1147-68-716 **Nadia Heninger*** (nadiah@cs.ucsd.edu), UCSD Computer Science and Engineering, 9500 Gilman Drive, Mail Code 0404, La Jolla, CA 92093-0404. *Fun with the hidden number problem.* Preliminary report.

Let p be a prime, and let α be a secret integer modulo p. In the hidden number problem, one is given many samples of the most significant bits of $t_i\alpha \bmod p$ for random integers t_i, and one wishes to recover the secret α. There are algorithms for solving this problem using lattice techniques and Fourier analysis. In cryptography, these algorithms have found applications in recovering DSA and ECDSA secret keys from side-channel attacks against signature implementations. In this talk, I will report on successfully recovering secret ECDSA keys from cryptocurrency blockchains and network protocols due to implementation mistakes, and report on attempts to clarify bounds for which these techniques can be proven to work. (Received January 28, 2019)