MATH 5346 / 4000 : Introduction to Cryptology
Section 102, M-F 12:00–1:50, MATH 012.

Course Information:

Instructor:	Chris Monico
Email:	`c.monico@ttu.edu`
Office:	MA-252
Office Hours:	M-F, 2:30–3:30.

Important Dates:

Last day for student-initiated drop on MyTech with penalty	Monday, June 25.
Last day of classes	Tuesday, July 3.

Grading Policy: Your final grade in this course will consist of the following weighted components:

Homework:	50%
Presentation:	20%
Attendance:	30%

Homework must be **legible and stapled**. You are encouraged to work in groups of two on homework assignments (each group need only submit one copy of solutions).

Your final letter grade for this course will be determined as follows.

90–100%	A
80–89%	B
65–79%	C
55–64%	D
0–54%	F

Attendance: Class attendance is *mandatory*. An absence will be excused *if and only if* you are absent for one of the following reasons:

- You are out of town performing duties on behalf of the university (i.e., athletics). Advance notification is required.

- Religious holy day (see below).

- Hospitalization (requires verification from the Center for Campus Life).

Expected Learning Outcomes Students will learn the basics of cryptology, including at least:

- The classical ciphers: monoalphabetic substitution, Vigenère and its variants, Playfair, the one-time-pad, bifid, and transposition. Cryptanalysis of some of these.

- Public-key systems, including RSA, Diffie-Hellman, and elliptic curve cryptosystems. Algorithms for factoring integers and computing discrete logarithms.

- Other topics: stream ciphers, AES, digital signatures.

ADA Accommodation: Any student who, because of a disability, may require special arrangements in order to meet the course requirements should contact the instructor as soon as possible to make any necessary arrangements. Students should present appropriate verification from Student Disability Services during the instructors office hours. Please note instructors are not allowed to provide classroom accommodations to a student until appropriate verification from Student Disability Services has been provided. For additional information, you may contact the Student Disability Services office in 335 West Hall or 806-742-2405.

Religious Holy Day Observance (OP 34.19)

1. "Religious holy day" means a holy day observed by a religion whose places of worship are exempt from property taxation under Texas Tax Code §11.20.

2. A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.

3. A student who is excused under Section 2 may not be penalized for the absence; however, the instructor may respond appropriately if the student fails to complete the assignment satisfactorily.

Academic Integrity I take academic integrity extremely seriously. In particular, I have a zero-tolerance policy for both cheating and plagiarism. I define *plagiarism* as claiming the work or ideas of someone else as your own. Copying homework, phrases, sentences, or mathematics from any other source (including another student or a solutions manual) without citation is therefore plagiarism. Yes - it is very possible to plagiarize mathematics and it is just as offensive as every other instance of plagiarism. I would hope that you do not want someone else to claim credit for your hard work and I therefore expect that you will not claim credit for someone else's work under any circumstances. If you use (read, look at, listen to, copy,...) a source other than the textbook then cite it, being as specific as possible (e.g., if you used a web site then give the URL - but if you forgot to write it down or cannot find it, the next best thing would be the name of the web site; if you cannot remember that, then at least acknowledge that it came from the web but you cannot remember where).

All instances of cheating on exams will be dealt with as strictly as allowed by TTU OP 34.12. Instances of plagiarism will be dealt with on a case-by-case basis and may range from a written warning to an automatic assignment of an F in the course, depending on the severity of the offense.