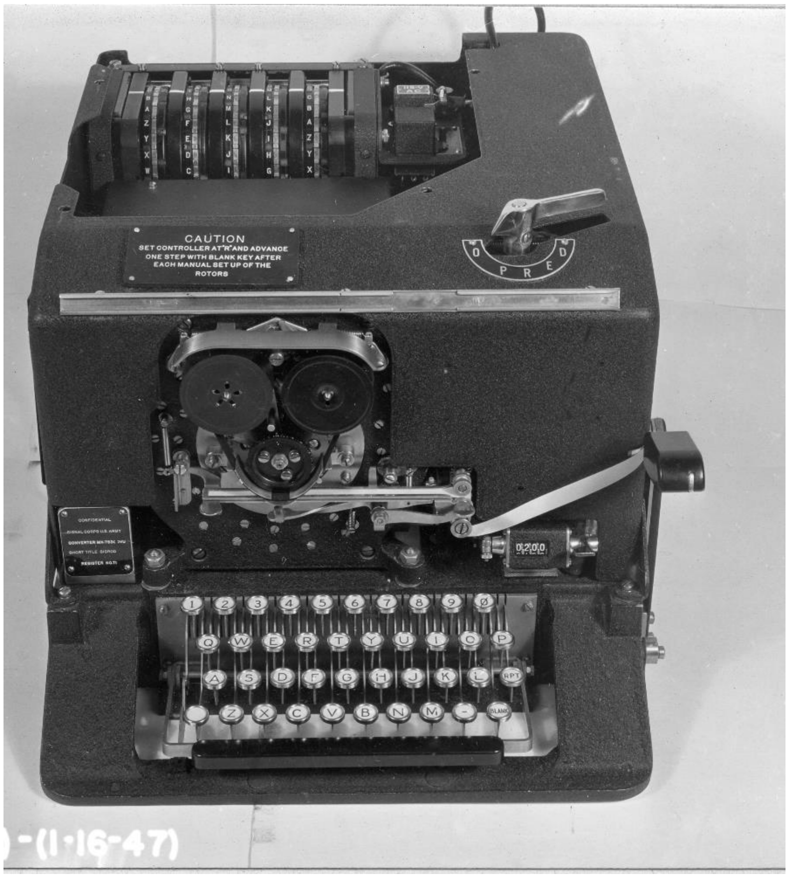
Changing Machines March 18

During World War II the United States had the most secure cipher machine of any nation involved in the conflict. The device, known to the Army as the SIGABA, and to the Navy as the ECM, had been developed before the war in exchanges of cryptographic ideas between the two services. It incorporated the best ideas of William Friedman, Frank Rowlett, and Laurance Safford, and depended on an innovative way to use rotors --- rotating wired wheels, which were a frequently-used feature of cipher machines around the world.

Although the SIGABA/ECM had kept high-level American communications secure during the war, there was some apprehension in the military cryptologic services that continued use of it might make it vulnerable to enemy exploitation. Cryptographers worried that word would get around about its internal workings, or that simple accumulation of large amounts of traffic would help foreign cryptanalysts.

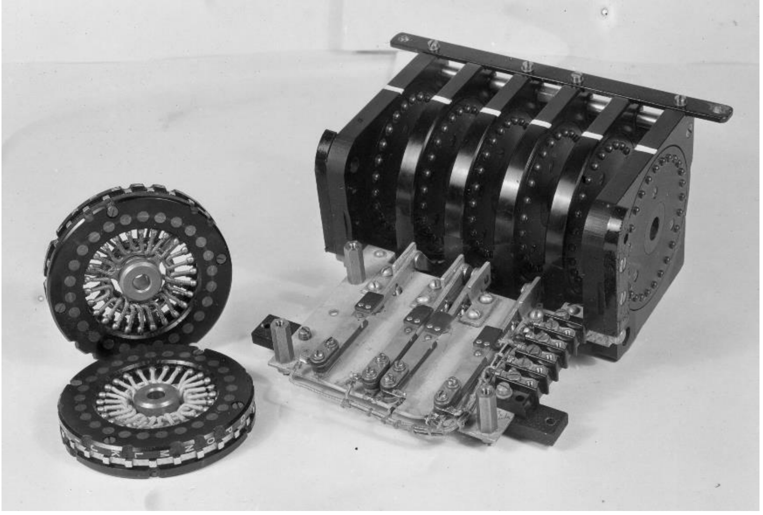
The Army and Navy began working on alternate cryptographic machines. These efforts were consolidated by the Armed Forces Security Agency, the first U.S. centralized cryptologic organization, when it was established in 1949, and, eventually, by NSA.

One user of the SIGABA/ECM was the system of military attachés around the world. The Army Security Agency (ASA), successor to the wartime cryptologic organization, was developing a plan for replacing the SIGABA, soon after the end of the war, a number of Army attaché offices that did not use the SIGABA requested a machine for encryption. The ASA determined that a device known as the SIGROD* would be suitable.


CAUTION
SET CONTROLLER AT "R" AND ADVANCE
ONE STEP WITH BLANK KEY AFTER
EACH MANUAL SET UP OF THE
ROTORS
O P R E D
)-(1-16-47)

SIGROD.

The SIGROD was a rotor-driven, semi-portable, electro-mechanical device weighing 137 pounds. It used a standard typewriter keyboard to print messages, either encrypting or decrypting, to a printed, gummed tape. It was capable of operating at 50 words per minute, and was considered secure for material up to TOP SECRET. The SIGROD exterior resembled the SIGABA. However, the SIGROD used 5 rotors, compared to 15 in the SIGABA; in addition, the stepping mechanism for the rotors in the SIGABA was considerably more complex.



SIGROD rotor basket

The ASA leadership put certain conditions on distribution of the SIGROD to attachés worldwide. First, it had to be certain that the volume of communications justified the deployment of such a sophisticated machine. Each office where the machine was to be located had to have adequate security, preferably a separate room to which access could be controlled. The office also had to have provisions for maintenance of the machine and training its operators. Each request for a SIGROD would have to be considered individually.

By March 1949, the date of the last wrapup report on attaché use of the SIGROD, 52 of the 60 offices worldwide were using the machine. At least one office, in Kabul, was seeking to upgrade its security situation. The few remaining offices apparently did not meet the minimum amount of traffic volume.

* In the Army in that period, virtually all communications and communications security equipment started with the letters “SIG.” This trigraph was followed by three or four random letters that had no relation to the equipment itself. Seemingly, the only requirement was that the final result be pronounceable.

508 caption: 1) a cubical machine, with a keyboard in front, and 5 rotors emplaced inside the top; a paper tape and an ink ribbon run across the front above the keyboard. 2) a rectangular metal piece with recesses into which rotors may be emplaced; to the left of this are two rotors, small wheels with wiring in the center.