Symposium on Theoretical Aspects of Computer Science 2010 (Nancy, France), pp. 33-34
www.stacs-conf.org

MATHEMATICS, CRYPTOLOGY, SECURITY

JACQUES STERN [1]

[1] Professor, Department of Computer Science, Ecole normale suprieure,
Chairman, Agence nationale de la recherche
E-mail address: Jacques.Stern@ens.fr

Abstract. In this talk, I will review some of the work performed by the research community in cryptology and security since the invention of public key cryptography by Diffie and Hellman in 1976. This community has developped many challenging lines of research. I will only focus on some of these, and moreover I will adopt an extremely specific perspective: for each chosen example, I will try to trace the original mathematics that underly the methods in use.

Over the years, maybe due to my original training as a mathematician, I have come to consider that linking recent advances and challenges in cryptology and security to the work of past mathematicians is indeed fascinating.

The range of examples will span both theory and practice: I will show that the celebrated RSA algorithm is intimately connected to mathematics that go back to the middle of the XVIIIth century. I will also cover alternatives to RSA, the method of "provable security", as well as some aspects of the security of electronic payments.

Key words and phrases: Mathematics, Cryptology, Security.

27th Symposium on Theoretical Aspects of Computer Science, Nancy, 2010
Editors: Jean-Yves Marion, Thomas Schwentick
Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany
Digital Object Identifier: 10.4230/LIPIcs.STACS.2010.2441