Call for Papers
SantaCrypt 2009

3 – 4 December, 2009, Prague, Czech Rep.
http://mkb.buslab.org

Intro

Santa's Crypto Get-Together (SantaCrypt) started in December 2001 as the first annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security. This get-together of experts is organised in order to foster exchange of information and ideas on past, ongoing, and also future projects. We recognise the need of experts meeting their colleagues without the hassle of taking care of their (potential) customers, bosses and other distracting forces. ;-) The workshop is run in English in the first day and then Czech and Slovak the second day.

There will be five invited lectures:

- Kenny Paterson (Royal Holloway, UK): *Cryptography and secure channels*.
- Paul Leyland (Cepia Technologies, CZ): *Use of Graphics Processing Units in cryptography*.
- Otokar Grošek (Slovak University of Technology): *Latin squares and cryptography*.
- Vlastimil Klíma (independent cryptologist, Prague, CZ): *SHA-3, BMW & EDON-R hash functions.*
- Pavel Vondruška (Telefónica O2 Czech Republic): *Development of cryptographic devices in the Czechoslovak Republic.*

Detailed information, including registration guidelines, will be available in the due course on workshop web pages: http://www.buslab.cz/mkb.

Instructions for Authors

The program committee will accept submissions targeting cryptanalysis, applied cryptography, security applications of cryptography and other related areas. Proposals should be of 5-15 pages and formatted for anonymous evaluation (no names of authors or apparent references), and they will be accepted in two tracks – KEYMAKER (students) and standard track. Word and LaTeX templates for submissions are also available from the workshop web: http://mkb.buslab.org. Submissions can be written in Czech, Slovak, or English.

Submissions should be mailed to matyas AT fi.muni.cz, and clearly marked either KEYMAKER or STANDARD TRACK. The final deadline for the submissions is *30th September 2009*. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by *30th October*. Camera-ready versions for the workshop proceedings have to be delivered by *19th November*.

Important Dates

Submission deadline: 30th September, 2009
Acceptance/rejection notification: 30th October, 2009
Camera-ready format: 19th November, 2009
Workshop: 3rd – 4th December, 2009

Program Committee

Jan Bouda, Masaryk U., Brno, Czech Republic
Petr Hanáček, Brno U. of Technology, Czech Republic
Vashek Matyáš, Masaryk U., Brno, Czech Republic – Chair
Štefan Porubský, Academy of Science, Prague, Czech Republic
Zdeněk Říha, Masaryk U., Brno, Czech Republic
Luděk Smolík, Siegen, Germany
Jiří Tůma, Charles U., Prague, Czech Republic
Jozef Vyskoč, VaF, Rovinka, Slovakia