Public Key/Two-Key Encryption:

- Uses two keys: a public and a private key
- Based on mathematical functions
- Gets rid of security issue of shared keys
- Asymmetric ciphers are based on mathematical functions rather than bit-based operations
- Consists of: plaintext (message), encryption algorithm, public key, ciphertext (the encoded plaintext message), private key, and decryption algorithm.
- Use of certificated authorities to advertise public keys
- RSA used in most cases now
- Key size is always an issue if the algorithm itself isn’t attacked using cryptanalysis.
- Public key algorithms:
  - RSA
  - Diffie-Hellman
  - DSS
  - Elliptic Curve

Requirements for Public Key Systems:

- Easy for sender to encrypt with public key
- Easy for receiver to decrypt with private key
- Easy to create two keys
- Impossible for someone to determine private key from public key
- Useful if keys can be used for either role
- Impossible for someone to otherwise determine original message without keys

Digital Signatures:

- Used for authenticating integrity (not confidential)
- Encrypted hash code with private key
- Messages are safe from being altered

Digital Envelopes:

- Protects a message without a shared key
- A symmetric key is encrypted and decrypted with message using receiver’s public key and receiver’s private key, respectively.

Random Numbers:

- Should be uniform in distribution: equal occurrence of all values in range
- Should be independent: no value can be found using information from another
• Used for many security measures such as: public key algorithms, sessions keys, handshaking, etc.
• Pseudorandom numbers are sequences that are produced with possibly predictable results
• True random numbers use non-deterministic sources as a seed e.g. radiation, time, etc. with non-predictable results