HOW TO EXCHANGE SECRETS – COMMUNICATION OF CRYPTOGRAPHIC KEYS

RENATE SCHEIDLER

ABSTRACT. Conventional (one-key) cryptographic systems, such as the Data Encryption Standard (DES) or the new Advanced Encryption Standard (AES), are the preferred secure communication schemes for many applications. This is because they are both fast and sufficiently secure for most applications. The real difficulty in employing such cryptosystems is the problem of securely transmitting a secret cryptographic key between communicants. This talk describes a solution to this problem – a means by which a secret key can be safely transmitted across an insecure channel. Our key exchange protocols are based on the algebra and arithmetic of reduced principal ideals in a real quadratic number field.

This research was conducted in collaboration with H. C. Williams and M. J. Jacobson, Jr., both at the University of Calgary, and J. A. Buchmann at the Technical University of Darmstadt, Germany.

Despite the quite algebraic and number theoretic nature of this topic, this presentation is designed to be accessible to a general mathematics-trained audience.