For Your Information

DMS Employment Opportunities

Several of the technical staff of the Division of Mathematical Sciences (DMS) of the National Science Foundation (NSF) serve one- to two-year visiting scientist or Intergovernmental Personnel Act appointments as program directors while on leave from universities, colleges, industry, or national laboratories. Since the timing of these positions is staggered, the division continually seeks talented applicants. In 2001 the division will be seeking to make appointments in all areas. Permanent program director appointments will also be considered.

The positions involve responsibility for the planning, coordination, and management of support programs for research (including multidisciplinary projects), infrastructure, and human resource development for the mathematical sciences. Normally this support is provided through merit-reviewed grants and contracts that are awarded to academic institutions and nonprofit, nonacademic research institutions.

Applicants should have a Ph.D. or equivalent training in a field of the mathematical sciences, a broad knowledge of one of the relevant disciplinary areas of the DMS, some administrative experience, a knowledge of the general scientific community, skill in written communication and preparation of technical reports, an ability to communicate orally, and several years of successful independent research normally expected of the academic rank of associate professor or higher. Skills in multidisciplinary research are highly desirable. Qualified women, ethnic/racial minorities, and/or persons with disabilities are strongly urged to apply. No person shall be discriminated against on the basis of race, color, religion, sex, national origin, age, or disability in hiring by the NSF.

Applicants should send a letter of interest and a vita to Bernard R. McDonald, Executive Officer, Division of Mathematical Sciences, National Science Foundation, 4201 Wilson Boulevard, Suite 1025, Arlington, Virginia 22230; telephone 703-292-4851; fax 703-292-9032; e-mail: `bmcdonal@nsf.gov`.

—NSF announcement

Departments Again Coordinate Job Offer Deadlines

Once again this year, a group of mathematical sciences departments will coordinate their deadlines for acceptance of postdoctoral job offers. The purpose is to ensure that applicants do not have to make decisions about job offers before the results of the National Science Foundation postdoctoral fellowship competition are announced.

The departments have agreed not to require applicants who are less than two years past the Ph.D. to decide on a job offer before Monday, February 12, 2001. The agreement affects offers of postdoctoral positions, not tenure-track offers. The list of participating departments, together with additional information, may be found on the Web at `http://www.ams.org/employment/postdoc-offers.html`.

—Allyn Jackson

Oral History Project in Mathematics

The 1930s saw the flowering of a unique mathematical community in Princeton. This community was unlike any other in America before that time and perhaps afterwards and had an important influence on American mathematics. Half a century later, in 1984, one of the original participants, Albert Tucker, decided to capture on tape some of the personal reminiscences of the remaining survivors of the period. The tapes were transcribed and organized into a body of written transcripts. Unfortunately this document existed only in a few copies and was not very accessible to the public.

In 1999 Robert Jantzen, a former Princeton undergraduate and Ph.D. advisee of one of the mathematicians from that decade, Abraham H. Taub, stumbled upon this oral history project. It seemed clear that the World Wide Web was the natural way to make the material available. The resulting Web-enhanced online version is now available at `http://www.princeton.edu/mudd/math`.

—Robert Jantzen, Villanova University

Advanced Encryption Standard Choice Is Rijndael

In 1977 the National Bureau of Standards (now the National Institute of Standards and Technology, or NIST) adopted an IBM-designed cipher that encrypted 64-bit blocks under 56-bit keys as the Data Encryption Standard (DES). This launched the career of one of the most widely used encryption algorithms. But with only 56 bits of key, DES is now obsolete. In its place many people are now using triple-DES, a multiple version of an algorithm that does not perform particularly well. So in 1997 NIST announced a competition for an Advanced Encryption Standard (AES), an algorithm with 128-bit blocks and 128-, 192-, and 256-bit keys to replace DES. NIST sought a symmetric-key algorithm for "sensitive, unclassified" information. The chosen algorithm would have to be available royalty-free worldwide. Winners would get fame and glory—and probably a lot of consulting. And AES would undoubtedly become one of the most widely used cryptographic algorithms in the world.

