# Ausklang

Bevor sich unsere Wege wieder trennen, möchte ich Ihnen, lieber Leser, verehrte Leserin, das folgende Wort des Dichters Novalis (1772 - 1801) in Erinnerung rufen.

In diesem Gedicht drückt sich die Sehnsucht nach einer Welt aus, in der Kryptologie überflüssig ist. Nach Meinung des Dichters wird diese Welt Wirklichkeit, wenn man nur ein Zauberwort weiß und es ausspricht:

Wenn nicht mehr Zahlen und Figuren
sind Schlüssel aller Kreaturen,
wenn die, so singen oder küssen,
mehr als die Tiefgelehrten wissen,
wenn sich die Welt ins freie Leben
und in die Welt wird zurückbegeben,
wenn dann sich wieder Licht und Schatten
zu echter Klarheit werden gatten
und man in Märchen und Gedichten
erkennt die wahren Weltgeschichten,
dann fliegt von *einem* geheimen Wort
das ganze verkehrte Wesen fort.

* *
*

# Literatur

Die Bücher von Kahn [13] und Franke [10] sind sehr lesenswerte Darstellungen der Geschichte der Kryptologie, in denen insbesondere die Entwicklungen bis 1945 detailliert geschildert sind. Zur Vertiefung der in diesem Buch dargestellten Themen können [1], [6], [12] und [19] dienen, während die Lektüre der empfehlenswerten kryptographischen Bücher [7], [11] und [12] erhebliche mathematische Anforderungen an den Leser stellt.


1. H. Beker and F. Piper: *Cipher Systems. The Protection of Communication.* Northwood, London 1982.

2. T. Beth, P. Heß und K. Wirl: *Kryptographie.* Teubner, Stuttgart 1983.

3. M. Beutelspacher: *Kultivierung bei lebendigem Leib.* Drumlin Verlag, Weingarten 1986.

4. K. Bosch: *Elementare Einführung in die Wahrscheinlichkeitsrechnung.* Vieweg-Verlag, Braunschweig/Wiesbaden $^{5}$1984.

5. D. Chaum: *Security without Identification: Transaction systems to Make Big Brother Obsolete.* Comm. ACM **28** (1985), 1030-1044.

6. D. W. Davies and W. L. Price: *Security for Computer Networks.* John Wiley & Sons 1984.

7. D. Denning: *Cryptography and Data Security.* Addison Wesley, Reading, Mass. 1983

8. W. Diffie and M.E. Hellman: *New directions in cryptography.* Trans. IEEE Inform. Theory, IT-22, 6 (1976), 644-654.

9. A. Fiat and A. Shamir: *How To Prove Yourself: Practical Solutuions to Identification and Signature Problems.* Manuskript.

10. H.W. Franke: *Die geheime Nachricht.* Umschau-Verlag, Frankfurt/Main 1982.

11. F.-P. Heider, D. Kraus und M. Welschenbach: *Mathematische Methoden der Kryptographie.* Vieweg, Braunschweig 1985.

12. P. Horster: *Kryptologie.* B.I.-Wissenschaftsverlag, Mannheim - Wien - Zürich 1985.

13. D. Kahn: *The Codebreakers.* Macmillan, New York 1967.

14. A.G. Kohnheim: *Cryptography. A Primer.* John Wiley & Sons, New York 1981.

15. J.L.Massey: *Shift-register Synthesis and BCH Decoding.*IEEE Inform. Theory, IT-15, 1 (1969), 122-127.

16. K. Rihaczek: *Datenverschlüsselung in Kommunikationssystemen.* Vieweg-Verlag, Braunschweig/Wiesbaden 1984.

17. R. Rivest, A. Shamir and L. Adleman: *A method for obtaining digital signatures and public key cryptosystems.* Comm. ACM **21** (1978), 120-126.

18. C.E. Shannon: *Communication theory of secrecy systems.* Bell. Sys. Tech. J. **30** (1949), 657-715

19. G. Weck: *Datensicherheit.* Teubner, Stuttgart 1984.