A EUROPEAN CALL FOR CRYPTOGRAPHIC ALGORITHMS: RIPE; RACE INTEGRITY PRIMITIVES EVALUATION

J. Vandewalle[1] D. Chaum[2] W. Fumy[3]
C. Jansen[4] P. Landrock[5] G. Roelofsen[6]

[1]Katholieke Universiteit Leuven, E.S.A.T.
Kard. Mercierlaan 94, B-3030 Heverlee, Belgium

[2] C.W.I., Kruislaan 413
NL-1098 SJ Amsterdam, The Netherlands

[3] Siemens AG, Gunther-Sharowsky-Str. 2
P.O. Box 3240, D-8520 Erlangen BRD

[4] Philips Usfa B.V., Meerenakkerweg 1
NL-5600 MD Eindhoven, The Netherlands

[5] Dept. of Mathematics, Aarhus University
DK-8000 Aarhus, Denmark

[6] PTT Dr. Neher Laboratories, P.O. Box 421
NL-2260 AK Leidschendam, The Netherlands

ABSTRACT

The first aim of this paper is to situate the call for integrity and authentication algorithms within research on cryptography and within evolution of telecommunication. Motivations for submitting primitives and details on the submission process are also given.

I . BACKGROUND AND DIFFICULTIES IN STANDARDIZING CRYPTOGRAPHIC TECHNIQUES

Last year an interesting collection [1-6] of status reports on cryptography appeared in the proceedings of IEEE. These papers contain more details on a number of important issues like Kerckhoff's assumption (the security of a cipher must entirely reside in the secret key), secret and open research in cryptology,

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 267-271, 1990.

the status of cryptanalysis, standardization efforts, controversy and public acceptance.

In this context it is important to mention that widespread use of cryptography in an open network requires interoperability, and hence some standardization. Such standardization of public algorithms can then be combined with a public scientific evaluation and may lead to wide acceptance, which again stimulates the market. On the other hand, the public nature of the algorithms and their widespread use increases the visibility and the target and hence will attract more attacks. In the international scientific community as present at Crypto and Eurocrypt it is generally agreed that open research on cryptography should produce secure and practical algorithms that can withstand even massive attacks. The DES is such an algorithm that has been analysed extensively and is widely used and standardized [2]. There is a general consensus today that DES is a rather good algorithm with an unfortunately small key [1]. If such algorithms are used internationally for data confidentiality, however, there may be a conflict with national interests [1,7].

II . A BREAKTHROUGH IN EUROPEAN TELECOMMUNICATION

By 1992 the European Community plans to set up a unified European market of about 300 million customers. In view of this market integrated broadband communication (IBC) is planned for commercial use in 1995. This IBC will provide high speed channels (64 kbps, 2 Mbps and more) of image, voice, sound and data communications and will support a broad spectrum of services like telex, telefax, telephony, teletex, videotex, electronic mail, telenewspaper, teleconferencing, videoconferencing, cable TV, telebanking, teleshopping, home banking, EFT, POS, mobile telephony, paging, alarm service, directory services, etc. These services can be home based, office based, (private or public) manufacturing or mobile. They may include dialogue service or messaging or retrieval or a distribution service.

It is clear that the majority of these services offered in future networks are crucially dependent on cryptography for security. Figure 1 indicates the relationship between on the one hand the cryptographic algorithms and their modes of use, and on the other hand the security mechanisms, security services and applications as they are desired in IBC. Data confidentiality is not always required, but integrity is needed for authentication, non repudiation, access control etc.

In order to pave the way towards commercial use of Integrated Broadband Communications (IBC) in Europe by 1995, the commission of European commu-

nities has launched the RACE program (Research and development in Advanced Communications technologies in Europe) [8,9]. Under this RACE program pre-competitive and pre-normative work is going on. After a RACE definition phase (1 January 1986 to 31 December 1986) several RACE projects have started at the end of 1987. Within RACE, the RIPE project (RACE Integrity Primitives Evaluation) will put forward an ensemble of techniques to meet the anticipated integrity requirements of IBC. The members of the RIPE project are: Centre for Mathematics and Computer Science, Amsterdam (prime contractor); Siemens AG; Philips Usfa BV; PTT Research, The Netherlands; Katholieke Universiteit Leuven; Aarhus University.

