

Colossus : El secreto mejor guardado por los ingleses durante la Segunda Guerra Mundial

Si la bomba atómica fue el secreto mejor guardado por los norteamericanos durante la Segunda Guerra Mundial, su equivalente en Inglaterra fue el Colossus, la primera computadora electrónica del mundo, que se diseñó explícitamente para poder descifrar los mensajes secretos de los nazis. Esto marcó el inicio de la escuela inglesa de cómputo electrónico, que dio al mundo la primera computadora con programa almacenado de la historia, la primera unidad de control microprogramada y muchas otras valiosas contribuciones a la computación moderna. Sus orígenes Thomas H. Flowers era un ingeniero de la Post Office Research Station (PORS), que se incorporó al proyecto de la Heath Robinson (una máquina propuesta por el matemático Maxwell Herman Alexander Newman para acelerar la decodificación del código Enigma de los alemanes) con la finalidad de rediseñar su contador electrónico. Al ver las dificultades mecánicas de la máquina, Flowers tuvo la osada idea de proponer que los datos de las cintas se almacenaran internamente, de manera electrónica. Ni Wynn-Williams ni Harold Keen (los expertos en electrónica de Bletchley Park) creían que la máquina de 1,500 bulbos que Flowers propuso, funcionaría. Pero, afortunadamente, Newman lo apoyó de cualquier manera y el proyecto fue autorizado(1,2), ante el desconsuelo de W. G. Radley (director de la PORS), que tuvo que poner a la mitad de su personal a trabajar día y noche durante 11 meses consecutivos (la PORS tenía órdenes directas de Churchill de dar prioridad máxima al trabajo proveniente de Bletchly Park). La máquina, que sería llamada después Colossus, fue diseñada por Thomas H. Flowers, S. W. Broadbent y W. Chandler de forma ultrasecreta. Ni siquiera ellos mismos pudieron ver nunca todas las partes de la máquina y nunca se hicieron reproducciones de los diseños originales, los cuales se tomaron directamente de las notas elaboradas por sus creadores. Nunca hubo manuales, ni registros o preguntas sobre sus piezas o la cantidad de labor consumida. Su ensamblaje y el montaje de sus conexiones internas se efectuó por etapas, usando personal distinto, para que nadie supiera los detalles de toda la máquina(1). La primera Colossus se puso en funcionamiento en diciembre de 1943. Para alivio de Flowers, la máquina resolvió adecuadamente su primer problema en sólo 10 minutos, repitiendo además el resultado de manera consistente en, al menos, dos ocasiones consecutivas (la Heath Robinson solía dar resultados ligeramente distintos si se resolvía el problema en repetidas ocasiones. Esto se debía a algunas dificultades en la forma en que se obtenían los pulsos para el conteo que efectuaba la máquina)(3,4). Colossus usaba una lectora fotoeléctrica similar a la de la Heath Robinson, pero mucho más rápida (leía 5,000 caracteres por segundo). Los contadores que usaba eran bi-quinarios, basados en las ideas publicadas por W. B. Lewis, quien trabajó junto con Wynn-Williams en Cambridge, pero no participó directamente en Bletchley Park(3). Características principales Algunas de las características más importantes de Colossus eran las siguientes (2,3,5):

- Usaba bulbos a gran escala y empleaba el sistema binario.
- Sus datos de entrada los leía de una cinta de papel perforada usando una lectora fotoeléctrica.
- Usaba circuitos de dos estados y sus operaciones eran controladas mediante los pulsos de su reloj interno, lo que hacía posible operarla a cualquier velocidad, lo cual era muy útil para probarla.
- Sus circuitos permitían efectuar conteos, aplicar operaciones Booleanas y efectuar operaciones aritméticas en binario.
- Sus funciones lógicas podían manejarse de manera preestablecida usando un tablero de interruptores, o podían seleccionarse de manera condicional (había una especie de menú con las configuraciones posibles). usando relevadores telefónicos.
- Era totalmente automática.
- Tenía una memoria de cinco caracteres de cinco bits cada uno, los cuales se almacenaban en un registro especial.
- Su velocidad de operación era de 5,000 Hertz (ciclos por segundo), esto contrasta notablemente con la velocidad de las computadoras modernas, que es del orden de millones de Hertz.
- Medía 2.25 metros de alto, 3 metros de largo y 1.20 metros de ancho.
- Sus resultados se almacenaban temporalmente en relevadores para luego darles salida a través de una máquina de escribir eléctrica que funcionaba a una velocidad de 15 caracteres por segundo.
- Permitía saltos condicionales.
- No contaba con programas almacenados internamente y era, obviamente, una máquina diseñada explícitamente para tareas criptográficas.

