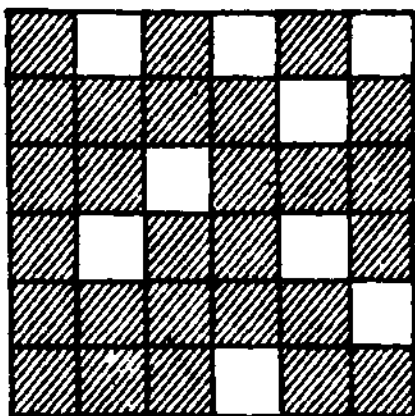


complicated, but as the development was progressive the French never lost cryptanalytic contact. Painvin solved one that spring thanks to a Bavarian prince's telling his parents, the king and queen, that he had been wounded. The **polyalphabetic** systems culminated in one used between Berlin and Constantinople. It employed 25 alphabets, required 32 tableaux, and was so excessively complex that only cipher clerks comfortably ensconced in quiet, well-equipped headquarters offices could handle it. In fact, it was *too* elaborate, and the pendulum swung away from substitution to transposition. At the end of 1916, transposition messages again appeared in German military communications.

By January, 1917, the French cryptanalysts recognized these as turning grilles. About all that these grilles have in common with the fixed concealment grille of Cardano is the name and the openings in the mask. The turning grille is usually a square sheet of cardboard divided into **cells**; one quarter of these are punched out in a pattern such that when the grille is rotated to its four positions, all the cells on the paper beneath will be exposed and none will be exposed more than once. A 6 x 6 grille might look like this:



This is laid over a sheet of paper and the first nine letters are written through the apertures. Then it is turned 90 degrees, the next nine letters are written through the openings in their new position, and so on for two more turns. By then each of the 36 cells on the paper will have a letter inscribed in it, and the cryptographer can read it off in any pattern he chooses—usually by rows. Messages longer than 36 letters must repeat the process; in the last section of less than 36 letters, the unwanted cells can simply be blocked out.

The Germans provided their signal troops with a variety of sizes for different length messages. Each grille had a codename: ANNA for 25 letters, BERTA for 36, CLARA, 49, DORA, 64, EMIL, 81, FRANZ, 100. These codenames were changed weekly.

Grille systems are particularly susceptible to multiple **anagramming**—which is the general solution for transposition systems—because their sections are of necessity of equal length. But the system produces intriguing geometrical symmetries, and the French soon devised attacks exploiting this and other weaknesses. The grilles lasted four months.

Britain, too, had her military **cryptanalytic** bureaus. But she had made no more preparations for them before the war than she had done for Room 40, and her Army cryptanalysts, expert though they became, never achieved the proficiency of the French.

Her setup was essentially the same as France's. The head organization, M.I. 1(b), was attached to the War Office. A field agency was established at British Expeditionary Force headquarters, and individual cryptanalysts were stationed with the several armies.

M.I. 1(b) was still a small, four-man **section**—1(b)—of the Military Intelligence Division in December of 1915 when Malcolm Vivian Hay of Seaton was placed in charge. Hay, then 34, was the grandson of the second son of the seventh Marquess of Tweeddale and had succeeded to the Seaton Estates near Aberdeen when he was 2. After an education at Beaumont College and abroad, he returned to supervise his farms; he joined the Gordon Highlanders as a captain at the outbreak of war. He was machine-gunned at the Battle of Mons and was captured by the Germans when he was left on the field by the British retreat. Partly paralyzed as a result of his head wound, he was repatriated in February, 1915, as unfit for military duty. After learning to walk with the aid of a cane, he was promoted to major and given command of M.I. 1(b).

He began at once to scour the universities for bright young men, preferably language scholars, to supplement the three original civilians on the staff: J. St. Vincent Pletts, a radio engineer from Marconi's Wireless Telegraph Company; J. D. Crocker, a young Cambridge scholar, and Oliver Strachey of the Indian Civil Service, who liked cryptanalysis so much that he switched after the war from administering the East Indian Railway to **codebreaking** for the Foreign Office. Hay recruited a remarkable concentration of men who were later to achieve eminence, if listing in *Who's Who* may be taken as an index. Among them were his chief assistant, John Fraser, 32, later professor of Celtic as a fellow of Jesus College, Oxford; Arthur SurrIDGE Hunt, 45, then and later professor of papyrology at Oxford and one of the world's most eminent authorities on ancient writing; David Samuel Margoliouth, 58, professor of Arabic at Oxford, later president of the Royal Asiatic Society and author of many works on Arabic literature and history; Zachary Nugent Brooke, 33, then lecturer in history at Cambridge, later professor of medieval history there and an editor of the *Cambridge Medieval History*; Edward Thurloe Leeds, 39, then assistant keeper of the department of antiquities of the Ashmolean Museum and, after the war, keeper of that first public museum