

CIS 400/628, Spring 2005

Midterm Project Due 31 March 2005, 2 pm

Introduction

The midterm project is a solo project. For this project, you are to write a short (approximately five page) paper on a topic related to cryptography. You may choose one of the sample topics listed below, or my choose an alternate topic and submit it to me for approval. No two students may work on the same topic, so topics are first-come, first-served.

All topics must be approved by me by 10 Mar 2005 (topics in the following list are implicitly approved, but you should still check with me to ensure that no other student has chosen the same topic).

Formatting

You should use no larger than 12-point font and one-inch margins. You should submit a PDF file by e-mail to the TA mailing list.

If you work in Word and do not have Adobe Acrobat Distiller, you can either download a free PDF printer driver for Windows that will allow you to print to a PDF file instead of a printer. Alternatively, you can select a PostScript printer, print to a file, and then use a free utility such as ps2pdf (available on most Unix systems, and also available for Windows) to convert from PostScript to PDF. If you use a Macintosh, you can directly print to a PDF file.

Grading

Grading will be based on the following properties:

Formatting 10%

The paper should be typeset, and free from spelling errors. It should conform to the rules outlined above. Citations should be in proper format.

Grammar and Usage 20%

Does the writing follow the rules of English? Do nouns and verbs agree? Are articles used properly? Are sentences complete?

Organization and Style 30%

Does the writing flow? Is there a clear introduction/beginning and conclusion/ending? Are the main points of the paper clearly explained? Does each section support or develop one of the main points? Is each paragraph germane to its section, and each sentence to its paragraph?

Impact 40%

Does the writing achieve its purpose, either in making an argument, describing a technology, relating an event, etc.?

Note that in an excellently-written paper, grammar and organization will be transparent. That is, I won't notice how good they are until I'm finished. If, on the other hand, I struggle to get through a sentence because of improper grammar and usage, or have to reread a paragraph because it is out of place and doesn't contribute to the theme of the paper, I will give that paper a poor grade.

Sample Topics

- Describe current or past efforts to limit the availability of cryptography within the US.
- Summarize current legal protections in the US and the EU for encrypted information (e.g., under what circumstances can you be forced to reveal your encryption keys?).
- Describe restrictions on exporting cryptographic software from the USA and the EU (as of 2005).
- Describe one of the following candidates for the Advanced Encryption Standard:

Twofish	Serpent	RC6	DEAL
MARS	SAFER+	FROG	LOKI-97
CAST-256	Magenta	DFC	Rijndael

- Describe or develop a formal analysis of a key-exchange protocol.
- Historical roles of codes and ciphers, e.g.:
 - Cracking the Enigma cipher in WWII.
 - Cracking the Purple cipher in WWII.
 - The role that ciphers played in the execution of Mary, Queen of Scots.
 - Language-based codes (e.g., Codetalkers in WWII).
 - Decipherment of a dead language (e.g., the Rosetta stone, hieroglyphics, or linear-B).
- Describe a block cipher such as IDEA or Blowfish.
- Describe a side-channel cryptanalysis technique (e.g., differential power cryptanalysis on smart cards).