Encryption & Intercepting Information: Background, Cryptography

Introduction
1. How do you feel we should define strong encryption?
2. Introduce ourselves
   a. Our credibility as computer scientists
3. Encryption is something that affects everyone’s daily lives, but the government chooses data encryption standards today. Should encryption be a right? More specifically, should we as a country have an open discussion on encryption standards.

Body
1. Define encryption and how it affects our daily life
   a. Show where encryption is found
      i. Banks
      ii. Credit Cards
      iii. Store transactions
   b. Discuss the origins of encryption and how the government classified strong encryption as a munition
   c. Discuss data encryption standards
      i. What makes a strong encryption
      ii. Conflicts in standards?
         1. DES shift from 64 to 56 bits for encryption.
      iii. Who should decide encryption standards?
      iv. Should we have a right to encrypt our data?
2. How cryptography is affected by current events (changes in standards)
   a. Possibility of governments pressuring major tech companies to install backdoors
3. Discuss the 3 sides
   a. Government views on encryption
      i. How the government benefits from weaker encryption
         1. Easier access for law enforcement or possibly any individual
      ii. How the government benefits from strong encryption
         1. The government can protect their own sensitive information
   b. Consumer protection groups
i. How the public suffers from weak encryption
   1. Weak encryption lets identity thieves steal people’s information

ii. How the public benefits from strong encryption
   1. Private information is more secure

   c. Our views
      i. It’s a very delicate issue

4. General public’s apathy towards encryption and privacy
   a. Why don’t more people feel troubled by the government weakening encryption?
   b. By assuming the government will always be spying on our data and relying just on encryption to protect us, do we create certain standards regarding the government?

Conclusion
1. Summary
   a. Difficult to come to an answer that satisfies everyone
   b. What’s the future of encryption?

2. Closing statement
   a. How should we define strong encryption?
   b. The future of encryption will largely be determined by the conversations we are having about it. Thus, we need to change discourse we have regarding encryption.
Source List:

1. Tim Cook on Government Standards:  
   https://theintercept.com/2016/01/12/apples-tim-cook-lashes-out-at-white-house-officials-for-being-wishy-washy-on-encryption/

2. NSA response to Tim Cook:  

3. Americans’ Attitude About Privacy, Security and Surveillance  
   http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

4. Why We Need Encryption Even the NSA Can’t Decypher  
   http://www.newsweek.com/why-we-need-encryption-even-nsa-cant-decipher-352073

5. New Rules in China Upset Western Tech Companies  

6. Encryption as a munition:  
   https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States

7. Weak encryption and identity theft  

8. How a Crypto ‘Backdoor’ Pitted the Tech World Against the NSA  
   http://www.wired.com/2013/09/nsa-backdoor/

9. DES:  