MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #6

Problems for all

Problem 1. 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 2. Read *Solving the Enigma* and *The Cryptographic Mathematics of Enigma* at:

```
http://www.nsa.gov/publications/publi00016.cfm
http://www.nsa.gov/publications/publi00004.cfm
```

(a) How did luck contribute to the Allied cryptanalysts' efforts?
(b) Compare the contributions of the Polish, American, and British cryptographers.

Please write roughly 1–2 pages for this question.

Date: Due Wednesday, 15 October 2008.