Security Search Task

1. Semantic Algorithm

Meaning

A semantic algorithm is designed to understand the meaning and context of data rather than just its structure or keywords.

Used in

- Artificial Intelligence and Natural Language Processing (NLP)
- Search engines (like Google) — to understand the *intent* behind your search query.
- Chatbots and language models (like ChatGPT).

Example

When you search “best laptop for gaming,” a semantic algorithm understands that you mean high-performance laptops, not just the words “best” and “gaming.”

2. Asymmetric Algorithm

Meaning

An asymmetric algorithm (also called public-key cryptography) uses two different keys — a public key and a private key — for encryption and decryption.

Used in

- Secure communications
- Digital signatures.
- Online banking and HTTPS connections.

How it works

- You encrypt a message with the **public key**.

- Only the **private key** can decrypt it.

Examples

- RSA (Rivest–Shamir–Adleman)
- ECC (Elliptic Curve Cryptography).
- DSA (Digital Signature Algorithm).

3. Hashing Algorithm

Meaning

A hashing algorithm converts any input data into a fixed-size string (called a hash value or digest).

Used in

- Storing passwords securely.
- Checking file integrity.
- Blockchain technology.
- Data lookup (hash tables).

Key Properties

- **Deterministic** – same input → same hash.
- **Fixed size** – no matter the input length.
- **Collision-resistant** – hard to find two inputs with the same hash.

Examples

- **MD5** (old, insecure)
- **SHA-1 / SHA-256** (secure, commonly used).
- **BLAKE2 / BLAKE3** (modern, fast alternatives).