The project's motivation is the unique opportunity to attain consensus on openly available integrity primitives for the future IBC communication network.

III . THE RIPE CALL FOR INTEGRITY PRIMITIVES

In RIPE, it is advocated that the best way to achieve wide acceptance for a collection of algorithms for integrity and authentication is by an open call for such algorithms, similar to the call in the U.S., which has produced DES. These submissions will then be evaluated by RIPE. The project has put significant effort in creating the optimal conditions for standardization of integrity primitives. The scope of the project and the evaluation procedure were fixed after having reached consensus with the main parties involved. Also there is a cooperation between the RIPE project and the two other RACE projects on integrity (working on the functional specification of integrity and on techniques for integrity mechanisms, respectively). Therefore it is the project's firm belief that this work will lead to European standardization.

Submissions can be any digital integrity primitive, from conventional hash functions, one-way functions and message authentication algorithms, through digital signature techniques, all the way to protocols for providing security services. The scope excludes data confidentiality. Direct benefits for algorithm proposers are expected to include: lead time to develop implementations, retention of intellectual property protection and possible European standardization. Moreover the submitted integrity primitives will be treated confidentially during the evaluation. In exchange, those submissions finally selected must be made public and available for use in IBC on a non-discriminatory, but not necessarily royalty-free basis within the EEC.

In view of the potential use in IBC the submissions will be evaluated with respect to three aspects: functionality, modes of use, and performance. The evaluation will comprise computer simulation, statistical verification, and analysis of mathematical structure, particularly to verify their integrity properties.

All requests for further information and for the mandatory submission kits should be addressed to: Gert Roelofsen, PTT Research; P.O. Box 421; 2260 AK Leidschendam; The Netherlands; Telephone +31(70)332 64 10; Telex 311236 prnl nl; Fax +31(70)332 64 77; email g_roelofsen@pttrnl.nl. Apart from detailing the required form of submission, administrative information and formal procedures, the kit states some general conditions for submitting an integrity primitive and describes the RIPE project's commitments with respect to the confidentiality of submissions. The deadline for submissions is September 15, 1989. The evaluation results will be available by the end of 1990.

In conclusion, it is important to mention that the widest possible encouragement to submit should be given to individuals as well as companies, both within and outside the European Community. At the macro-economic level, this call provides a unique occasion for the international scientific community to see its work used widely, in accordance with an open scientific approach. At the micro-economic level it provides some direct benefits to submitters.

REFERENCES

[1] Massey J., "An introduction to contemporary cryptology", *Proc. IEEE*, Vol. 76, no. 5, May 1988, pp. 533-549.

[2] Smid M.E. and Branstad D.K., "The data encryption standard: past and future", *Proc IEEE*, Vol. 76, no. 5, May 1988, pp. 550-559.

[3] Diffie W., "The first ten years of public-key cryptography", *Proc. IEEE*, Vol. 76, no. 5, May 1988, pp. 560-577.

[4] Brickell E. and Odlyzko A., "Cryptanalysis: a survey of recent results", *Proc. IEEE*, Vol. 76, no. 5, May 1988, pp. 578-593.

[5] Simmons G., "A survey of information authentication", *Proc. IEEE*, Vol. 76, no. 5, May 1988, pp. 603-620.

[6] Abrams M.D. and Powell H.D., *"Tutorial computer and network security"*, IEEE Computer Society Press, Los Angeles 1987.

[7] OTR100, *"Draft RACE Workplan"*, Commission of the European Communities, 1987, Rue de la Loi 200, B-1049, Brussels, Belgium.

