Aerospace, Programming Languages, and Information Technology Co-Development: Wartime Computing and Code-Breaking

Brendan Sechter

2026-07-15

This third article of the twelve-part series covers computing efforts during the Second World War that ran in parallel with the Electronic Numerical Integrator and Computer hereafter ENIAC development treated in A238. Three principal wartime computing programs occupied territory that the preceding article's ballistic-table thread did not reach. The British code-breaking effort at Bletchley Park produced the electromechanical Bombe machines and the electronic Colossus, both purpose-built for cryptanalytic problems. The American cryptanalytic effort operated at similar scale using different technology and against different ciphers. The Manhattan Project at Los Alamos consumed the largest concentration of scientific computing labor of any wartime program, using IBM tabulating machines and human computer teams that later transitioned to electronic computers including the ENIAC in its first substantive use.

The framing established in A237 treats these three programs as instances of the aerospace-computing coupling operating under wartime intensification. Code-breaking supported air operations directly through decrypted target lists, weather forecasts for bombing missions, and submarine locations for anti-submarine air patrols. Manhattan Project computing supported weapons whose delivery vehicles were the heavy bombers of the strategic air campaign. Both programs also produced computing infrastructure, personnel, and engineering practice that transitioned directly to the postwar aerospace and defense computing effort.

The Cryptanalytic Problem

The German military used the Enigma cipher machine as its primary tactical communications cipher from the 1930s through the end of the war. The Enigma consisted of a keyboard, three or four rotor wheels selected from a larger set, a plugboard connecting pairs of letters, and a reflector. Pressing a key sent an electrical signal through the plugboard, through each rotor in sequence, through the reflector, and back through the rotors and plugboard to illuminate a different letter on a lampboard. Each keypress advanced the rotors, so the substitution changed at every character.

The Enigma keyspace for the standard three-rotor Wehrmacht configuration factors into rotor selection and order, starting rotor positions, plugboard configuration, and ring settings. The total number of daily key settings is approximately

$$N_{\text{Enigma}} = P(5,3) \cdot 26^3 \cdot \frac{26!}{6! \cdot 10! \cdot 2^{10}} \approx 60 \cdot 17{,}576 \cdot 1.5 \times 10^{14} \approx 1.6 \times 10^{20}$$

where $P(5,3) = 60$ counts the arrangements of three rotors drawn from a set of five, $26^3 = 17{,}576$ counts the starting positions, and the last factor counts the ways to plug ten pairs of

letters on the twenty-six-position plugboard. This keyspace was large enough to defeat brute-force enumeration by any pre-war computational means. The Enigma design was believed by its German operators to be effectively unbreakable, and the intelligence value of this belief lay in the messages the operators were willing to send under its cover.

The theoretical bound on cipher security was not established until Shannon 1949 published his Communication Theory of Secrecy Systems. Shannon showed that perfect secrecy, meaning that the ciphertext gives an eavesdropper no information about the plaintext, requires

$$H(K) \geq H(P)$$

where $H(K)$ is the Shannon entropy of the key and $H(P)$ is the entropy of the plaintext. For a message of n characters, plaintext entropy per message ranges from approximately $n \cdot 1.5$ bits for natural German text with typical redundancy to approximately $n \cdot \log_2 26 \approx 4.7n$ bits for maximum-entropy content, while Enigma's daily key carries approximately $\log_2(1.6 \times 10^{20}) \approx 67$ bits. Messages of length on the order of tens of characters therefore fall outside the perfect-secrecy regime and are in principle vulnerable to cryptanalysis given sufficient computational effort and known-plaintext exploits. The one-time pad, which does satisfy perfect secrecy by using a key of length equal to the message, was known but was operationally impractical for high-volume military traffic.

Bletchley Park and the Bombes

The initial break of Enigma was accomplished by Polish mathematicians at the Cipher Bureau in Warsaw during the 1930s. Rejewski Zygalski and Różycki used a combination of theoretical analysis, exploitation of German operational procedure that repeated the message key twice at the beginning of each transmission, and an electromechanical device called the Bomba to identify daily rotor settings. Rejewski's own primary account of the mathematical methods used, published in Rejewski 1981 in the IEEE Annals of the History of Computing after several decades of official secrecy in Poland, remains the standard technical source on the Polish work. The Polish work was transferred to the British Government Code and Cypher School in July 1939, weeks before the war began, and became the foundation for the substantially expanded effort at Bletchley Park.

