for her codebreaking work during the war. Because of Murray's poor health, the Murrays moved to Scotland, where they developed a shared interest in Scottish history.

After her retirement, Clarke helped Sir Harry Hinsley on what became Appendix 30 to volume 3, part 2 of the 1988 *British Intelligence in the Second World War*—a substantially revised assessment of the Polish, French, and British contributions to breaking Enigma.

Summary

Clarke was a lady in the tradition of her day. She was congenial but shy, kind, gentle, truthful, nonaggressive, agreeable to all, and always subordinate to the men in her life, except in Hut 8, where she was treated as an equal. Although she recognized and later mentioned some of the impediments and unfairness she met as a woman at Cambridge and Bletchley Park, she never directly confronted them.

She was a highly intelligent person of exceptional gifts. Clarke was fully able to hold her own in the male-dominated world of outstanding British wartime codebreaking—she was one of only three female cryptanalysts who worked on the different Enigma machines. She was an enthusiastic and encouraging colleague who was much admired by all who worked with her at Bletchley Park and GCHQ.

Although the remaining secrecy associated with cryptanalysis still makes it impossible to be more specific about her accomplishments, it is clear that her work on the Naval Enigma helped to shorten the war and saved many lives on both sides of the conflict.

—Ralph Erskine, I.J. (Jack) Good, Eric A. Weiss

Photo Credits

Photo of women working on codebreaking in Bletchley Park are ©Crown. Reproduced by kind permission, Director, GCHQ.

Photo of Joan Clarke reproduced, with permission of the Clarke family, from www.bletchleyparkresearch.co.uk/research-notes/women-codebreakers/.

Celebrating

Women's History Month

Looking Back a Quarter-Century

Twenty-six years ago, the September 1991 issue of the *Notices* carried a special issue devoted to the theme "Women in Mathematics." Below are some of the pieces from that issue:

"In Her Own Words: Six Mathematicians Reflect on Their Lives and Careers" (with contributions by Joan S. Birman, Deborah Haimo, Susan Landau, Bhama Srinivasan, Vera Pless, and Jean E. Taylor)

"The Past, Present, & Future of Academic Women in Math Sciences" by L. Billard

"Top Producers of Women Mathematics Doctorates" by Allyn Jackson

"Mathematics and Women: The Undergraduate School and Pipeline" by D. J. Lewis

"Merging and Emerging Lives: Women in Mathematics" by Claudia Henrion

"The Escher Staircase" by Jenny Harrison

"Mathematics and Women: Perspectives and Progress" by Alice T. Schafer

"A Brief History of the Association for Women in Mathematics: The Presidents' Perspectives" by Lenore Blum [Available on the AWM web site at www.awm-math.org/articles/notices/199107/blum/]