Fall 2017

Project 9 Requirements

Shiu-Kai Chin

Abstract

The objectives, requirements, and relevant information for Project 9 are stated here. Submission of your files is done through the course website.

1 Purpose

The purpose of this project is for you to demonstrate the following:

Capabilities: to produce a basic technical report of professional quality containing:

- Code solutions to Exercises 15.6.1, 15.6.2, and 15.6.3.
- Session transcripts showing proof results
- Explanations as required by each problem
- All source code for each exercise in the appendix

Reproducible Proofs and Documentation: All your datatypes, definitions, theorems, and proofs are contained in HOL theories. All your theories are pretty-printed as stand-alone LaTeX reports.

- Your HOL theories must be built using *Holmake*
- Your pretty-printed HOL theories must reside in a subdirectory called HOLReports and be maintained using *make clean* and *make*

Use of Relevant Tools and Techniques: LaTeX, AUCTeX, emacs, ML, and HOL

Deliverables and Evidence: a pdf of your report with *all source files allowing others to reproduce your report.*

2 Project Requirements

Your report shall have content to reflect Exercises 15.6.1, 15.6.2, and 15.6.3. Specifically,

2.1 Theorem and Theory Names

Use the following names:

Theory Name: `cryptoExercisesTheory`

Theorem Names: In all the exercises use the names below.

Exercise 15.6.1: `exercise15_6_4_1a_thm` and `exercise15_6_4_1b_thm`
Exercise 15.6.2: `exercise15_6_4_2a_thm` and `exercise15_6_4_2b_thm`
Exercise 15.6.3: `exercise15_6_4_3_thm`

2.2 Report Contents

Front Matter: Title, Author, Date, Abstract, Acknowledgments, and Table of Contents

Chapter 1: Executive Summary

Chapter 2: Exercise 15.6.1 with the following subsections

1. Proof of `exercise15_6_1a_thm`
2. Proof of `exercise15_6_1b_thm`

Only one problem statement covering both sections is needed. Each section must include relevant code and transcripts of definitions and proofs.

Chapter 3: Exercise 15.6.2 with the following subsections

1. Proof of `exercise15_6_2a_thm`
2. Proof of `exercise15_6_2b_thm`

Only one problem statement covering both sections is needed. Each section must include relevant code and transcripts of definitions and proofs.

Chapter 4: Exercise 15.6.3 with the proof of `exercise15_6_3_thm`. The chapter must include a problem statement, relevant code, and transcripts of proofs.

Appendix A: Contains the source code file *cipherScript.sml*.

Appendix B: Contains the source code file *cryptoExercisesScript.sml*.

2.3 Pretty-Printed Theories in HOLReports

Your pretty-printed theories must include the following theories:

1. *cipherTheory*, and
2. *cryptoExercisesTheory*.

3 Relevant Information

3.1 Submission Guidelines

Deadline: consult course website

Content & format: gzipped tar file of your Project9 subdirectory containing a pdf of your report and all source files allowing complete reproduction of your report. Your Project9 subdirectory will have the following structure and naming conventions:

- You will have 2 subdirectories in Project9:

  HOL: which contains all your source code, e.g., HOL script files, and

  LaTeX: which contains all the files for your project report, e.g., style files, LaTeX files for your report, figures, etc.

- Definitions and proofs of all exercises will be in their corresponding script files
- Your **HOLReports** folder will be *subdirectory of your HOL folder*. Within HOLReports will be the following files:

  Holmakefile: which includes all the paths to theories needed, and specified in a way that does not require third parties to alter path information to compile pretty-printed reports.

documentation.sml: which contains all commands necessary to pretty print your theory files

Makefile: which is the script defining *make clean* and *make* commands that remove or build all pretty-printed HOL theory files, respectively.

How submitted: through course website

Other information: you will be allowed an unlimited number of attempts to submit your files up to the deadline. Your grade is based on the last submission.

3.2 Grading Criteria

Project Report					
Deliverable Item	**Problem Statement**	**Relevant Code**	**Definition & Proof Transcripts**	**Code in Appendix**	**Total**
Chapter 1: Executive Summary	4 points for summary	N/A	N/A	N/A	4 points max
Chapter 2: 15.6.1	1	2	2	1	6 points max
Chapter 3: 15.6.2	1	2	2	1	6 points max
Chapter 4: 15.6.3	1	1	1	1	4 points max
Appendix A: *cipherScript*	N/A	1	N/A	N/A	1 point max
Appendix B: *cryptoExercisesScript*	N/A	5	N/A	N/A	5 points max
Report Content Subtotal	7 points max	11 points max	5 points max	3 points max	26 points max
LaTeX folder with all necessary files to reproduce report with no errors					26 points max
				Report Total	52 points max
HOL Script Files and HOLReports Files					
Deliverable Item					**Total**
HOL theories build with *Holmake* error free: 2 points per item					10 points max
Pretty-printed HOL theories in LaTeX compile using *make* error free: 2 points per definition or theorem					10 points max
				HOL Script and HOLReports Files Total	20 points max
				Grand Total	**72 points max**