COMMUNICATIONS

Piccolo players

The wartime rush to adapt for radio communication the teleprinter or Teletype system originally developed for line operation remains an example of the danger of making use of technology standards for a different purpose without a fundamental rethink. Compared with alternative forms of machine telegraphy, including high-speed Morse and the Hellschreiber system, conventional r.t.t.y. with five-unit code and frequency-shift keying has always demanded, if error rates are to be kept low, a very good signal-to-noise ratio, freedom from interference and multipath effects, and preferably diversity reception. To minimize these problems, the seven-unit code and other error-correcting techniques, including automatic repetition, have come into widespread use, though clearly these are palliatives rather than cures.

Many years ago it was recognized that under difficult radio conditions an improvement was possible by the use of multi-tone signalling. J. V. Beard and A. J. Wheeldon (*Point-to-Point Telecommunications* June 1960, pp.20-48) showed that two-tone a.m. transmission could offer substantial improvement over f.s.k. in conditions of selective fading, weak signals and interference. However, a series of counter-attacks on two-tone transmission, based on results over high-power point-to-point circuits, appeared soon afterwards, since when binary f.s.k. has remained the dominant system for h.f. – though with at least one notable exception.

Since October 1962, the Communications Engineering Department of the Foreign & Commonwealth Office (formerly Diplomatic Wireless Service) has been using the Piccolo system based on multiple frequency-shift keying as the basis of its main h.f. network that links more than 50 British embassies to Hanslope Park, near Newport Pagnell. The original Piccolo system, with no less than 32 tones, imposed stringent requirements on frequency stability but, due to signal integration techniques using resonant LC filters, it could produce clean copy from signals almost buried in noise. It was thus far more suitable than conventional f.s.k. for use with relatively low-power transmitters located in residential areas, often with a flag-pole-type aerial. Harold Robin, Don Bayley and J. D. Ralphs made many attempts to interest British firms and organizations in the system and for a time Marconi undertook to market equipments built by D.W.S. More recently, manufacture and marketing has been by Racal, although clearly it has never been an easy task to introduce a relatively costly, non-compatible system. By 1968, by which time the Mark III unit was being introduced, I was lamenting in print on the reasons why Piccolo went flat and on the general lack of interest in this technically elegant British system.

Recently a new Mark VI system has been developed that reduces the number of tones from 32 to 6 for ITA-2 and 12 for ITA-5 (*Radio and Electronic Engineer* Vol. 52, no. 7, pp.321-330, July 1982). Although this clearly loses a little in basic performance, it halves the bandwidth requirements and reduces the formerly extremely stringent frequency stability requirements. It also makes for rather lower capital costs and permits the use of either forward error correction or automatic request for repeats. Combined with the Piccabell selective calling system that summons an off-duty operator for urgent traffic, it remains one of the few technically successful attempts to match r.t.t.y. to simple low-power h.f. circuits. But it remains to be seen whether the Mark VI system (to be marketed by Racal as the LA1117 modem) will at last achieve the wider commercial acceptance that the Foreign Office engineers have always felt it deserved, but which has so far always eluded the earlier models.

Project Raven

Much though some engineers may regret it, the British communications industry has become increasingly coupled to meeting military or "defence" requirements; a market that has (so far) not been under pressure from Japan and one in which a good deal of expertise has been acquired by British design teams. A major Australian project, born in 1976 and due in service in 1986, "Project Raven," covering e.c.m.-resistant h.f. and v.h.f. vehicle and manpack tactical systems for ranges up to 2000 miles, looks like bringing major contracts to Plessey Australia (with Plessey UK participation). In 1981 "project definition" contracts were awarded to both Plessey and Racal Milcom but the latest A$7-million contract for design and establishment of production facilities has been won by Plessey who hope it will lead to production contracts worth A$150M to A$200M.

Technically an interesting feature of the Plessey proposals is the use of electronic null steering of simple twin aerials to provide some 40dB rejection of a single jammer as an electronic-counter-counter-measure. Null steering as an antijam protection system is considered now feasible even for manpack v.h.f. sets and may be extended to h.f. In general Plessey engineers argue that while simple frequency hopping systems are of considerable value against an unsophisticated opponent they are particularly vulnerable to d/f-assisted attack. They list priorities for e.c.c.m. in the following order: imperceptibility; inscrutability; physical invulnerability; and electromagnetic invulnerability. A simple null-steering technique for h.f. communications was described at the recent IEE conference "H.F. communication systems and techniques" by J. K. Webb (Mitre Corporation) using a quadrature phase-shift channel with an auxiliary aerial.

Secrets of Hut 6

In the decade since the disclosure of the breaking of the German Enigma cipher machine (as well as the Abwehr and police hand ciphers and the Italian machine cipher) in the books by Gustave Bertrand "Enigma" and Frederick Wintherbotham "The Ultra Secret", there have been a spate of further books and memoirs of the fascinating Bletchley Park operation. But most of the insider books have reflected the views of the Intelligence analysts and distribution people of Hut 3 rather than those of the actual cryptanalysts of Hut 6, who were responsible for codebreaking, or the signals people and radio operators who intercepted the traffic. Few of the many authors, with the exception of Bertrand whose teams were in France and not at B.P., have been in any position to draw conclusions of permanent value to the black arts of codebreaking and Sigint.

For this reason it seems a pity that a new book "The Hut Six Story" by Gordon Welchman (published in the USA by McGraw Hill and in the UK by Allen Lane) has attracted less public interest and fewer reviews than the earlier books. For Welchman joined the B.P. team of cryptanalysts in 1939, worked in Hut 6 and later became Assistant Director of Mechanization. After the war, his plans for the peacetime GCHQ were largely rejected but instead of returning to the academic field he entered industry, joined the brain drain in 1947, and for many years worked in the field of communications systems planning for The Mitre Corporation, the US Federal Research Centre, etc. concerned with battlefield communication systems etc.

The earlier accounts, while differing in the credit given to the Polish and French cryptographic organizations, have largely supported the idea that Enigma could always be cracked by rigorous mathematical attack when backed up by some prior knowledge of the machines. Most (Bertrand's excepted) played down the role of Hans-Thilo Schmidt, the German who provided the French with a mass of information on Enigma ciphering procedures. Few have shown any clear understanding of why the German cryptographers had every reason to believe their system was totally secure in those pre-computer days.