University of Lethbridge

MATHEMATICS & COMPUTER SCIENCE

Speaker: **Dr. Hugh Williams**
Mathematics & Statistics, University of Calgary
iCORE Chair, Algorithmic Number Theory & Cryptography

Title: **Privacy & Encryption: A Personal View**
iCORE Distinguished Lecture Series via videolink

Date: **Wednesday, November 13th**

Time: **4:00 p.m. in B660**

ABSTRACT
The rapid and uncontrolled proliferation of various communication devices and media has had the unfortunate consequence of a steady and profound erosion of personal privacy. While any attempt at giving a definition of privacy will invariably fail, we all have an instinctive understanding of what is meant by the term; however, it is often far more than what we believe. One of the most striking features about privacy is the way it is over venerated in summary form and then under-valued in the detail. One of these details is information privacy. Control over who knows what about us, for what purposes, and to whom it is disclosed, is the main concern of this dimension of privacy. In the e-world, personal information is in a very real sense the person. Thus, it is essential that we have confidence in the capacity of the information collector to secure our personal information. This can only be achieved through the very technology that threatens our privacy. One important ingredient in these privacy-enhancing technologies is cryptography.

Briefly put, cryptography is the study and development of techniques for rendering information unintelligible to all but intended recipients of that information. If a sender and receiver of a message wish to communicate over an insecure channel (mobile phone, internet) and want to ensure that no other unauthorized party can read their transmission, they will make use of a particular cryptosystem. A conventional cryptosystem can be thought of as a large collection of transformations (ciphers), any one of which will render the original message (plaintext) to unintelligible ciphertext, but in order for the receiver to read the message, he must know which particular transformation was used by the sender. The information that identifies the transformation used by the sender is called the key. It is important to point out that if an eavesdropper gets hold of some message and its encrypted equivalent, he should not be able to extract the key from this information. Nor should the system be vulnerable to an adaptive attack; such attacks make use of information previously acquired to obtain new information from the sender and so on until the system is broken. This is what makes cryptography fascinating. How can we protect our communications against these kinds of attacks? Remember also that a good cryptostystem must resist an attack even from the inventor of the system.

In this talk, which is intended for a non-specialist audience, I will describe several features both of privacy and modern encryption.

I will conclude with a discussion of some of the current and future activities of the iCORE Chair in Algorithmic Number Theory and Cryptography (ICANTC) team.

SHORT BIOGRAPHY

Hugh Williams (BSc, 1966; MMath, 1967; PhD, 1969, University of Waterloo) came to Calgary in September of 2001 from the University of Manitoba, where he was Associate Dean of Science for Research Development and Professor in the Department of Computer Science. He is also an Adjunct Professor in the Department of Combinatorics and Optimization at the University of Waterloo. He was appointed the Alberta Informatics Circle of Research Excellence Chair in Algorithmic Number Theory and Cryptography (ICANTC) in the Department of Mathematics and Statistics at the University of Calgary. His extensive research and leadership background, coupled with a strong international reputation in cryptography and number theory, provides the foundation for building a Western Canadian focal point in pure and applied cryptography. This will be utilized to investigate the high-end theoretical foundations of communications security. Professor Williams' research is specifically aimed at the development, improvement and implementation of mathematically based cryptosystems. He was one of the first to use modern mathematical techniques for securing and authenticating communication, and he has developed a widely used public key cryptosystem. He has authored over 130 refereed journal papers, 20 refereed conference papers, 20 books or book chapters, and he has served for almost 25 years as an Associate Editor of Mathematics of Computation, the most prestigious journal of computational mathematics.

ALL ARE WELCOME