UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII Dipartimento Ingegneria Informazione

Seminar Announcement

Wednesday February 12, 14:30
Engineering building, room 160/2

The Discrete Logarithm Problem (DLP) and its Generalization to the Semigroup Action Problem (SAP)

Joachim Rosenthal
University of Zurich

The Discrete Logarithm Problem (DLP) in a group has been a cornerstone of modern cryptography. In this overview talk we first show that it is possible to relax the group axioms to consider semigroups and Moufang loops to study the DLP problem.

Then we concentrate on the Semigroup Action Problem (SAP) which vastly generalizes the DLP. This general concept was introduced by G. Maze, C. Monico and the speaker in 2002. It encompasses many group based public key protocols currently under intense investigation. It turns out that when the acting semigroup is abelian one readily can build a key exchange as well as onway trapdoor function. For general semigroup actions (not necessarily commutative) one still can create a zero knowledge proof and hence a digital signature protocol.

The last part is devoted to construction techniques of interesting semigroup actions starting from semirings. Tropical semirings have been employed by J. Chen, D. Grigoriev and V. Shpilrain. In this talk we concentrate on congruence-simple finite semirings which were classified by J. Zumbrägel in 2008.

For further information please contact Prof. Marco Baldi (m.baldi@univpm.it)