The British Bombe designed by Turing and Gordon Welchman and manufactured by the British Tabulating Machine Company under Harold Keen was an electromechanical machine that tested candidate rotor configurations against a suspected plaintext-ciphertext pair called a "crib" and rejected configurations that produced logical contradictions in the plugboard connections. A single Bombe testing one rotor ordering swept all $26^3 = 17{,}576$ starting positions in approximately 20 minutes, giving a per-machine testing rate of

$$r_{\text{Bombe}} \approx \frac{17{,}576}{20 \cdot 60 \text{ seconds}} \approx 15 \text{ rotor positions per second}$$

with each position implicitly testing consistency against the crib across the roughly 1.5×10^{14} plugboard settings that the logical constraint construction rejected en masse. Bletchley Park operated approximately 200 Bombes by 1943 with the 60 rotor orderings distributed across the machine pool. The aggregate daily throughput of

$$R_{\text{Bletchley}} \approx r_{\text{Bombe}} \cdot N_{\text{Bombes}} \cdot T_{\text{operational seconds}} \approx 15 \cdot 200 \cdot 72{,}000 \approx 2 \times 10^8 \text{ rotor-position tests per day}$$

covered the full rotor keyspace many times over, sufficient to break the daily Enigma keys within hours of intercepting the first messages, per the accounts in Hodges 1983 and in the collected primary documents in Copeland 2004.

The Bombe was electromechanical rather than electronic and used its rotor-emulation mechanism to search the keyspace by physical rotation of dozens of drum sets. The machines were operated by Wrens of the Women's Royal Naval Service under strict security. Bombe operations directly supported convoy protection in the Battle of the Atlantic by locating German submarines through decrypted position reports, and supported bombing operations by identifying target defenses and weather conditions. Welchman's own primary account of the Bombe operation and the Hut 6 organization that ran the Enigma attack, published in Welchman 1982 after his retirement, was the first public detailed technical description of the Bombe methodology.

Lorenz and Colossus

The German High Command used a different cipher for strategic communications between senior commanders. The Lorenz SZ40 and SZ42 cipher machines, known at Bletchley Park as "Tunny," implemented a stream cipher on standard five-bit teleprinter code using twelve keying wheels arranged in three groups. The wheels combined into a key stream that was added modulo two to the plaintext bits according to the Vernam cipher construction, established by Vernam 1926 for wire-service teleprinter encryption,

$$c_i = p_i \oplus k_i$$

where p_i is the i-th plaintext bit, k_i is the corresponding key-stream bit generated by the wheel machine, and $\oplus$ is bitwise addition modulo two. The Vernam cipher is unconditionally secure when the key stream is truly random and used only once. Tunny's key stream was not random but generated deterministically from a finite wheel state, which meant the same key stream could be reconstructed from a known-plaintext break and then applied to other messages sharing overlapping key. The keyspace for a single message setting exceeded the Enigma keyspace by several orders of magnitude, and the Tunny traffic was substantially more valuable strategically because it carried senior-level orders.

Cryptanalysis of Tunny was achieved by Bletchley Park mathematicians including Bill Tutte who reconstructed the machine structure from intercepted traffic without ever seeing the machine itself. The initial machine solution was accomplished by manual and semi-manual methods and by an electromechanical device called the Heath Robinson. The Robinson used two tapes moving at high speed past photocell readers to correlate the intercepted traffic against a candidate wheel setting. Robinson performance was limited by tape stretching, tape breakage, and photocell response time.

Tommy Flowers of the General Post Office Research Station at Dollis Hill proposed replacing the Robinson tapes and photocells with an all-electronic machine that generated the candidate key stream internally using thermionic valves. Flowers's own primary technical account of the Colossus design, published in Flowers 1983 in the IEEE Annals of the History of Computing after the machine's declassification, describes the engineering decisions that made large-scale valve computing operationally reliable. Flowers's proposal was received skeptically at Bletchley Park because valve reliability was widely doubted for machines with valve counts above a few hundred. Flowers's telephone-exchange engineering experience gave him confidence that valve reliability could be managed by leaving the valves powered continuously to avoid thermal cycling, which was the dominant failure mode. He committed his own laboratory to building a prototype at his own initiative.