- Internamente generaba cadenas de 501 bits en anillos de la misma longitud que los interruptores mecánicos de cada uno de los 12 discos de la SZ42 de Lorenz.

Programación primitiva Los resultados producidos por Colossus no eran el texto final decodificado, sino más bien un mensaje intermedio que debía ser procesado a mano(5). Sin embargo, Irving John Good y Donald Michie descubrieron que, efectuando ciertos cambios en las conexiones de la máquina mientras ésta estaba en operación, era posible que Colossus realizara la tarea que los criptógrafos efectuaban a mano(1).

Éste fue un descubrimiento muy importante y la técnica se incorporó de manera automática en la Mark II Colossus, completada el 1 de junio de 1944, (esto fue cinco días antes del histórico desembarco en Normandía) sólo un mes después de haber sido encargada (se dice que Flowers sospechaba que le pedirían más máquinas, así que antes del intempestivo encargo, ya había avanzado bastante en el siguiente modelo de Colossus con la ayuda del personal de la PORS). Descendientes La Mark II Colossus era cinco veces más rápida que su predecesora, pues usaba una memoria temporal implementada con registros de cinco etapas, además de operar en paralelo y realizar automáticamente la reutilización de información descubierta por Good y Michie(6,7). La nueva versión de Colossus usaba 2,400 bulbos y era mucho más flexible que su predecesora. De hecho, se sabe que Geoffrey Timms demostró al final de la guerra que casi se podían efectuar multiplicaciones en base 10 con ella (la razón por la que no podía completarse la multiplicación era porque los circuitos se complicaban tanto con esta operación que los pulsos del reloj se debían retrasar, lo que causaba errores de conteo en el cálculo(2). Se estima que hacia el final de la guerra había al menos 10 máquinas Colossus en operación (todas ellas distintas) y varias más estaban produciéndose(6). También parece ser que se construyó toda una serie de pequeñas máquinas y acoplamientos especializados en Bletchley Park en esta época(3). Flowers diseñó otra máquina más después de la guerra: la Super Robinson. Esta máquina era un híbrido entre Colossus y Heath Robinson, porque usaba en gran medida los circuitos de la primera para sincronizar cuatro cintas que eran procesadas en paralelo usando un sistema mecánico como el de la segunda(3,6). Destino incierto Aparentemente se destruyeron ocho de las 10 máquinas Colossus de Bletchley Park en 1946, por orden directa de Winston Churchill. Una más sobrevivió hasta los 1950, y la última fue desmantelada en 1960 cuando todos los diagramas de sus circuitos y sus planos fueron quemados. Se sabe que varios científicos norteamericanos vieron funcionar a Colossus en visitas secretas a Bletchley Park después de la guerra, pero el gobierno británico vetó toda la información sobre la máquina durante 30 años. Las razones no fueron sólo militares, sino también políticas, pues se sabe que hubo al menos un bombardeo alemán a una ciudad inglesa que pudo haberse evitado gracias a Colossus, pero que se dejó proceder (a costa de un sinnúmero de muertes) para proteger uno de los secretos mejor guardados durante la Segunda Guerra Mundial.

Bibliografía: (1) Andrew Hodges, "Alan Turing: The Enigma", Simon and Schuster, New York, 1983. (2) Irving John Good, "Pioneering Work on Computers at Bletchley", en N. Metropolis, J. Howlett & Gian-Carlo Rota (Editores), "A History of Computing in the Twentieth Century. A Collection of Essays", Academic Press, New York, pp. 31-45, 1980. (3) Brian Randell, "The Colossus", en N. Metropolis, J. Howlett & Gian-Carlo Rota (Editores), "A History of Computing in the Twentieth Century. A Collection of Essays" Academic Press, New York, pp. 47-92, 1980. (4) Michael R. Williams, "A History of Computing Technology", Prentice Hall, Englewood, New Jersey, 1985. (5) J. A. N. Lee, "Computer Pioneers", IEEE Computer Society Press, Los Alamitos, California, 1995. (6) Donald Michie, "The Bletchley Machines", en Randell, Brian (Editor), "The Origins of Digital Computers". Selected Papers, Springer-Verlag, pp. 327-328, 1973. (7) William E. Boggs, "Colossus", en Ralston, Bryan & Reilly, Edwin D., "Encyclopedia of Computer Science", Van Nostrand Reinhold, Third Edition, New York, pp. 189-190, 1993. Este artículo es un extracto del libro Breve Historia de la Computación y sus Pioneros. Volumen I: Los Orígenes del Hardware", del mismo autor, y próximo a publicarse por la editorial Xview.