

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 19.

Last time: We discussed the basic theory of the RSA scheme. Today we discussed the upcoming midterm. The outcome of this discussion will be posted on the website. We also covered some classical background on cryptography and cryptanalysis.

We introduced the ciphers in 5.1. The shift cipher, the affine cipher, the substitution cipher can all be decrypted using frequency analysis. We introduced the Vigenère cipher and mentioned that it, too can be deciphered using frequency analysis. We then discussed the Pohlig-Hellman exponentiation cipher.

A one-way function on $U \subset \mathbb{N}$ is a one-to-one function $f : U \rightarrow U$ such that $f(x)$ is easy to compute, but in general $f^{-1}(x)$ is impractical to compute. If $f^{-1}(x)$ becomes easy to compute if some additional special information is known the f is called a *trapdoor one-way function*.

We considered the function $x \rightarrow x^e \pmod{n}$ which is believed to be a one-way function if $n = pq$ is a product of two large primes. We discussed how to use this to produce electronic signatures.