[8] OTR200, *"RACE Workplan"*, Commission of the European Communities, 1988, Rue de la Loi 200, B-1049, Brussels, Belgium.

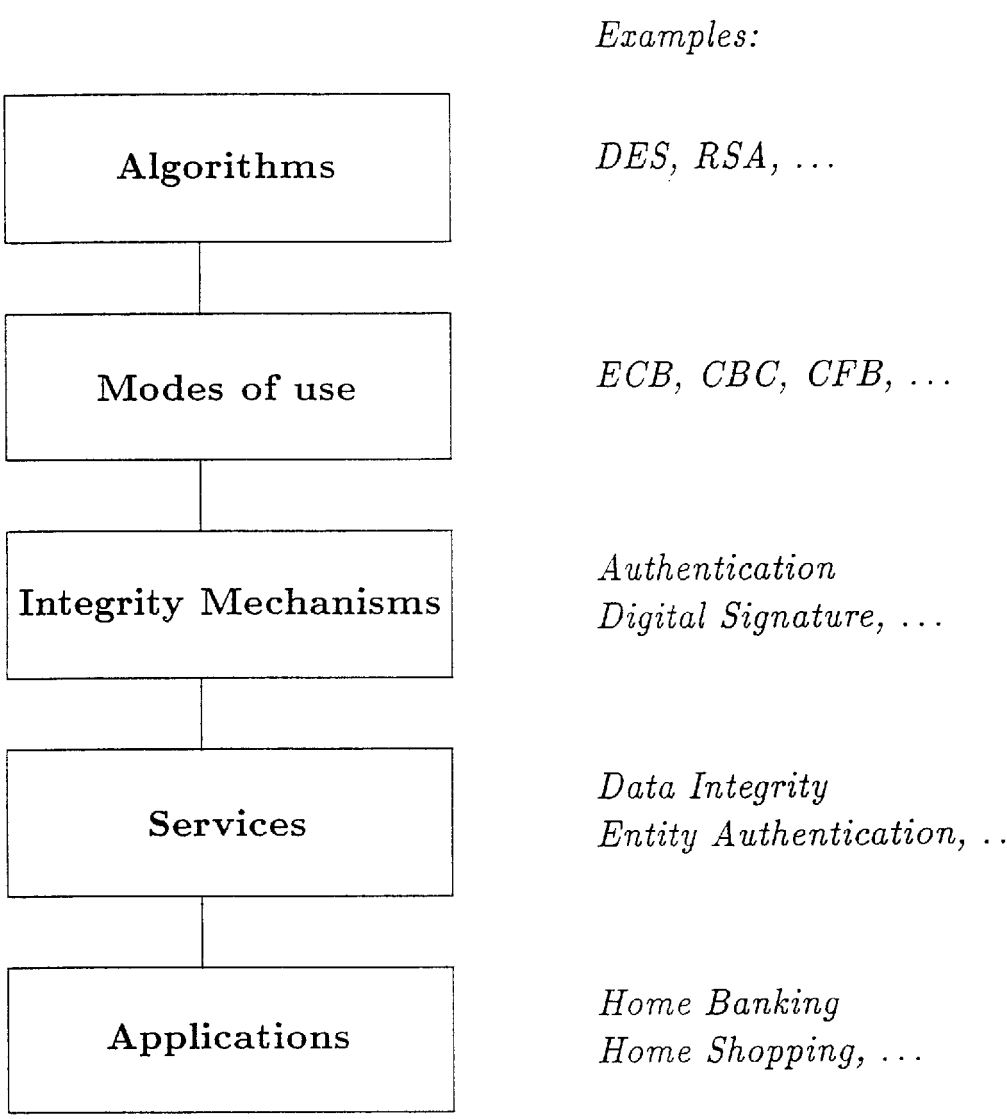

Figure 1. Security architecture and relationship with modes of use and cryptographic algorithms