

Class Presentations

Cryptography
Jan Term 2020

Topic: For this project, you will work in teams of two¹. Each team will select a topic related to cryptography to research and present to the class. The topic may be primarily historical or primarily technical but must your presentation must include each of the following:

- Historical context and significance
- Define all new terms/notation
- *Thorough* discussion of mathematical ideas
- Either work a simple example with the class or show an example of the concept being applied
- Class activity to engage students with the content (be creative)
- Treats or snacks for class (optional: has no impact on grade)

I will need to approve what topic you select, but I am pretty flexible as long as it is meaningfully related to an area of cryptography. If you need some help getting started thinking about ideas, begin by looking into some of the topics below or go here: http://en.wikipedia.org/wiki/Outline_of_cryptography.

- Common data compression algorithms (zip, tar, etc.) and their relative advantages and disadvantages
- Cryptography in a resource constrained application (such as smart cards, cell phones, or ATMs)
- Cryptography on the internet: SSL, ssh, https, their strengths and weaknesses
- DVD encryption and how it was broken
- Cryptocurrencies – such as Bitcoin
- Electronic voting
- Japanese ciphers in World War II
- Kerberos
- Pretty Good Privacy (PGP) - social, political, technical aspects
- Random numbers: generating them and testing for randomness
- The Merkle-Hellman cryptosystem (knapsack)
- Autonomous vehicle security systems
- The VENONA project
- WEP and WPA wireless encryption
- The Cayley-Purser Algorithm
- Information Theory (Claude Shannon)

You'll need to ensure that the scope of your topic is not too broad or too narrow given the time restriction and reference requirements given below.

References: You will need multiple sources pertaining to your topic get a full and well-rounded understanding of that topic. Feel free to use books, articles, websites, or any other source you want. You will need to compile a list of at least 5 resources. *At least two resources must **not** come from websites.* In addition to each reference, you will also include a short (4-5 sentence) summary of the

¹ Since we have 19 students in our class, we will need one team of three. The first students who request to be a team of three will get it.

reference and what you plan to use from it in your presentation. I will not be picky about the citation style as long as you are consistent with all of your resources.

Outline: Your group will need to turn in a thorough outline of your talk **Wednesday, Jan 22nd**. This must include a detailed account of what will be covered in the talk. Also indicate which team members will be discussing which sections. I don't need a word-for-word description of your talk, but I do need more detail than 5 or 6 bullet points.

Class Presentation: Your presentation should be a clear and thorough overview of your research. *It needs to be 20-25 minutes long* for teams of two and *30-35 minutes long* for teams of three. This includes the time spent on the class activity. You will lose points for a short presentation, so you will want to practice beforehand to work out the timing issues.

Multiple Choice Questions: Your group will need to submit to me **six** multiple choice questions (with 4 choices each) of varying difficulty. These will be due to me **Wednesday, Jan 22nd**. Your group may email me (nmoyer@whitworth.edu) the questions along with the answers. I will select three of them to put on the final quiz during the last day of class.

Grading:

Presentation	55%
References/Summaries	15%
M/C Questions	5%
Presentation Outline	10%
Class Evaluation	15%

Schedule:

Date	Due
1/10	Topic and names of group members
1/16	List of references/summaries
1/17	Sign-up for presentation time
1/22	Presentation Outlines and Questions
1/22,23,24	Class Presentations

More details:

This project is worth 25% of your grade. The grade you get on this project will be directly determined by the effort you put into this project. Since you are mature, responsible adults, I am going to assume that the workload will be evenly distributed among group members. *Have fun exploring cryptography!* I am excited to see what you guys will learn through this process.

One more note: I consider the days of presentations to be just as much of a learning experience as any other day in class. The only difference is that you will be the ones teaching instead of me. You will still need to be in class and paying attention (and even taking notes) every day while groups are presenting. You will be evaluating each presentation, and you will also be accountable for the material presented.

On the last quiz I will ask a two multiple choice questions from each of the presentations.

Criteria—Goal	5 Exemplary	4 Good	3 Satisfactory	2 Marginal	1 Needs Improve- ment
Purpose —Clearly provided motivation and context to the topic: why is this important, how does it relate to things we've studied?	attempt at making the motivation and context memorable.	audience knows exactly why this topic is important + how it fits in.	attempt at giving context and motivation	context or motivation not given.	no context or motivation
Explanation (x2) —Explained the concepts clearly.	gave truthful, clear, and memorable explanations	gave truthful and clear explanations	gave truthful explanations	some minor errors in explaining concepts	no/ insufficient explanation or contained major errors
Demonstration (x2) —Either worked a simple example with the class or showed another example of the concept being applied	outstanding example	clear example	example tough to follow	example lacking in some way	no example
Organization —Organized presentation in a manner that enhanced the audience's understanding	great organization that enhanced the presentation	the organization was clear	there was some organization	organization was clearly lacking in some spots	un-organized to the point of distraction
Materials —Used clear visual aides, not too much on a slide/screen, readable from the back of the room; appropriate English syntax and grammar used	outstanding slides	slides were clear	slides were legible	hard to read some slides	could not read or understand the slides
Time —Did not take too little time, so that material was explained inadequately, or too much time, leaving inadequate time for other team members (speakers should be given an equitable portion of the presentation for the material that they must present)	plenty of time for questions, but covered everything thoroughly	enough time for everyone	managed to cover all the material	had to skip something, or wasted time unnecessarily	completely blew the schedule
Presentation Skills —Faced and made eye contact with members of the audience, words and phrases enunciated well, spoke loud enough to be heard	so good you did not want them to stop	most speakers made eye contact, had clear voices	could understand everyone	some speakers were hard to understand	most speakers were hard to understand
Polish and Attitude —Made clear that the presentation was rehearsed and ready to go; demonstrated a positive attitude and enthusiasm about the presentation, able to handle questions and comments positively	made you want to join their team	presenters were relaxed, answered questions easily	seemed positive	seemed unsure of themselves	seemed genuinely embarrassed to be there

Score will be multiplied by 2 to get 100 total points