Spring 2023: Syllabus for NTCrypto

Prof. Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA

For all of my courses

[Specific Number Theory & Cryptography info starts on the next page.]

Who?	Prof. King	Eddress:	squash@ufl.edu
Office:	402Little	Tel:	352-294-2314
Math Dept:	3^{rd} floor Little	Dept.Tel:	**352-294-2350**

To find my office (402 Little Hall; Top floor, NE corner) just "Maximize x, y and z." (Note: I do *not* pick up tel. messages remotely, but do read email multiple times a day. It is almost always better to email me first, before telephoning my office.)

Class attendance is required, and is part of a student's CP, Class participation, grade.

Contacting Prof.K. If you need to get an important message to me (e.g, you'll be missing an in-class exam), it is *particularly important* that you **email me** *from your **UF eddress*** as soon as possible; preferably several weeks or days before the exam; several hours before, if you didn't know in advance.

I do *not* pick up office phone messages remotely, so it is important that you email me. If urgent, you should also tel. the math dept, **352-294-2350**, and they can contact me at home. The secretaries can also put a note in my mailbox if you request it. [All these tel.numbers are *wired phones*; they do not take text-messages.]

IMPORTANT: I will primarily use **email** for contacting students, *not* Canvas-mail. I ask that students read email *at least* twice a day morning/evening (excepting for religious observance).

IMPORTANT: Students will be typesetting solutions to problems and will need a real **computer**; a cellphone does not suffice. Also, students will need access to a **printer**, as some of the typeset assignments will need to be handed-in on paper (not electronically).

As some office-hours will be via Zoom, students will need Zoom-capability.

Prof.K's clickable links:

- Teaching Page http://squash.1gainesville.com/teaching.html Has important info for *all* my courses. Gives links to *Putnam competition*, *Robert Long essay competition*, links to the free mathematical typesetting language TEX/LATEX.

  The Teaching Page also has an extensive list of:

  Usually Useful Pamphlets.

- Our NTCrypto Webpage: http://squash.1gainesville.com/course.NTCryp.curr.html Info for the current semester, as well as links to previous versions (see Nostalgia) of NTCrypto, containing previous exams and microquizzes, for your studying pleasure!

- Prof. King's page at UF http://people.clas.ufl.edu/squash/ has a link to the *Robert Long essay competition.*

- Prof.K schedule & office hours http://squash.1gainesville.com/info.jksched.html

- Math Dept. homepage http://www.math.ufl.edu/ . Searchable. A wealth of information on applying to grad school, seminars, conferences, faculty,staff,grad listings, tutors for hire.

University resources, clickable:

* UF syllabus policy https://people.clas.ufl.edu/squash/univ-syllabus-policy/

* Accommodation for students with disabilities https://disability.ufl.edu/students/get-started/

* UF Teaching Center https://academicresources.clas.ufl.edu/ has free tutoring, both in-person and via zoom.

* Writing Studio https://writing.ufl.edu/writing-studio/ 2215 Turlington, 352-846-1138.

* The UF Help desk http://helpdesk.ufl.edu/ 352-392-4357.

* End-of-Semester student evals of professors https://gatorevals.aa.ufl.edu/students/

LOR: Letter-of-recommendation. I base LORs substantially on how a student "thinks on his/her feet"

I require **two** courses with me, at least one of which is *proof-based*, as well as the student actively participating in class. (Occasionally, one course may suffice if it is a **graduate course** or a **Special Topics** course, e.g, my MATHEMATICAL CRYPTOGRAPHY course.)

Microquizzes. There will be some number of "pop" (unannounced) microquizzes (***MQ***), each worth 30points. (Just handing-in the MQ with name and ordinal earns 5points.)

MQs never occur on religious holidays; ***email me*** *of all such religious dates by the first Wedn. after Add/Drop.*

Usually, a pop-quiz has a single, easy question. I use them partly for attendance, and checking that an idea from the previous class caught on.

IMPORTANT: I *drop* the lowest microquiz score. AND: There is **No makeup** for the first missed MQ, regardless of reason; that is what the dropped-score is for.

If a 2$^{\text{nd}}$ MQ is missed, I may give a make-up, if there was an emergency or if I knew in advance (e.g, you are giving a talk at a conference, and you let me know well in advance). □

Class Archive. We will all use our NTCrypto Archive, a LISTSERV, to communicate to the whole class.

