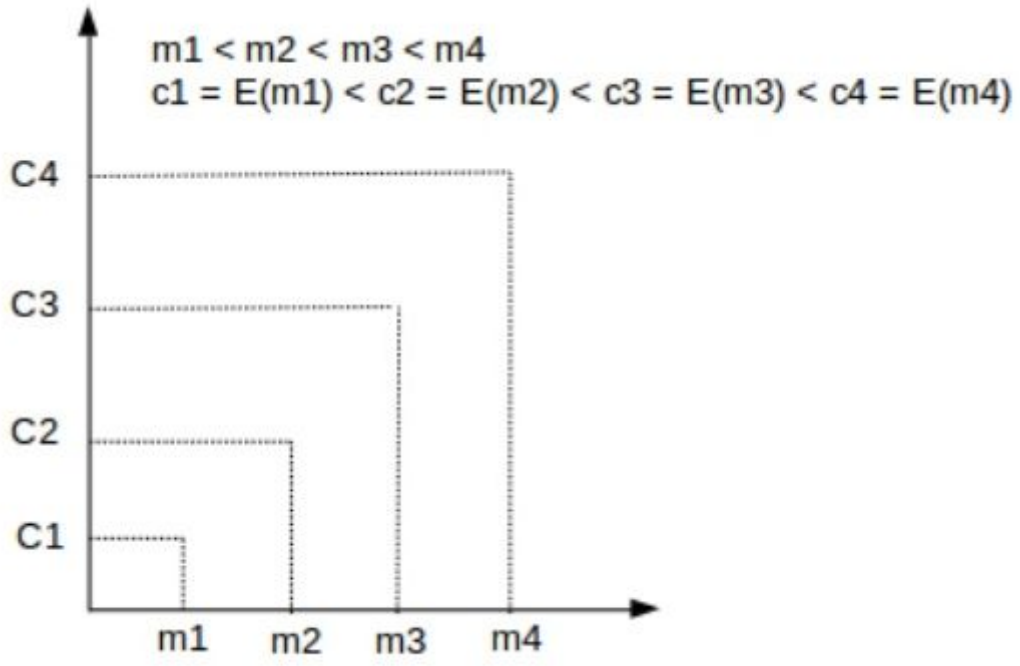
Order-Preserving Encryption (OPE) - Introduction

- Initially introduced by Agrawal et al. (SIGMOD 2004) to efficiently perform range queries on encrypted databases
- OPE is a deterministic symmetric encryption scheme with an encryption algorithm that preserves numerical ordering of plaintexts in the ciphertexts
- Hence, records in an untrusted database can be encrypted using an OPE scheme, while maintaining the database functionality
    - e.g. a range query can consist of the encryptions of the two end-points of a given range and the database returns all ciphertexts that fall into this range
- Even if the OPE scheme uses a strong encryption algorithm, it is possible to reconstruct parts of the encrypted data, due to the order-preserving property

Example for OPE:
Let E(・) be a deterministic symmetric encryption algorithm.
Let m1, m2, m3 and m4 be plaintext messages.
Let c1, c2, c3 and c4 be ciphertext messages.
Then the following figure illustrates the concept of an order preserving encryption scheme:



Reference: Nagendra Posani, Georgia Institute of Technology,
https://www.slideshare.net/NagendraChowdary/searchable-encryption