International Conference on Applications of Computer Algebra July 19-22, 2007

Coding Theory and Computer Algebra Systems:
From DTMF to RSA and Beyond

Chen-Han Sung

Texas A&M International University
Email: drsung@tamiu.edu

Abstract

Touch-tone telephone dialing and message exchanging through electronic communications are examples of everyday use of coding theory. Today, the Dual Tone Multi-Frequency (DTMF) system is the basis for touch-tone telephone dialing, while the Rivest-Shamir-Adleman (RSA) scheme is the most widely accepted public key cipher over telephone lines and satellite links.

The DTMF minimizes data corruption and the RSA makes data visible only to the desired party. Those represent the two central issues in data communication. Both are cared by proper coding.

Using computer algebra systems allows students to concentrate on the mathematical ideas and not be distracted by the symbolic-numeric computations involved. Computer algebraic systems are also used in research and under further development on themselves. When dealing with the coding theory at junior, senior, and graduate levels, those aspects are even more apparent.

Algorithms, examples (such as DTMF, RSA, etc.), technology tools, and some issues on using computer algebra systems for algebraic computations and approximate computations in coding theory will be presented. The possibility to avoid long and/or tedious computations and to improve concept understanding during the teaching and learning processes will be discussed.