The basic cryptographic principle of Navy machine is to have five 26-point ciphering rotors, the rotatory displacements of which are controlled by three similar rotors, the rotatory displacements of which are in turn irregular and are controlled by the combined effects of three 10-point and two 26-point rotors. The minimum possible cryptographic cycle is (acoording to Navy) 26 x 651 = 16926 units; the maximum is 17676 x 651 = 11,441,976 units for any given initial key settings.

The machine has many valuable features. It weighs about 105 pounds and is composed of a single unit. It has an operating speed of at least 50 words per minute. The control is such that if operated in encipherment at a speed greater than that at which cryptographic functioning is possible, the effect is merely to drop out single letters of the plain text, so that no errors in cryptographic functioning are made by the machine due to excessive operating speed. It has automatic means for setting up the message key and for advancing the rotors at a high speed from an initial starting point to make a correction. The ciphering elements are on a removable chassis, so that this assembly can be placed in a safe when the machine is not in use. The typewriting element is a tape printer, and can be used as an ordinary typewriter for plain language for address and signature.

The basic cryptographic principle of having the output of electrical rotors control the displacements of ciphering rotors was invented by Messrs. Friedman and Rowlett, and is covered in secret patent application #70,412 filed March 23, 1936. This principle was disclosed and explained to various members of the Code and Signal Section, Navy Department at three conferences in 1935.

This principle also formed the basis of the designs submitted by the office of the Chief Signal Officer to Signal Corps Laboratories in connection with development of proposed converter M-161.

copy ✓