Exploiting Weaknesses of Order-Preserving Encryption

Goal

In this challenge, you will see that it's not always necessary to break encryption in order to infer information from protected data. We're showcasing this in this challenge using the example of Order-Preserving encryption (http://cryptowiki.net/index.php?title=Order-preserving_encryption). Order-Preserving encryption (OPE) has been quite popular for some time, because it allowed to upload encrypted data to a database, while maintaining full database functionality. However, along with the benefits of OPE, there are some weaknesses.

Scenario

You will be given read access to a MySQL database, which contains sensitive personal data *(ID, FirstName, Name, Age, Address, Profession, Income)*. The data is encrypted using an Order-Preserving encryption scheme, except for the attribute *ID*, which is unencrypted in order to perform queries more efficiently.
You know that the dataset contains persons of age starting from 1 and that there's only one person of age 25.

Challenge

1) Find the only person of age 25 and find out the income of that person.
2) Find the age of the person with id 1001.

Technical Details

Install any MySQL client of your choice and connect to the database using the following credentials:

hostname: mysqltest.c1yf7tazddjt.us-east-1.rds.amazonaws.com
port: 3306
username: h4ck3r
password: 31337

Having connected to MySQL, select the schema "Montrehack" and use the table "PersonalData".