SSN Lab Assignment:
Symmetrical encryption

1. DES

Watch this visualization:

1. Next, use the DES simulator (launch *.jar* file). Step through the process of encrypting your name with the key 0x0101010101010101 and write the internal state of the device at the 8th round.
2. Inspect the key schedule phase for the given key and explain how the sub keys are generated for each of the 16 steps.
3. Comment on the behavior of DES when using the given key.

2. AES

Watch this visualization:

4. Identify the Shannon diffusion element(s).
5. Also identify the Shannon confusion element(s).

3. RC4

Follow these instructions, identify the URL and your personal archive accordingly, download it and inspect its contents. There are two files encrypted with the RC4 cipher. One of the files was encrypted using a 40 bit key that when represented in ASCII starts with the character a and contains only lowercase letters while the other uses a 48 bit key that can be written only with digits. Identify the encrypted files and using the brute force tool from this gist find the keys and decrypt the file. *(Most likely you will have to install the pycrypto and numpy libraries first.)*

6. (a) How did you identify the encrypted files?

   (b) What is the effective key strength for each of the keys?

(c) Instrument the code to find out how many decryption attempts you can perform in one second. Where is the most time spent ?

(d) Modify the code to support parallel execution and calculate the speedup.

(e) If the same message would be encrypted with a key of length 48 bits but which uses all the printable characters, how much time would it take to explore the full key space ?

4. AES - 2

7. Modify the code to support AES brute-force in CBC mode. How many keys can you test per second? Julian Assange has released an insurance file encrypted with AES256. Assuming that no disruptive technological breakthrough will take place in the future and the performance of CPUs will double every 18 months, when will it be possible to brute-force the file in reasonable time, i.e. less than 1year, using a single computer?