Abstract: Capacity theory is an area of mathematics which comes from physics yet has many surprising arithmetic applications. Motivated by these applications, Cantor and Rumely generalized the notion of capacity to subsets of adelic points on curves. In this talk I would like to present their theory as a “black box”, and show how one can apply the capacity machine to more concrete problems. In particular, I would like to discuss how capacity theory can be used to understand certain problems in cryptography. This is joint work with T. Chinburg, B. Hemenway and N. Heninger.

(Disclaimer: This talk is not actually designed for engineers)