

## Cryptology – F08 – Week 6

### Lecture, February 22

We continue with chapter 5, concentrating on quadratic residuosity and the Jacobi symbol.

### Lecture, February 28

We will continue with chapter 5.

### Lecture, March 3

We will begin on chapter 6.

### Lecture, March 7

We will continue with chapter 6 and cover the McEliece Cryptosystem (copied from the earlier edition of the textbook).

### Problem session March 6

1. Do problems 5.14, 5.18, 5.22, and 5.25 in the textbook.
2. Suppose you, as a cryptanalyst were interested in an RSA modulus  $N$ , and you were given a  $t$  such that  $a^t \equiv 1 \pmod{N}$  for all  $a \in Z_N^*$ . (Note that  $t$  is not necessarily  $\phi(N)$ . In the case  $N = 69841$ ,  $\phi(69841) = 69300$ , but  $t$  could have many other values including 2310 and 138600.)
  - a Give an efficient algorithm for determining the message  $m$  which was encrypted using the public exponent  $e$ , producing the ciphertext  $c$ .
  - b Give an efficient algorithm for factoring  $N$ . (Hint: some ideas from the Miller-Rabin primality testing algorithm may be helpful.)