Call for Papers
SantaCrypt 2008

4 – 5 December, 2008, Prague, Czech Rep.
http://www.buslab.cz/mkb

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:

- Eli Biham (Technion, Haifa, Israel): *On the (in)security of the ciphers and protocols of GSM*.
- Richard Clayton (University of Cambridge, UK): *Can cryptography secure the Internet?*
- Jozef Gruska & Jan Bouda (MU, Brno): *New directions in quantum cryptography.*
- Martin Hlaváč & Tomáš Rosa (UK, Praha & e-banka): *Towards disclosing the RSA private key of an e-passport.*
- Zdeněk Říha (MU, Brno): *On security and crypto issues of e-passports.*

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://www.buslab.cz/mkb. 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 2008*. Submissions will be evaluated by the program committee and authors will be informed about the evaluation results by 21st October. Camera-ready versions for the workshop proceedings have to be delivered by 18th November.

Important Dates

Submission deadline:	30th September, 2008
Acceptance/rejection notification:	21st October, 2008
Camera-ready format:	18th November, 2008
Workshop:	4th – 5th December, 2008

Program Committee

Dan Cvrček, Technical U. & Masaryk U., Brno, Czech Republic

Vlastimil Klíma, independent cryptologist, Czech Republic

Vashek Matyáš, Masaryk U., Brno, Czech Republic – Chair

Zdeněk Říha, Masaryk U., Brno, Czech Republic & JRC Ispra, Italy

Martin Stanek, Comenius U., Bratislava, Slovakia

Luděk Smolík, Masaryk U., Brno, Czech Republic & Germany

Pavel Vondruška, Telefónica O2 & Charles U., Prague, Czech Republic