CCSU
Central Connecticut State University

Department of Computer Science Lecture

March 6th 2012 3:05-4:20 pm Copernicus 210

Algorithms and Software Tools for Learning Mathematical Fundamentals of Computer Security with demonstration of the Java Applets

Vladimir V. Riabov, Ph.D.

Rivier College, 420 S. Main Street
Nashua, NH 03060-5086

ABSTRACT: Java applet-based tools were developed for exploring mathematical foundations of computer security techniques (that are not often taught, or inadequately covered, in CS curricula) including sets, permutations, combinations, and probability; number theory (divisibility, primes, groups, rings, and Galois fields); modular arithmetic; authentication algorithms, and hashes. The tools could be used by students to examine cipher puzzles, MonoAlphabetic and shift substitution ciphertexts, Playfair and Vigenère ciphers, message digests, digital signatures, and public key cryptosystems. In an attempt to overcome the common "Math-phobia" of students, some standard statistical/probability problems were re-cast using scenarios that were more 'security-related', and perhaps more in keeping with current events: "CIA Hiring"; "Delta Force"; and "Ethnic Dispute". Prior basic knowledge in Discrete Mathematics, Computer Organization and Networking Technologies would help students follow the lecture.

BRIEF BIOGRAPHY: Dr. Vladimir V. Riabov is a professor and director of Computer Science programs at Rivier College, Nashua, NH. He published more than 120 journal articles and conference papers on Networking Technologies, Computer Security, Computational Algorithms, Code Testing, and Hypersonic Flows. Vladimir received a Ph.D. in Mathematics and Physics from Moscow Institute of Physics and Technology and M.S. in Computer Information Systems from Southern New Hampshire University.

E-mail: vriabov@rivier.edu
Web: http://www.rivier.edu/faculty/vriabov/