1035-G1-293 **Cheryl Beaver*** (beaverc@wou.edu), 345 N. Monmouth Ave., Monmouth, OR 97361.

Zero-Knowledge Proofs: How to convince someone you know everything without telling them anything.

From the simple example of Ali Baba proving he knows a magic word to complex digital signature schemes, the ideas behind zero-knowledge protocols can be used as fun cryptographic examples for undergraduate students at different levels. A zero-knowledge proof is a probabilistic proof in which one party called the Prover convinces another party called the Verifier that they know a certain fact. The Prover's attempt at a proof generally takes the form of an interactive challenge-response protocol. Once the protocol is complete, the Verifier decides whether to accept or reject the proposed proof. If accepted, the Verifier believes the Prover indeed knows the fact, but learns nothing about that fact. The ideas behind a zero-knowledge proof are relatively simple and are accessible to any student with an elementary understanding of probability. For more advanced students, the concept can be used to develop identification and digital signature schemes creating an appropriate topic for a number theory course or undergraduate research project. (Received August 30, 2007)