Abstract:
I will discuss some basic algorithmic questions in algebra that are crucial for non-commutative cryptography:
1. How can one amplify the hardness of algorithmic problems?
2. What are good scrambling functions?
3. How does compression affect complexity of algorithmic problems?