PART II CODING AND CRYPTOGRAPHY
READING LISTS

The notion of an ‘error-correcting code’ did not exist prior to 1940 and those who wish to learn about error correction from one of the pioneers in the subject will do well to consult Richard Hamming’s own book on the matter [3] (Hamming died only in 1998). For the present course, the best book for further reading is Welsh [11] (I was taught by him and used the book myself as an undergraduate). After this, the book of Goldie and Pinch [9] provides a deeper idea of the meaning of ‘information’ and its connection with the topic. Lecture notes representing various interpretations of the Schedules are to be found on the course page: http://www.dpmms.cam.ac.uk/study/II/ Coding/ [2], and the notes by my immediate predecessors Carne and Körner are strongly recommended. The book by Koblitz [7] develops the number theoretic background. For budding cryptologists and cryptographers (as well as those who want a good read), see Kahn’s book [4].

The end the beginning, this quotation from Galbraith[1] (referring to his time as ambassador to India) taken from Koblitz [7], puts everything we do in perspective.

> I had asked that a cable from Washington to New Delhi . . . be reported to me through the Toronto consulate. It arrived in code; no facilities existed for decoding. They brought it to me at the airport — a mass of numbers. I asked if they assumed I could read it. They said no. I asked how they managed. They said that when something arrived in code, they phoned Washington and had the original read to them.

References

[1] U. Eco *The Search for the Perfect Language* (English translation), Blackwell, Oxford 1995.

[2] Course page on Maths Faculty website.

[3] R. W. Hamming *Coding and Information Theory* (2nd edition) Prentice Hall, 1986.

[4] D. Kahn *The Codebreakers: The Story of Secret Writing* MacMillan, New York, 1967. (A lightly revised edition has recently appeared.)

[5] D. Kahn *Seizing the Enigma* Houghton Mifflin, Boston, 1991.

[6] M. Kline *Mathematical Thought from Ancient to Modern Times* OUP, 1972.

[7] N. Koblitz *A Course in Number Theory and Cryptography* 2nd edn (1994), Springer.

[8] D. E. Knuth *The Art of Computing Programming* Addison-Wesley. The third edition of Volumes I to III is appearing during this year and the next (1998–9).

[9] G. M. Goldie and R. G. E. Pinch *Communication Theory* CUP, 1991.

[10] T. M. Thompson *From Error-correcting Codes through Sphere Packings to Simple Groups* Carus Mathematical Monographs **21**, MAA, Washington DC, 1983.

[11] D. Welsh *Codes and Cryptography* OUP, 1988.

SM, Lent Term 2012

[1] J.K. (Ken) Galbraith was a Keynesian economist and a leading advocate of 20th century American liberalism. Under JFK he served as the U.S. Ambassador to India from 1961 to 1963 and was notable for his severe criticism of Mountbatten, the last Viceroy, over his role in the partition of India in 1947.