







2a. The computational artifact that represents my computing innovation is data encryption. Data encryption is a form of data security where data is transformed into an incomprehensible format so that only people with a certain key can unlock and read the data. The first part of the artifact explains what data security is, which is any security measure to protect data from unwanted access and corruption (“What Is Data Security…”). It then provides examples, such as a password, biometrics, physically masking data, and backing up data in case of data corruption or loss. The next part of the artifact explains how data is encrypted. There are usually two keys, a private key and a public key. The public key takes data then encrypts it. In order to read the encrypted data, the reader needs a private key to decrypt the data. Both keys are unique (Wikipedia contributors). The final part of the artifact explains the most popular medium in which data is encrypted, which is SSL. SSL provides keys and certificates to companies for encryption (Russell, Aaron).

2b. In order to create this artifact, I used a website called piktochart. I started off by choosing a template that had steps and explanation blocks on it already. There was an extra block on the end, so I had to delete that block to make the artifact shorter. I found images from Google to provide a visual explanation of common forms of data security. I then used icons from piktochart for the explanation of how data is encrypted. I then found the SSL logo on the SSL website and put it on my artifact. I then used easybib to cite my sources.

2c. A beneficial effect that encryption has on society is that it can be used to protect a user’s private data. If a hacker or malicious software intercepts or steals a user’s encrypted data, the data will be useless and the information itself will be protected. This can prevent the theft of information transferred online, such as credit card numbers, bank account logins, social security numbers, and any other important data. It can also protect from unauthorized access to information or databases. For example, the password on a phone protects from other people stealing the physical phone and accessing all the data in it. A harmful effect of encryption, however, is that malicious sources can use encryption as well to send and receive information. For example, terrorists can use encryption to send information to plan a terrorist attack. If the FBI intercepts this information, it could take too long to decrypt the data before it’s too late. While encryption protects private data, it can also be used for evil intent by sending malicious information.

2d. The kind of data that data encryption would use is almost any kind of data. Anything from text files, pdfs, to entire folders can be encrypted. That’s the point of encryption, to secure any form of data and prevent it from being read by unwanted people. Typically, the data communicated between a user and a server is encrypted, such as entering your credit information to buy something online. My innovation consumes a form of data such as text or an image and outputs a scrambled file that when opened, is incomprehensible. The data will be modified based on the key provided, in which case an encryption pattern, cipher, or algorithm uses the key as instructions to scramble. One of these, for example, is the AES algorithm, which is used by the NSA. This algorithm places the data into a table, mixes the rows and columns, then substitutes, mixes, and transposes the data in the table multiple times. One data privacy concern is that the complexity of these ciphers and algorithms need to become more complex as time goes on. Computers get faster and better, allowing them to, through trial and error, guess more and more keys in a smaller amount of time. For example, a modern computer can crack an Enigma machine in a tiny fraction of a second. As computers get faster, they can crack an encryption faster and potentially steal data, causing a data privacy concern.

2e.

1. “What Is Data Security? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/26464/data-security.
2. Wikipedia contributors. "Encryption." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 8 Oct. 2019. Web. 11 Oct. 2019.
3. Russell, Aaron. “What Is SSL?” *SSL.com*, SSL, 2 Oct. 2019, www.ssl.com/faqs/faq-what-is-ssl/.