🔒 Cipher / Algorithm Cheat Sheet (Security+ Focus)

1. Symmetric Encryption (same key for encrypt & decrypt)

👉 **Block Ciphers** (fixed-size blocks: 64-bit, 128-bit, etc.)

- **DES** – 56-bit key, **deprecated** (broken).
- **3DES (Triple DES)** – applies DES 3×, but slower. **Deprecated**.
- **AES (Advanced Encryption Standard)** – 128/192/256-bit, **recommended replacement for DES/3DES**.
- **IDEA (International Data Encryption Algorithm)** – used in older PGP, **largely replaced by AES**.
- **Blowfish / Twofish** – alternative block ciphers (Twofish was an AES finalist).

👉 **Stream Ciphers** (bit/byte at a time, faster, used in real-time comms)

- **RC4** – used in old SSL/WEP; **deprecated, insecure**.
- **ChaCha20 / Salsa20** – modern, secure stream ciphers (ChaCha20 often used in TLS instead of AES).

2. Asymmetric Encryption (keypair: public/private)

Used for **key exchange, authentication, digital signatures**.

- **RSA** – encryption + digital signatures; still common.
- **ECC (Elliptic Curve Cryptography)** – more efficient than RSA, smaller key sizes.
- **DSA (Digital Signature Algorithm)** – used for signatures only.
- **ECDSA** – elliptic curve version of DSA.
- **Diffie-Hellman** – key exchange (not encryption itself).
- **ElGamal** – asymmetric encryption, less common now.

👉 Exam trap: Asymmetric is *never* used for encrypting bulk data — only for exchanging keys or signing.

3. Hashing Algorithms (fixed-length, one-way, integrity)

- **MD5** – 128-bit, broken, not recommended.
- **SHA-1** – 160-bit, deprecated.
- **SHA-2 (SHA-256, SHA-512, etc.)** – secure, recommended.
- **SHA-3** – newest standard, secure.
- **RIPEMD** – secure but less common.
- **HMAC (Hash-Based Message Authentication Code)** – adds a secret key to hashing for authentication.

4. Block Cipher Modes of Operation (how block ciphers are applied)

- **ECB (Electronic Codebook)** – simplest, weakest (patterns show). ❌ Not recommended.
- **CBC (Cipher Block Chaining)** – uses IV, better than ECB.
- **CFB (Cipher Feedback)** – turns block cipher into **stream cipher**.
- **OFB (Output Feedback)** – also stream-like, less common.
- **CTR/CTM (Counter Mode)** – uses counter + key → turns block into stream.
- **GCM (Galois/Counter Mode)** – based on CTR, but adds authentication (integrity + confidentiality). **Recommended** in modern protocols (TLS, IPsec).

5. What Replaces What (Security+ Exam Gotchas)

- **DES → replaced by AES**
- **3DES → replaced by AES**
- **IDEA → replaced by AES**
- **RC4 → replaced by AES (or ChaCha20 in some modern protocols)**
- **MD5 / SHA-1 → replaced by SHA-2 or SHA-3**

6. Key Management Concepts

- **IV (Initialization Vector):** random value, prevents identical plaintext from making identical ciphertext. Not secret.
- **Salt:** random value added to passwords before hashing → defends against rainbow tables.
- **Nonce ("number used once"):** similar to IV, ensures uniqueness.
- **KDC (Key Distribution Center):** Kerberos component, hands out TGTs.
- **TGT (Ticket-Granting Ticket):** proof of identity.
- **TGS (Ticket-Granting Service):** issues service tickets for specific resources.