The Colossus Mark 1 was operational at Bletchley Park in February 1944 with approximately

1,600 valves. The Colossus Mark 2, delivered in June 1944 in time for the Normandy invasion, contained approximately 2,400 valves and processed the intercepted teleprinter tape at 5,000 characters per second, with pattern comparison operating at effectively

$$r_{\text{Colossus Mk 2}} = N_{\text{parallel streams}} \cdot r_{\text{tape}} = 5 \cdot 5{,}000 \approx 25{,}000 \text{ characters per second}$$

through parallel processing across five bit streams corresponding to the five bits of the ITA2 teleprinter alphabet. Ten Colossi were built by the end of the war. Colossus performed statistical tests including cross-correlation between the ciphertext and candidate wheel settings, computing statistics of the form

$$Z(\Delta) = \sum_{i=1}^{N} c_i \oplus k_i(\Delta)$$

where c_i is the intercepted character sequence, $k_i(\Delta)$ is the candidate key stream at wheel offset Δ, and $\oplus$ is the modulo-two operation. Wheel settings that produced statistically anomalous values of Z were candidates for the correct setting. The full historical reconstruction is available in Copeland 2006 and in the primary technical account by Randell 1980. The wartime technical report on the Tunny break authored by Good, Michie, and Timms at Bletchley Park in 1945, declassified in the early 2000s and transcribed at alanturing.net, remains the most detailed primary account of the machine reconstruction and cryptanalytic methods.

Colossus was the first large-scale programmable electronic digital computing device to enter operational service, predating the ENIAC's operational deployment by roughly two years. The machine was not general-purpose in the sense that ENIAC became after its stored-program conversion, but its purpose-built architecture executed a range of statistical operations against the intercepted Tunny traffic under operator control from switches and plugboard patch cables. The value of Colossus was that it made the daily break of Tunny traffic tractable within the operational time window that made the decrypted content actionable for military planning.

The American Cryptanalytic Effort

The United States conducted its own cryptanalytic effort at similar scale to the British effort, focused primarily on Japanese ciphers under the codeword MAGIC. The Japanese diplomatic cipher known as PURPLE was broken by a team led by Frank Rowlett at the Signal Intelligence Service through analytical methods that reconstructed the machine's internal structure without direct access to a physical example. Once the structure was recovered, an electromechanical analog was built from telephone stepping switches to allow rapid decryption of intercepted messages given the daily key setting, playing an operational role analogous to that of the reconstructed Tunny machines at Bletchley Park rather than to that of the Enigma-attack Bombes. The Japanese naval cipher JN-25 was broken by a separate team under Joseph Rochefort at Station HYPO in Hawaii using IBM tabulating machines to correlate encrypted messages against candidate code-book entries.

The IBM tabulating machines used for Japanese cryptanalysis were the same class of machine used for scientific computing at the Aberdeen Proving Ground and at other wartime scientific installations. The Manhattan Project at Los Alamos also used IBM tabulating machines, adapted for scientific rather than commercial calculation, to perform hydrodynamic and neutron-diffusion calculations at scale.

Both the British and American cryptanalytic efforts operated under strict secrecy that persisted for decades after the war ended. Colossus itself was destroyed at the end of the war

on Churchill's order, and the fact of its existence was not publicly acknowledged until the mid-1970s. The cryptanalytic personnel returned to civilian life without being able to describe what they had done during the war, which produced a gap in the postwar history of computing that was not filled until the declassifications of the 1970s and 1980s.

Manhattan Project Computing

The Manhattan Project consumed the largest concentration of scientific computing labor of any wartime program. The design of the plutonium implosion device required detailed hydrodynamic simulation of the shockwave that compressed the plutonium core to supercritical density. Analytic solutions were not available. Numerical solutions required calculations at a scale that human computer teams alone could not sustain within the wartime schedule.

The criticality condition for a nuclear chain reaction is expressed through the effective neutron multiplication factor

$$k_{\text{eff}} = \nu \cdot \frac{\Sigma_f}{\Sigma_f + \Sigma_c + P_L}$$

where ν is the mean number of neutrons produced per fission, Σ_f is the macroscopic fission cross-section, Σ_c is the macroscopic capture cross-section, and P_L is the neutron leakage probability. A configuration with $k_{\text{eff}} > 1$ sustains an exponentially growing chain reaction. The implosion problem required raising k_{eff} from subcritical to supercritical in a few microseconds by compressing the plutonium core so that P_L drops sharply while Σ_f rises. The hydrodynamic shockwave that accomplishes the compression follows approximately adiabatic behavior under the polytropic-gas approximation

$$P \cdot V^{\gamma} = \text{constant}$$

with adiabatic index γ appropriate to the compressed material, though the actual computation used substantially more detailed equations of state and radiation-transport terms. Both quantities required numerical evaluation at every point of a spatial grid at every time step of the microsecond-scale implosion, with the wartime calculations mostly exploiting spherical or cylindrical symmetry to reduce the effective dimensionality to one or two spatial coordinates rather than a full three-dimensional grid, which is what produced the computational demand within the resources available.

