Emerson Gann

CSS 337

Research Topic

Due 4/28/21

I have two topics that I thought would be good to research. I would appreciate feedback on which would be better or has more potential. If neither is aligned with the course material enough, I can select a different topic but these were the most fascinating to me.

The first topic is how the Venona project managed to break a misused one-time pad system. I would research the specific details on how the intelligence agencies managed the project, correlated the data, and linked enough of it in order to decrypt some of the messages. This would otherwise be impossible since a proper one-time pad is unconditionally secure. I think it is an interesting case study where a perfectly good encryption scheme had a flaw intentionally added due to logistical constraints which rendered it vulnerable to cryptanalysis.

The second topic is the evolving legal views on cryptography to secure digital media. Specifically I would look at evidence that may be related to criminal investigations, and how legally secure certain lock schemes are versus others. For example, there have been instances where a judge has ruled that compelling a suspect to give up his/her password to unlock a phone would violate his/her 5th amendment rights. But in other cases, such as unlocking a phone secured with a fingerprint or facial recognition instead of a password, it is not a 5th amendment violation since that info is not contained in the suspect's mind and so it is not 'technically' self-incrimination.