Cryptography Summary:

Chapter 2: Cryptographic Tools

- **Symmetric Encryption:**
  - Uses a single key for both encryption and decryption.
  - Includes algorithms like DES, Triple DES, and AES.
  - Attacks include brute force and cryptanalysis.
- **Hash Functions:**
  - Ensure message integrity with properties like collision resistance.
  - Widely used in password storage and intrusion detection.
- **Public-Key Encryption:**
  - Asymmetric approach using public and private keys.
  - Algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography.
- **Digital Signatures:**
  - Provide authentication, data integrity, and non-repudiation.
  - Examples: DSA, RSA, ECDSA.
- **Random Numbers:**
  - Used for key generation, session keys, and preventing replay attacks.
  - Can be truly random (TRNG) or pseudorandom.

Chapter 20: Symmetric Encryption and Message Confidentiality

- **Symmetric Encryption Basics:**
  - Conventional encryption with five ingredients: plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.
  - Key distribution is a critical challenge.
- **Encryption Techniques:**
  - **Block Cipher Structure:** Substitutions and permutations with parameters like key size and rounds.
  - **Stream Ciphers:** Encrypts data one element at a time; faster but less common than block ciphers.

- **Key Algorithms:**
  - DES, Triple DES, AES.
  - Modes of operation: ECB, CBC, CFB, OFB, CTR.
- **Key Distribution Methods:**
  - Includes physical delivery, encryption with existing keys, and third-party key delivery.

Chapter 21: Public-Key Cryptography and Message Authentication

- **Hash Functions (SHA):**
  - Examples include SHA-1, SHA-2, and SHA-3.
  - Applications include message authentication and integrity.
- **HMAC:**
  - Combines cryptographic hash functions with a secret key for integrity and authenticity.
- **RSA Encryption:**
  - Based on exponentiation modulo a large prime.
  - Public-private key structure for encryption and decryption.
- **Diffie-Hellman Key Exchange:**
  - Enables secure key exchange over an insecure channel.
  - Relies on the difficulty of computing discrete logarithms.
- **Cryptographic Attacks:**
  - Brute force, mathematical, timing, and chosen ciphertext attacks.
  - Countermeasures include constant execution time, random delays, and blinding.