The Los Alamos computing group under Richard Feynman coordinated the IBM tabulating machine calculations. Feynman's own accounts, collected in Feynman 1985, describe a workflow in which physicists specified the calculation, human computer teams performed the initial arithmetic on desk calculators, and IBM machines performed the repetitive parallel arithmetic across large batches of intermediate results. The batch structure of the IBM tabulating machines matched the structure of the Manhattan Project calculations, which were dominated by grid-based finite-difference schemes on regular arrays.

The ENIAC's first substantive calculation, per Metropolis and Nelson 1982 and the retrospective in Metropolis 1987, was a Monte Carlo simulation of thermonuclear reaction rates for the hydrogen bomb feasibility study conducted for Edward Teller and John von Neumann at Los Alamos. The Monte Carlo method exploits the statistical convergence of averages of random samples to compute expectations of quantities that would otherwise require intractable multidimensional integration. The standard error of a Monte Carlo estimate of a quantity with standard deviation σ from N samples is

$$\epsilon_{\mathrm{MC}} = \frac{\sigma}{\sqrt{N}}$$

which converges slowly but is dimension-independent, making Monte Carlo the preferred approach for high-dimensional integrals such as those arising in neutron transport and thermonuclear reaction rate calculation. The ENIAC calculation used approximately one million punched cards of input and output and ran for several weeks at Aberdeen before returning results that informed subsequent hydrogen bomb design work at Los Alamos.

Wartime Computing Scale and Legacy

The combined wartime computing effort involved several thousand human computers, several hundred electromechanical and electronic machines, and cross-organizational personnel networks that included essentially every trained American, British, and refugee European mathematician, physicist, and engineer of relevant age. The personnel who developed wartime computing infrastructure supplied the founding cadre for the postwar computing industry. Mauchly and Eckert of the ENIAC founded the Eckert-Mauchly Computer Corporation that produced the UNIVAC. Aiken continued the Harvard Mark series. Stibitz continued at Bell Labs. Turing continued at the National Physical Laboratory in the United Kingdom on the Automatic Computing Engine design and later at Manchester on the Manchester Mark 1. Von Neumann continued at the Institute for Advanced Study on the IAS machine and its many copies.

The wartime problems also produced postwar research programs. Cryptanalysis matured into modern computer security. Ballistic-table computation matured into scientific and engineering computing. Manhattan Project hydrodynamics matured into computational fluid dynamics. Numerical weather prediction, begun as a wartime problem for bombing meteorology, matured into contemporary numerical modeling of atmospheric and oceanic systems following the seminal Charney Fjørtoft von Neumann 1950 barotropic vorticity integration on ENIAC. Each of these fields inherited both the computing techniques the wartime programs developed and the general recognition that large-scale computation had become an essential component of scientific and engineering work.

The secrecy imposed on the cryptanalytic effort had consequences for the historical record. The Colossus was unknown until the mid-1970s. The Polish contribution to Enigma cryptanalysis was not publicly acknowledged until similar declassifications. The role of the American cryptanalytic effort in the Pacific war was incompletely documented until decades after the war. These gaps produced a distorted early history of computing in which the ENIAC received disproportionate credit as the first electronic digital computer, when in fact Colossus preceded it by roughly two years for a narrower but nonetheless substantial computational scope.

Framework Application to the Wartime Era

The six-axis framework introduced in A237 applies to the wartime era with axis weightings that shifted substantially from the pre-war baseline treated in A238.

The first axis is numerical computation demand. Wartime demand added cryptanalytic and physics calculations to the ballistic-table baseline. Cryptanalytic operations on Bletchley Park Bombes reached tens of millions of rotor configurations per hour per machine. Manhattan Project calculations reached comparable operation counts per weapon design iteration. Ballistic-table demand continued from the pre-war baseline and grew as new weapons entered service. The total wartime computational demand exceeded any pre-war precedent

by orders of magnitude and required the concentration of resources that only wartime mobilization made available.

