1 Integrity and Security of Information

The integrity, security and privacy of electronic information encompass aspects of computer security, computer engineering, computer science, law, psychology, sociology, and mathematics. We are proposing the establishment of an academic cluster in coding, integrity and secure transmission of electronic information. We will present, in broad strokes, a few of the current compelling, interdisciplinary themes of the proposed area, along with some of the impact on information technology, economic development, and educational infrastructure. If interest warrants, these general themes can later be given a more detailed structure for what might be done at LSU.

Information integrity and security involve creating algorithms for the correct transmission of data across noisy channels (error-correction) as well as protocols for encrypting data for quick transmission (Fast Fourier Transform), protocols for privacy (public-key cryptosystems, currently based on the difficulty of factoring large numbers), protocols for verifying authenticity (signature schemes), and algorithms for detecting intrusion. The mathematical underpinning of all of this is the study of finite fields and group theory; today the subject has gotten quite sophisticated, using elliptic curves, abelian varieties, and modular forms, subjects that in the recent past were the stuff of pure mathematics. There is every reason to think that these connections will grow rapidly; more and more texts in application areas are appearing trying to explain just enough of these advanced topics so that the technological expertise of the next generation of technology is enhanced. We propose that LSU become more actively involved in the creation of this expanding interface between Algebra and the Information Age.

As an example of what can be done in this area, Purdue University recently established CERIAS, their Center for Education and Research in Information Assurance and Security. Its mission statement is: "To establish an ongoing center of excellence, which will promote and enable world class leadership in multidisciplinary applications to information assurance and security research and education. This collaboration will advance the state and practice of information security and assurance. The synergy from key members of academia, government, and industry will promote and support projects of research, education, and community service." Sponsored by major corporations such as Cisco Systems, Lilly, Sun, Citigroup, Hewlett-Packard, Intel, Lockheed-Martin, Microsoft, TRW, and Raytheon, CERIAS staff includes distinguished Purdue faculty in Computer Science, Electrical and Computer Engineering,

English, Linguistics, Industrial Engineering, Computer Science Technology, Political Science, Psychological Sciences, and Sociology. Several of the Computer Science faculty are mathematicians trained in classical number theory. Their program involves all aspects of computer security, including psychological profiling of potential hackers, and political and sociological aspects computers, including privacy issues. CERIAS has K-12 programs in the local Indiana schools, has graduate students, many from math, has many projects and awards.

Although we are not proposing that LSU duplicate the efforts of CERIAS, we believe there are many opportunities to do something in this general area. There are already faculty within LSU whose expertise impinge on the safe and secure transmission of information and related societal issues. Coding theory courses have been taught in Electrical Engineering and Mathematics. The Mathematics department has an international recognized group of faculty in algebraic number theory, a theoretical field of great importance to understanding current methodologies. The Office of Computer Services is working directly with the FBI on issues of everyday computer security.

By fostering an initiative focused on the issues of information integrity and security, we feel that LSU would be able to make a strong contribution to this burgeoning area, would provide a forum in which LSU engineers, computer scientists, mathematicians and social scientist could work together in development of these applications and would make a direct and immediate toward the goals of Vision 2020.