MCS 425: Codes and Cryptography (Fall 2021)
Project Guidelines

Objectives.
1. A project report + optional supplemental material (webpage, code with documentation, etc.).
   Your project report will be shared with your classmates (and possibly future students as well).
2. A 15-minute presentation in class (2-minute transition + 10-minute talk + 3-minute Q&A).

Teams. You may work alone or with one other student. The grading standards for contribution
(see below) will be more stringent for teams of 2 than for teams of 1.

Submission instructions.
• Submit a single .pdf or .zip file on Gradescope.

Timeline.
• Oct 20: Decide on teams and project title.
• Nov 15 – Dec 1: Class presentations.
• Dec 5: Project due (at 11:59pm CDT).

Grading. The projects will be graded out of 20 points (with up to 4 bonus points) as follows:
• Logistics (6 points):
  – (2 points) Decide on teams and project title by Oct 20.
  – (2 points) Confirm your presentation dates by Nov 8. Show up on time (in person or
    over Zoom) for your presentation.
  – (2 points) Submit a project report by Dec 5 (slides or transcript of slides do not count).
• Presentation (8 points): This part will be graded solely by other students. The following
  criteria are provided as guidelines. You are welcome to discuss/post your criteria on Piazza.
  – Did the presentation attract other students to learn more about the project?
  – Did the presentation give a good overview of the chosen topic and the project?
  – Was the presentation well-organized?
• Contribution and Originality (6 points): Your project report will be assigned a score (usually in the range of 3-6 points) by the instructor.
  – How creative is the idea and the execution of the project?
  – Will the project be useful to students and researchers in cryptography?
  – Does the project explore in depth a topic that we did not cover in class?
  – Does the project offer something that cannot be easily found from textbooks or Internet?

• Extra credit (up to 4 bonus points):
  – You will be asked to assign a score (usually in the range of 5-8 points) to other teams’ presentations. If your evaluation is among the top 40% most accurate evaluations (measured by the $\ell_2$-distance to the aggregated evaluation), you will receive 1-2 bonus points.
  – The top 20% project reports will receive 1-2 bonus points.

Examples of project ideas. Here are some potential topics for the course project. This list is far from comprehensive and is meant to inspire you to think about what you want to work on. You are encouraged to pick a topic that aligns with your interest!

• Survey the history of some classical cryptosystems and/or where they are still used (e.g., one-time pads, Enigma).

• Compare letter frequencies in different languages. For these languages, write code for ciphertext-only attacks on Vigenère ciphers.

• Implement your favorite factoring algorithm and compare it with available factoring packages/modules.

• Investigate the effectiveness of different primality tests. Survey more sophisticated primality tests (e.g., Miller-Rabin, AKS).

• Build an interactive webpage to explain how the RSA cryptosystem works.

• Survey quantum factoring algorithms and quantum-resistant cryptography.

• Compare empirically the collisions of hash functions to the birthday problem approximation.

• Explore basic cryptographic protocols for secure multi-party computation (e.g., oblivious transfer, garbled circuit).

• Gather a list of interesting and neat cryptographic problems and their solutions (e.g., coin flipping over the telephone, Yao’s Millionaires’ problem, private set intersection).

• Explore elliptic curves and their applications in cryptography.

• Explore lattice-based cryptography and/or homomorphic encryption.

• Interview researchers in cryptography.