The second axis is real-time control. Fire-control computers deployed in operational combat continued the pre-war trajectory at greatly expanded scale. The Ford Instrument Mark 1 continued in service. The Kerrison Predictor was deployed against V-1 flying bombs in 1944 with substantial operational success. The Norden bombsight was deployed on essentially every heavy bomber. Cryptanalytic operations were not real-time in the sense of fire control but were time-critical in the sense that decrypted content lost operational value quickly, which pushed the Colossus and Bombe programs toward faster machines with higher throughput.

The third axis is reliability and verification. The Colossus valve-reliability engineering by Flowers established techniques for large-scale valve machines that ENIAC later applied. Continuous power to prevent thermal cycling, systematic hot-swapping of failing valves, and physical layout designed for maintenance access all originated in the Colossus program and transferred to postwar electronic computers. Verification of cryptanalytic results was performed by attempting to decrypt other messages with the same candidate settings, providing external check against the machine implementation.

The fourth axis is networking and distribution. The Bletchley Park operation depended on radio intercept stations across Britain and its allied territories, on the transportation of intercepted tapes to Bletchley by dispatch rider or teleprinter link, and on the distribution of decrypted intelligence to operational commands. The Chain Home radar network continued in operation for air defense. Manhattan Project computation was distributed across multiple sites including Los Alamos, Oak Ridge, and various IBM installations, connected by courier and secure telephone.

The fifth axis is software engineering as a discipline. Wartime computing produced substantial proto-software-engineering practice including the switch-and-patch-cable configuration of Colossus, the plugboard programming of the ENIAC, the systematic procedure manuals for IBM tabulating machine calculations, and the cryptanalytic worksheet notations that Bletchley Park developed. Turing's contributions to the theoretical foundations of computing predated the war in Turing 1936 and continued during and after it. Grace Hopper's work with the Harvard Mark I introduced the first program notation for the machine that later evolved into automatic programming and eventually into high-level languages, documented in Hopper 1946 as the machine's official operating manual.

The sixth axis is semiconductor economics and dual-use. The vacuum-tube industry was substantially expanded by wartime demand for radar, radio, cryptanalytic electronics, and computing. Learning-curve cost reduction as formalized in the preceding series articles applied to vacuum tubes during and after the war. The manufacturing infrastructure that produced the Colossus valves, the ENIAC valves, and the millions of other valves in wartime military electronics became the postwar consumer electronics manufacturing base that persisted until the transistor supplanted the vacuum tube in the late 1950s.

Conclusion

The Second World War was the formative moment for large-scale electronic digital computing. Three distinct computing programs at Bletchley Park, in the American cryptanalytic effort, and at Los Alamos each produced computing capability at scales that no pre-war program had approached. The cryptanalytic programs pioneered the engineering techniques including valve-reliability engineering, statistical computation, and industrial-scale searching of large discrete spaces that the postwar computing industry inherited. The Manhattan Project pioneered scientific computing at scales that later became routine for weapons design, weather forecasting, and computational physics. The ENIAC's first substantive calculation for the hydrogen bomb feasibility study connected the ballistic-table thread from the preceding article

to the atomic-weapons thread that dominated the immediate postwar computing agenda.

The next article in the series treats the transition from wartime to peacetime computing in the context of early Cold War air defense, culminating in the Semi-Automatic Ground Environment hereafter SAGE system as the largest computing project of the 1950s and the direct genealogy from SAGE to commercial timesharing and to modern distributed computing.

References

Books

- Copeland 2004
- Copeland 2006
- Feynman 1985
- Hodges 1983
- Kahn 1996
- Rhodes 1986
- Welchman 1982

Reference

- Flowers Colossus
- Polish Cryptanalysis of Enigma
- Rowlett and PURPLE
- Tutte and Tunny
- Turing at Bletchley

Related Posts

- A237 Framing and the Co-Development Mechanism
- A238 Pre-War Computing Origins and Ballistics

Research

- Charney Fjørtoft von Neumann 1950
- Flowers 1983
- Good Michie Timms 1945 General Report on Tunny
- Hopper 1946 Mark I Manual
- Metropolis 1987
- Metropolis and Nelson 1982
- Randell 1980
- Rejewski 1981
- Shannon 1949 Secrecy Systems
- Turing 1936
- Vernam 1926