BOB JONES UNIVERSITY
EST. 1927

College of Arts & Sciences

CpS 306
Applied Cryptography
Spring 2024

Instructor:	Jordan Jueckstock
Office:	AL 76 *(3rd floor, east hall)*
Office Hours:	MWF 3pm / TTh 10am *(others by appt. only)*
Email:	jpjuecks@bju.edu

Course Description:

Introduction to the field of cryptography. Topics include classical, private-key, and public-key cryptography and the application of the various types to computer, communications, and internet security.

Course Context:

The material and activities in this course contribute particularly to student progress toward the following Cybersecurity program learning outcomes:

- Cy1: Apply introductory cybersecurity principles to both policy and practice
- Cy2: Design, implement, and evaluate a computing-based solution to meet a given set of secure computing requirements
- Cy5: Apply biblical principles of ethics in computing

Course Reading:

- *Real World Cryptography* by David Wong. Manning Publications Co., 2021.
  ISBN: 978-1-61729-671-0 **("RWC"; required)**

Course Goals:

The goals this semester are:

- To understand the motivations, capabilities, limitations, and ethics of practical cryptography
- To demonstrate technical familiarity with state-of-the-art cryptographic primitives (e.g., hashes, ciphers, key exchanges, signatures) and protocols (e.g., TLS, Signal, Bitcoin)
- To gain insight into the platform cryptography provides for trustworthy information system design, development, and deployment

Schedule:

The anticipated schedule of lecture topics, class milestones, and due dates is maintained on the CpS 306 website at https://protect.bju.edu/cps/courses/cps306/schedule/.

Assignments:

Quizzes cover topics that have been recently introduced in class to check student comprehension of the presented materials. Quizzes are graded in class.
Lab assignments are small to medium implementation (i.e., programming, usually) exercises to give you practical experience with concept or technology that is currently being discussed or will be used in an upcoming challenge.
Challenges are larger-scale *individual* assignments that require original thinking to solve a nontrivial problem using newly acquired concepts and skills; challenges are focused on learning to *attack* vulnerable crypto-enabled applications.

Tests cover all theoretical and practical topics covered in class, with special emphasis on prompting students to think through the implications of what they have learned (i.e., explaining "how" and "why" is more important than just remember "what"). All tests are cumulative; the final exam is simply the last test (same format, same point value; happens to cover all the material).

The **Design Project** is an information system engineering project in which students must analyze a given problem scenario, determine a viable threat model, and design a cryptographically secured information system (i.e., an application, or set of applications) to address that threat model. The design process will include adversarial peer review of designs and will be turned in/graded across multiple checkpoints.

Grading			
#	*Category*	*Pts.*	*Total*
12*	Quizzes	10	100
10	Labs	10	100
5	Challenges	50	250
3	Tests	100	300
1	Design Project	300	250
	Informal Pitch	*25*	*25*
	Draft Proposal	*50*	*50*
	Peer Reviews	*75*	*75*
	Final Proposal	*100*	*100*
	Optional Prototype	*50*	*0*
	Total		**1000**

* Lowest *two* quizzes dropped

Scale	
A	900+
B	800-899
C	700-799
D	600-699
F	0-599

Grading:

Grades are computed on a simple 10-point scale (see below) based on points earned out of 1000. Grades are not rounded up (or down—which probably should go without saying). Instead, all students are allotted 5 bonus "grace points" (which have the effect of rounding up, e.g., 695 to 700). The instructor reserves the right to confiscate these grace points, at his sole discretion and at any time, for repeated (or egregious) displays of disrespect to either the instructor or fellow students. *(Students who lose their grace points will be informed as soon as possible.)*

Course Policies:

- *Attendance*: Absence/tardiness are reported per University policy. Assessment of University vs. personal absences, and official penalties for too many personal absences, are handled by the registrar's office.
- *Deportment*: Students and instructor will address each other with professional respect and courtesy, no matter how much fun we are (or are not) having. Students shall refrain from talking (or whispering, or texting, or tapping messages in Morse code, or…) during lectures, presentations, etc. unless otherwise indicated by the instructor.
- *Technology*: personal computers (which, let's be honest here, includes phones and smart watches) will not be used in class unless called for by the instructor (e.g., during lab sessions). Phones, smart watches, and other communication doodads should be kept silent and passive except for high-priority communications previously discussed with the instructor (e.g., waiting for word about a sick family member).
- *Due dates:* See the department late policy https://cs.bju.edu/academics/policies/late-work-policy/. Unless otherwise specified, submissions must be received by 11:59pm on the day they are due.
- *Academic Integrity*: See the department policy: https://cs.bju.edu/academics/policies/academic-integrity-policy/. "Challenges" are considered "programs" (i.e., individual assignments).

Copyright Policy:

Copyright 2021-2024 Jordan Jueckstock as to this syllabus and all lectures. Students are prohibited from selling (or being paid for taking) notes during the course to, or by any person, or commercial firm without the express written permission of the professor teaching the course.