Encryption Notes

- From ibm.com/topics/encryption
    - Encryption – way of translating data from plaintext to ciphertext in order to protect it from potential attacks.
    - Two types: asymmetric and symmetric encryption
        - Asymmetric aka “Public-Key Cryptography”
            - Encrypts/decrypts data with 2 separate keys: “public” and “private”
            - RSA: encrypt with public key, decrypt with private key
            - Public key infrastructure (PKI): method of governing encryption keys through the use of digital certificates
        - Symmetric
            - Only one secret key is used to both encrypt plaintext and decrypt ciphertext
            - Data Encryption Standards (DES): low-level encryption block cipher algorithm; converts plaintext in 64-bit blocks using 48-bit key
            - Triple DES: runs DES three times – encrypts, decrypts, then encrypts again
            - Advanced Encryption Standard (AES): referred to as the gold standard for data encryption, used worldwide as U.S. government standard
            - Twofish: considered one of the fastest encryption algorithms, free to use