

## **Criptografia e Teoria da Informacao: Um Relacionamento Quente.**

Anderson Nascimento  
(Eng. Elétrica, UnB)

As muitas intersecções entre a teoria da informação e a criptografia são bem representadas na figura de Claude Shannon. Shannon criou Teoria da Informação com a publicação de "A Mathematical Theory of Communication Systems" em 1948 e também foi o primeiro a formalizar o estudo da criptografia e transforma-la de arte em ciência com seu artigo "Communication Theory of Secrecy Systems" em 1949. Nesta palestra, apresentaremos uma visão geral tanto de teoria da informação quanto de criptografia com ênfase nos conceitos matemáticos que têm sido relevantes para o desenvolvimento recente das duas áreas. Particularmente, apresentaremos também as oportunidades de trabalho para matemáticos presentes na fronteira entre essas duas ciências.