Call for Papers: Special Issue on Applied Cryptography & Data Security

Journal of "Computacion y Sistemas" ISSN 1405-5546
National Polytechnical Institute of Mexico
Special Issue on January-March, 2009.

Important Dates

Manuscript submission deadline: March 1, 2008
Notification of Acceptance: June 13, 2008
Camera-ready manuscript due date: August 15, 2008
Publication: Issue January-March, 2009

Journal of "*Computacion y Sistemas*" seeks original manuscripts in English for a Special Issue on Applied Cryptography & Data Security scheduled to appear in the January-March issue of 2009. **Computacion y Sistemas (CyS)** is a quarterly published journal devoted to circulate original scientific and technological contributions in the field of Computer Science.

Cryptography provides techniques, mechanisms, and tools for private and authenticated communication, and for performing secure and authenticated transactions over the Internet as well as other open networks. It is highly probable that each bit of information flowing through our networks will have to be either encrypted and decrypted or signed and authenticated in a few years from now. Hence, it is fair to say that data security of digital systems largely depends on cryptography, since advances in cryptography make computer systems more secure/reliable.

The goal pursued in this Special Issue is to create a volume of recent work on advances in all aspects of cryptography and cryptanalyis as well as sound security applications. The particular topics which are of interest for this special journal issue include, but are not limited to the following topics:

- Symmetric cryptography
- Block ciphers
- Modes of operations
- Stream ciphers
- Hash functions
- Message Authentication Codes

- Boolean functions suitable for crytographic applications
- Public key cryptography
- Pairing based cryptography
- Random number generators
- Computer Arithmetic
- Efficient implementation of cryptographic algorithms
- Cryptanalysis
- Side-channel attacks
- Security Applications
- Secure Protocols
- Public Key Infrastructure
- Denial of Service
- Zero Knowledge Proofs
- Multy-party Computation
- Quantum Cryptography

Articles to be submitted to **CyS** must not have been previously published or simultaneously submitted to other journals, congresses, etc. If the article has already been presented, submitted or published elsewhere, the guest editors must be notified about it. The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. The length of the submission should be at most 20 pages including bibliography and appendices. It should use at least 10-point fonts and have reasonable sized margins. General guidelines for authors can be found in,
http://www.ejournal.unam.mx/normas.html?r=7&liga=4
Please submit full papers in PDF to:

Francisco Rodríguez-Henríquez
francisco@cs.cinvestav.mx

Debrup Chakraborty
debrup@cs.cinvestav.mx

Computer Science Department
CINVESTAV-IPN
Av. Instituto Politcnico Nacional No. 2508
Col. San Pedro Zacatenco.
07300 México, D. F.,
MÉXICO
Tel: (+52 55) 5061 3800 x 3758 y 3756
Fax: (+52 55) 5061 3757