MATH 295B/395A: CRYPTOGRAPHY
HOMEWORK #7

Problems for all

Problem 1–3. Read Section 15.1 (pages 368–376) of *The Pleasures of Counting* by Koerner, available at

`http://www.cems.uvm.edu/~voight/295/koerner.pdf`.

Do Exercises 15.1.1–15.1.3.

Problem 4. Decrypt the message

`CLV SSH = RDMVE PFZII EAVYS XFTHS FNMOB RRPDH VBSQH`

with the following Enigma settings:

```
Walzenlage (Rotors): I V III
Ringstellung (Ring setting): 13 06 24
Steckerverbindungen (Plug connections): AU PB EF IQ RH ZL DT MS CG KN
```

[Hint: The message is in German!]

Problem 5. Read Section 15.3 (pages 381–390) of *The Pleasures of Counting* (same link) and the Introduction (pages 1–13) of *The Codebreakers* by Hinsley and Stripp, available at

`http://www.cems.uvm.edu/~voight/295/hinsleystripp.pdf`.

How significant was the contribution of Ultra to the victory of the Allies in World War II? Take a clear stand on this question and write a paper (1–2 pages in length) of well-written argumentation.

Problem 6. Read Chapter 4 of *The Code Book* (pages 143–189)—it is a quick read. (No, you don't have to turn anything in.)

Date: Due Friday, 15 October 2010.