Preface

On 19th December, 1990 the Royal Netherlands Academy of Arts and Sciences organised a symposium on cryptography and data protection. Lecturers from various disciplines presented their point of view. Since the resulting multi-sided view on this contemporary topic is of interest for a broad scientific public, it was decided to publish the proceedings of the symposium.

The first paper, by J.L. Massey, gives an appraisal of the current status of cryptologic research. The principal concepts of both secret-key and public-key cryptography are described. Shannon's theory of secrecy and Simmons' theory of authenticity are reviewed. Some important public-key systems and cryptographic protocols are treated.

Public key cryptosystems are based on mathematical operations that are easy to perform, but without additional information difficult to undo. In the second paper H.C.A. van Tilborg provides some mathematical background to the logarithm system, the RSA System, both of which are explained by Massey, and the knapsack system. He further deals with some factorisation methods which were found in connection with developments in cryptography.

The next two lectures concern practical aspects of data protection. J.H. van Bemmel discusses the purposes of computer storage and electronic exchange of medical data and the consequences for data protection. To this end he considers the different types of medical data and their use, the different users of medical data and some legal aspects of privacy.

Application of data protection in financial systems is treated by T.W.M. Jongmans. The urgency of protection here is obvious, since the data themselves are money. He compares the classical basis of security with the modern security techniques. Here theoretical cryptographic systems, discussed by Massey, find a practical implementation. This is illustrated by the security concept for the National Payments Circuit. He further indicates which difficulties of operating encryption techniques arise in practice.

Legal aspects of data protection are discussed by H. Franken. The rapid developments in information technology and telecommunications stimulate abuse and create uncertainty. In particular, it is not clear whether data should be considered as goods and be subject to laws dealing with goods. New criminal and civil laws have to delimit the border between what is permitted and what is not. Franken stresses the limited function of the law, since for genuine enforcement the criminal law should be invoked sparingly and cannot replace measures initiated by the owners and users themselves.

The final paper by D. Chaum is a view in the future. It describes a system of card computers which provides security for the users without the need to reveal their identity. In place of the variety of 'tokens' issued by organisations today one single credit-card sized card computer would suffice. Chaum explains the principles of digital signatures, payment transactions and credential transactions based on cryptographic systems treated by Massey, and discusses the advantages of the new system for individuals and organisations. His paper illustrates some concepts which are basic for developments which will change our financial system.

J.H. van Lint
R. Tijdeman
editors