HONS 195N: CRYPTOGRAPHY
FINAL PAPER

The paper should be **10–15 pages in length**; if your paper is slightly shorter or substantially longer, you will not be penalized. It should have an introduction, a compelling thesis, strong evidence and research, a conclusion, and be extremely well-written. Your target audience for the paper should be an educated reader who is not familiar with the world of cryptography, like a friend from another class; it should be complete and be coherent from start to finish.

You must choose a topic by Wednesday, November 18 and provide a rough outline or sketch (in a paragraph or two) of what you plan to cover. You must also come and talk to me (before or after class, in office hours, or by appointment) so that I can suggest further reading and directions.

You may use any of the standard bibliographic methods of citation, but you must be consistent throughout. You should use primary sources for as much of your research as possible. You are encouraged to contact Patricia Mardeusz `patricia.mardeusz@uvm.edu`, the UVM Libraries Liaison to the Honors College. She will meet with you in individual research consultations: "This is a wildly successful service. I love doing this and the student feedback has been extremely and unanimously positive."

It is *strongly* recommended that you turn in a rough draft of your paper to me before the end of classes—even one only partially finished—so that I can give you feedback. The quality of my comments will be proportional to its completeness and the amount of time that you give me to look at it.

The paper is due **Thursday, December 17, 2009**, at the time of the final exam, 3:30 p.m. Please note that the last day of class is Wednesday, December 9, and that there will be no final examination.

Here are some possible topics; they are meant to be inspirational rather than prescriptive.

- How did the roles of men and women differ at Bletchley Park?
- How did the American cryptographic efforts compare to that of the British and the Polish?
- How did the Allied experience with the Enigma machine shape cryptography after the war?
- How did Turing contribute to collaboration between the US and the UK?
- Describe the Abwehr Enigma machine (used by the military intelligence); were the Allies able to crack it?
- To what extent is it true that Bletchley Park can be located as the source for the modern computer?
- What is the halting problem in computer science, what was Alan Turing's contribution, and how did it naturally arise from his work in Bletchley Park?
- To what extent are German cryptographic efforts a microcosm for the supremacist culture of Nazi Germany?
- Discuss the role of cryptography in a period of literature (e.g. in the work of Edgar Allen Poe).
- What differed between Hut 6 and Hut 8?
- Riff on the Turing Test.
- Give a detailed (political?) analysis of Gordon Brown's apology to Alan Turing.
- What is quantum cryptography? or What is the future of cryptography?
- How did the GC&CS come into being and how was it situated with respect to other intelligence agencies in the UK?
- Why is the problem of integer factorization so difficult?
- ...

Date: 16 October 2009.