Cryptography Essentials

- **Hashing** – Transform messages into *deterministic*, *fixed-length* strings
- **Keys** / **Secret Keys** – Sequence of 1s and 0s used in cryptography

Symmetric Cryptography

- **Symmetric Cryptography** – set of mathematical operations that can be performed and verified/undone with *identical* keys
  - **Symmetric Encryption** – Transforms plain readable text into something unintelligible; and subsequently reverts it back to its original form
  - **Message Authentication Codes** / **HMAC** – Hashing a message in combination with a secret key to detect unauthorized changes to the message
  - **Pseudo Random Function** (**PRF**) – Generates *deterministic*, *arbitrary-length* value based on initial seed values

Asymmetric Cryptography

- **Asymmetric Cryptography**: Set of mathematical operations that can be **performed with *one* key** and **verified or undone with *another* key**
  - One key made freely available (**Public Key**); other kept secret (**Private Key**)
- Three operations:
  - **Asymmetric Encryption** - Transforms plaintext into something unintelligible using one key, and subsequently reverts it back with a different key
  - **Signatures** - Assures data has not been altered since it was signed
  - **Key Exchanges** - Allows two parties establish a mutual **shared secret**
- Three algorithms create the pillars of Asymmetric Cryptography:
  - **RSA** Algorithm can do **Encryption**, **Signatures**, and **Key Exchanges**
  - **Diffie-Hellman** (**DH**) Algorithm can only be used as for **Key Exchanges**
  - **Digital Signature Algorithm** (**DSA**) can only be used for **Signatures**