REFERENCES


[FRI 1923] FRIEDMAN W, Elements of Crypt Analysis, Aeegan Park Press, Laguna Hills, California, 1976, First Published in 1923


[PRE 1994] PRENEEL B, NUTTIN M and BULLENS J, Crypt Analysis of The CBF Mode of the DES with a Reduced Number of Rounds, CRYPTO 93, pp. 212-223, 1995


[RAB 1979] RABIN M O, Digitalised Signatures and Public Key Functions as Intractable as Factorisation, MIT Laboratory for Computer Science, 1979


[SHA 1951] SHANNON C E, Prediction and Entropy of Printed English, Bell system Technical Journal, 30, pp. 50-64, 1951