Once Add/Drop has ended, I will email out how to post-to/read-from our Archive, which plays the role of a NTCrypto Wikipedia that students build during the semester, acting as a reference for everyone in class.

Students will be posting problem-solutions to the Archive, as part of their CP (Class Participation) grade.

Canvas. Canvas will be used for recording grades, but not much else. We will primarily use *email* and our class Archive (a LISTSERV) to communicate with each other outside of class.

End-of-Semester Games Party! If COVID *et al* stays low, then we will have an *End-of-Semester Games Party*. (We might also have a "team building" *Games Party* mid-semester.) In the past, the Games Party has been on the last date of class, at Pascal's Cafe, in the

Christian Study Center of Gainesville
112 NW 16th Street

Abbreviations. MQ, Microquiz. OH, Office-Hour. CP, Class participation. IP, Individual Project. IOP, Individual Optional Project. RLEC, Robert Long Essay Competition.

RLEC. Each year, students who like to write short essays may enter the *Robert Long Essay Competition*. The RLEC has a monetary prize and, more importantly, looks great on a CV.

Office hours. My current *weekly schedule*. (OHs may change slightly during the semester, and other days/times may be available by appointment, sometimes via Zoom.)

Specific NTCrypto information:

Elementary Number Theory is a beautiful subject, in which both algebraic and number-theoretic thinking interact.

Here our four topics: Elem. NT, Cryptographic codes, and attempts to break them, Data compression codes, Error-correcting codes. All of this is done from an NT viewpoint.

This course does *not* teach how to make a *practical* cryptographic-system for commercial purposes. It is primarily a NT course, with applications to coding.

Textbook: An Introduction to Mathematical Cryptography, by Jeffrey Hoffstein, Jill Pipher & J.H. Silverman

Further text info at
Course Page: NTCrypto
http://squash.1gainesville.com/course.NTCryp.curr.html

Course/Room/time. MAT4930 0329 (25286)

The class meets in Little Hall room 219 [South side of the West wing, 2$^{\text{nd}}$-floor] on MWF at 7th period, [13:55-14:45], i.e 1:55PM to 2:45PM.

CP grades. Each of Jan., Feb., Mar. (and a part-score for Apr.) has a CP, Class participation, 45pt grade based on speaking in class, attending OHs (sometimes via Zoom), and *especially* posting solns to non-trivial problems to our Archive. A typical grade is 20. For *exceptionally* active students, I may give a grade a bit higher than 45.

MQ grades. Each microquiz is 30pts Typically, MQs are not announced. A MQ usually has a single routine question. The *lowest MQ score* is dropped; there is *no makeup* for the first missed MQ.

The classday following an in-class exam often has an MQ with a slight variation of a question from the exam.

NOTE: There will be a MQ the classday before, and the classday after, Spring Break.

NTCrypto Exams. In NTCrypto, some of the exams have a *team take-home component*, with team's of 3 (sometimes 2), students, followed by an *individual in-class component* that students take (unsurprisingly) individually.

A student's score is the sum of the take-home and in-class. There will be an end-of-semester take-home IP (Individual Project) that will be due the day after the semester's last class-day. [The Project *may* be optional; I will decide that later in the semester.]

Crypto exam-dates, Spring 2023:

(Note: Occasionally an exam needs to be moved a class-day *later* or a class-day *earlier*. Since that is a class-day, I do *not* [baring extenuating circumstances] if you miss class and the exam that day.) (BoC = *Beginning of Class*, and wATMP = *with All Team Members Present*.)

Home-U: PDF available evening of Tues., 14Feb; due BoC Monday, 20Feb.

Class-U: Wednesday, 22Feb.

Home-V: PDF available evening of Tuesday, 07Mar or Wedn., 8Mar morning. [Spring Break: March 11-18, Sat.-Sat.]

Home-V is due BoC Monday, 20Mar.

Class-V: Wednesday, 22Mar.

Class-W: Wednesday, 12Apr *Canceled.*

Friday, 14Apr: Canvas will have an *estimate* of current course-grade, the morning of this date.

<u>*Typeset*</u> IOP [Individual Optional Project]: Avail. Thur., 20Apr.. Due Thursday, 27Apr by 2PM, slid under my office door, LIT402.

Last day class, Wednesday, 26Apr: *Games Party!* and *Class Photo*, at *Pascal's Cafe*.

Sincerely, Prof. King