DISECTO
Paradigm Shifting Data Security

SDE (Python/Golang)

You can choose any ONE of the two tasks and share it as per the instructions given below.

Submission:

1. You can choose either Python or Golang for these problems
2. Keep the codebase on Git and share the link with us.
3. Write a short Readme file on Git for the project to explain your approach
4. Share all the necessary documents and links on the same mail chain of this Task.

Expectations:

1. Error handling & validation should be robust to handle any scenario.
2. Code Clarity
3. The standards you follow to write your code would play a good role in increasing your chances.
4. Estimated time for task submission is 4-5 days

DISECTO
Paradigm Shifting Data Security

Tasks:

Option 1. Cryptography

The problem will introduce you to the interesting concept of Homomorphic Encryption which is a unique property of some of the crypto algorithms.

1. Read about Homomorphic Encryption (HE)
    - Starting Point: https://blog.nucypher.com/an-engineers-guide-to-fully-homomorphic-encryption/
2. Implement Encryption and Decryption functions in any HE/Partially HE algorithm (Lattice-based preferred)
    - Feel free to use existing libraries in Python/Golang
3. Demonstrate the additive and multiplicative property of the chosen algorithm

The evaluation criteria will be based on the approach you follow in tackling the problem rather than the solution itself.

Option 2. Elastic Search

This task will give you an understanding of how to approach problems pertaining to very large datasets in terms of searchability.

1. Start with a large Dataset (100million-1 billion records). (Link for large dataset) or you can generate a custom DB with five simple fields (Name, Address, Phone Number, Gender, Date of Birth)
2. Use the open-source Elastic Library to perform search on different columns
3. Brownie Points for use of Fuzzy Search and implementation of string-based percentage Matching.
4. Benchmark the results for both the search terms available and not-available in the DB

Here the evaluation criteria will be based on the approach you follow in terms of the architecture of the deployed code; Pre-processing and Loading of Data, Database Architecture [Elastic DB, SQL, CSV, ZomboDB etc.]