

Literatur

- [1] C. A. Deavours: Unicity points in cryptanalysis. *Cryptologia* 1 (1977), 469–684.
- [2] M. E. Hellman: An extension of the Shannon theory approach to cryptography. *IEEE Trans Information Theory* 23 (1977), 289–294.
- [3] A. M. Jaglom, I. M. Jaglom: *Wahrscheinlichkeit und Information*. VEB Deutscher Verlag der Wissenschaften, Berlin 1967.
- [4] H. Jürgensen: Language redundancy and the unicity point. *Cryptologia* 7 (1983), 37–48.
- [5] H. Jürgensen, D. E. Matthews: Some results on the information theoretic analysis of cryptosystems. *CRYPTO* 83, 303–356.
- [6] J. Reeds: Entropy calculations and particular methods of cryptanalysis. *Cryptologia* 1 (1977), 235–254.
- [7] C. E. Shannon: A mathematical theory of communication. *Bell System Technical Journal* 27 (1948), 379–423, 623–656. [Online im WWW: <http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html>]
- [8] C. E. Shannon: Communication theory of secrecy systems. *Bell System Technical Journal* 28 (1949), 656–715. [Online im WWW: <http://www3.edgenet.net/dcowley/docs.html> oder: <http://www.cs.ucla.edu/~jkong/research/security/shannon.html>]
- [9] C. E. Shannon: The entropy of printed english. *Bell System Technical Journal* 30 (1941), 50–64.