RSA

RSA is an asymmetric key algorithm used to sign or encrypt data transmission. Knowledge of this algorithm and asymmetric encryption is important in any cyber-security researcher’s toolkit. Since the algorithm runtime is long, it is often used to encrypt a key that is later used in a type of symmetric encryption, like AES. It is generally to slow to encrypt data directly. For an in-depth explanation of the algorithm I found this video by F5 DevCentral helpful:

[How RSA Works](https://www.youtube.com/watch?v=rVQpK6NcYIE)

**Lab Exercise**

The Python code included is an example of RSA implementation from Pycryptodome. Just run the script and consider the questions included. To install pycryptodome, you can use pip:

*pip install pycryptodome*