In 1998 twenty-one industry and academic groups offered candidates; fifteen met NIST's submission criteria. In August 1999 NIST picked five finalists: MARS, RC6, Rijndael, Serpent, and Twofish (as the algorithms were known by their creators). The finalists reflected cryptography's internationalism: designers of the finalists hailed from more than a half dozen countries. On October 2, 2000, NIST announced its choice for the Advanced Encryption Standard: Rijndael (pronounced "Rhine Dahl"), an algorithm developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.

Rijndael should appeal to mathematicians; the cryptosystem is quite algebraic. Rijndael repeats rounds, with the number of rounds determined by key size. In the 128-bit key version, Rijndael runs for 10 rounds. As specified in the call for algorithms, Rijndael operates on a 128-bit block of data. It divides the block into sixteen 8-bit bytes and treats these as elements of $GF(2^8)$, defined by the polynomial $x^8+x^4+x^3+x+1$, which is irreducible over $Z/2Z$. The data are placed in a 4×4 array, and all operations occur on the bytes of the array.

Each round consists of four operations: one transforms the bytes, one tranforms the rows, one transforms the columns, and one adds in the key. First, each of the bytes is modified by maps easily described in the arithmetic of $GF(2^8)$: inversion (with zero mapped to itself) and an affine transformation; then the rows of the array are shifted circularly, with the bytes of row i moving $i-1$ locations to the right. Next the bytes in each column are mixed by multiplication: view the column elements as coefficients of a polynomial of degree 3, and multiply this polynomial by $3x^3+x^2+x+2$ modulo x^4+1. The last operation is an XOR of the key bits with the elements of the array.

The polynomials used for the field arithmetic were determined by two criteria: arithmetic efficiency and resistance to cryptanalytic attack. Though DES was first cracked by brute-force attack that searched the entire key space, linear and differential cryptanalysis are serious attacks on the security of the algorithm. Rijndael's multiplicative map and affine transformation were chosen for their ability to resist these. The polynomial $3x^3+x^2+x+2$ was picked for its combination of fast multiplication and diffusion power. (Diffusion is spreading changes in key or text bits into the cipher text.)

NIST's evaluation used published research from academic and industry experts and private advice from the National Security Agency (NSA). NIST based its decision on security, efficiency, and "algorithm and implementation" characteristics (including hardware and software suitability and simplicity). Security is difficult to assess. The breaking of an algorithm is clear, but there are no proofs of security, only proofs that an algorithm passes the tests we currently know to perform. By contrast, results of efficiency tests, even though only using current technology, provide more definitive information. Efficiency tests were conducted in a variety of venues, including fast implementations in C^{++}, Java, assembler code, FPGAs (Field Programmable Gate Arrays) and ASICs (Application Specific Integrated Circuits).

All finalists were fine on these measures, but some were finer than others. Why did NIST pick Rijndael? NIST judged the submission to be "the best overall algorithm for the AES…Rijndael's combination of security, performance, efficiency, implementability, and flexibility make it an appropriate selection for the AES."

Rijndael's cryptographic complexity rests on *several* well-studied cryptographic transformations, and the algorithm is easy to describe. The algorithm performs efficiently on a variety of platforms (NIST noted that it was a "good performer in hardware and software across a wide range of computing environments"), and the algorithm is relatively easy to defend against power and timing attacks. There were some comments that the polynomials chosen for Rijndael's primitives might lead to breaks. But $GF(2^n)$ is a field that NSA knows well, and it is fair to assume that Rijndael passed NSA's tests.

The process is not yet over. The AES selection has to undergo a public comment period, which should run through February 2001 (see `http://aes.nist.gov/` for more details). But if all goes according to plan, in late spring Rijndael, invented by two Belgians and vetted through a worldwide effort, will become the U.S. Advanced Encryption Standard.

(For more information and further references on DES and the AES process and candidates, see Susan Landau, "Standing the Test of Time: The Data Encryption Standard", *Notices*, March 2000, and "Communications Security for the Twenty-First Century: The Advanced Encryption Standard", *Notices*, April 2000.)

—Susan Landau, Sun Microsystems

Correction to Backlog

The backlog information for *ESAIM Probab. Statist.* was omitted from the "Journal (Electronic)" section of the "Backlog of Mathematics Research Journals" which appeared in the September 2000 issue of the *Notices*, pages 915–918. Number of articles posted in 1999—8; 1999 median time (in days) from: submission to final acceptance—460, acceptance to posting—109; formats: pdf, ps, dvi.