

Term Project Assignment

1 Schedule

Thursday, April 1	One-page project proposal due.
Monday, May 3	Final project report due.

2 Requirements

The purpose of the project is to give you a chance to explore in depth a topic that is related to the subject matter of this course. The project consists of two parts. The first part involves scholarly work—exploring a topic, reading relevant literature, proving theorems or possibly writing software and running experiments, and so forth. The second part involves writing a paper describing the results of the first part. The paper should be a 10–15 page essay or report that reflects the substantial amount of work that you put into the first part. The paper should make clear how you approached your topic, what resources you used, what you actually did, and what you learned. It should present your own conclusions and perspectives that you acquired in the course of your work.

The paper will be graded for writing quality as well as for technical content, so attention should be paid to organization, grammar, spelling, and scholarly style. All references used must be properly cited in the bibliography. Any data collected or code written should be attached as an appendix or submitted on-line.

3 Project Suggestions

Almost anything related to the course material is acceptable as a project topic. Because this is a course on *foundations* of cryptography, the main criterion for appropriateness is work that emphasizes provability and high level of rigor as opposed to heuristics and practical considerations. Some examples of appropriate topics are secure function evaluation, bit commitment, oblivious transfer, secret sharing, communication complexity of cryptographic protocols, pseudorandom functions, random oracle model, “black-box” versus “non-black-box” protocols, adversary models, and so forth. Helger Lipmaa maintains a wonderful cryptography web site at <http://www.adastral.ucl.ac.uk/~helger/>. Particularly helpful are his cryptography pointers at <http://www.adastral.ucl.ac.uk/~helger/crypto/>, which form an extensive directory to the cryptography literature.

Much more important than the choice of topic is what you are able to do with your topic. I want to see an original well-written essay that explains, integrates, and contrasts material from various sources, not one that simply condenses or paraphrases. Originality can take the form of comparisons between existing models, extensions to published results, new proofs of old theorems or new ways of presenting old results, interesting new research questions, and so forth. My goals for the project are that you should learn something new and that your paper should teach me something new.

For those registered for CPSC 461b: I certainly don’t expect original research results, but if you happen to do some original work, that’s fine too. I do expect a paper that reflects a significant

amount of effort invested over a period of time and that demonstrates your understanding of the topic.

For those registered for CPSC 561b: I expect a greater degree of originality and professionalism from graduate students than from undergraduates. While I still do not expect publishable research to come out of a course project, I will look for a product that is at the graduate level.

4 The Report

4.1 What Makes a Good Essay?

Past experience has shown that many Yale students do not know how to write an essay or scholarly paper. I can't really tell you how to write a paper in this brief handout, but the section title is intended to remind you that a project report *is* an essay of sorts, and the things you have learned in other courses about logical organization, writing style, use of proper grammar and spelling, and proper methods of citing other people's work all apply here.

Like an essay, the project report should have some ideas of your own to report. It should reach some conclusion, and it should give logical arguments and relevant data to support that conclusion. What I do *not* want in a paper is a simple paraphrasing of somebody else's work. Quoting other people's work, as a way to make a point, is perfectly acceptable, if properly attributed; simply copying their work, attributed or not, is not acceptable. I want to read about *your* ideas and *your* conclusions, not somebody else's. But of course you will rely on other people's work to support your arguments.

4.2 Required Form of the Report

Your paper should follow accepted guidelines for scholarly work in computer science. The paper should begin with title, author, date, and abstract. Every page must be numbered. The body of the paper should be divided into logical sections appropriate to the structure of the material. Each section should have a numbered section heading. Numbered and unnumbered subheadings should be used where appropriate. Figures and tables should have captions and should be referenced by number. Related work should be cited in the text, and full reference information should appear at the end in a bibliography. Any material copied verbatim should be enclosed in quotation marks as well as being properly cited. The bibliography should contain full information, including author, title, year, and publication data. If the publication is a conference proceedings, then the proceedings title, editor, organization or publisher, etc. should be included. If it's a book, then the publisher should be included. If it's a web page, then the URL and sponsoring organization should be mentioned.

4.3 Tools

Most mathematical papers in computer science are prepared using the \LaTeX typesetting system. (That is also the system that I use for preparing class handouts!) Because this is a computer science course, and because it is educational for you to learn to use the tools of the field, I am asking you to prepare your paper in \LaTeX and to prepare your references using the companion tool, \BIBTeX . Compared to papers produced on a typical word processor, the results from \LaTeX are much more professional looking. \LaTeX automatically numbers pages and sections, automatically produces a table of contents and list of figures (if desired) and generates page headers and cross-references. \BIBTeX takes information that you put into a bibliographic database and formats it according to

commonly-accepted styles. You don't have to remember whether the article title or journal title should be italicized, or where commas and periods are needed—it does all that for you. But the big win comes when typesetting equations and other mathematical notation. \LaTeX produces professional-quality typeset equations and formulas rather painlessly. Attempting to do the same in a word processor is clumsy at best, and the results are disappointing.

It does take some effort to learn how to use \LaTeX effectively. I would suggest looking at one of the two tutorials [Gre00, OPHS00] that are accessible via the “Online Documentation” section of the course web page. For the advanced \LaTeX user, I recommend [Lam94, GMS94]. There is also a wealth of information on the CTAN archives, available on the web at <http://www.tug.org>.

5 Hint

Start now! Locate your resources. Many but not all papers are available on the web. Non-electronic library materials can sometimes be hard to get and may need to be obtained on interlibrary loan (which can take weeks). Make sure your project is doable in the amount of time available. Your proposal should identify the resources necessary to carry out your project.

References

- [GMS94] Michael Goossens, Frank Mittelbach, and Alexander Samarin. *The \LaTeX Companion*. Addison Wesley Longman, Inc., Reading, Massachusetts, 1994.
- [Gre00] Harvey J. Greenberg. A simplified introduction to \LaTeX . Available for download from <http://www.tex.ac.uk/tex-archive/info/simplified-latex/>, April 2000. Also available on the CPSC 437 web site.
- [Lam94] Leslie Lamport. *A Document Preparation System: \LaTeX User's Guide and Reference Manual*. Addison Wesley Longman, Inc., Reading, Massachusetts, second edition, 1994.
- [OPHS00] Tobias Oetiker, Hubert Partl, Irene Hyna, and Elisabeth Schlegl. The not so short introduction to \LaTeX 2 ϵ . Available for download from <http://www.tex.ac.uk/tex-archive/info/lshort/english/lshort.pdf>, September 2000. Version 3.16. Also available on the CPSC 437 web site.