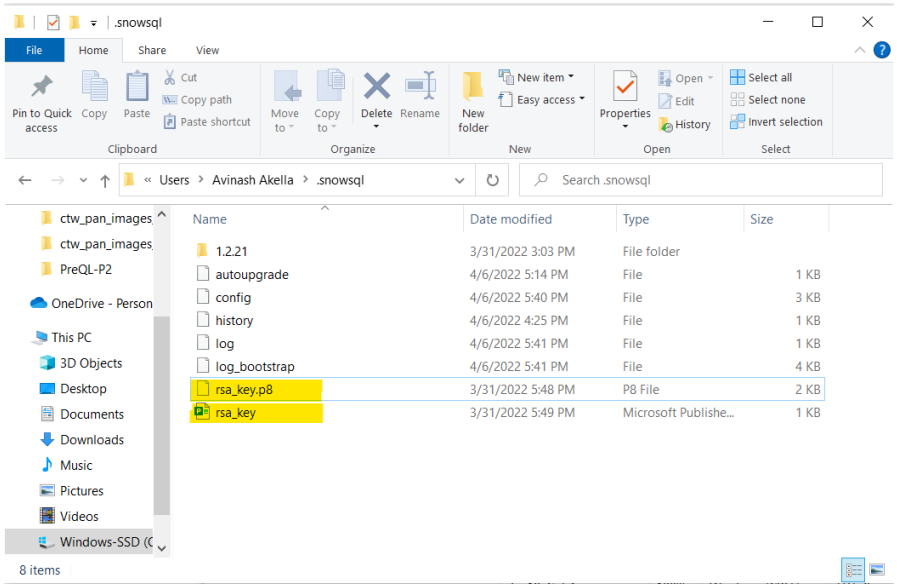
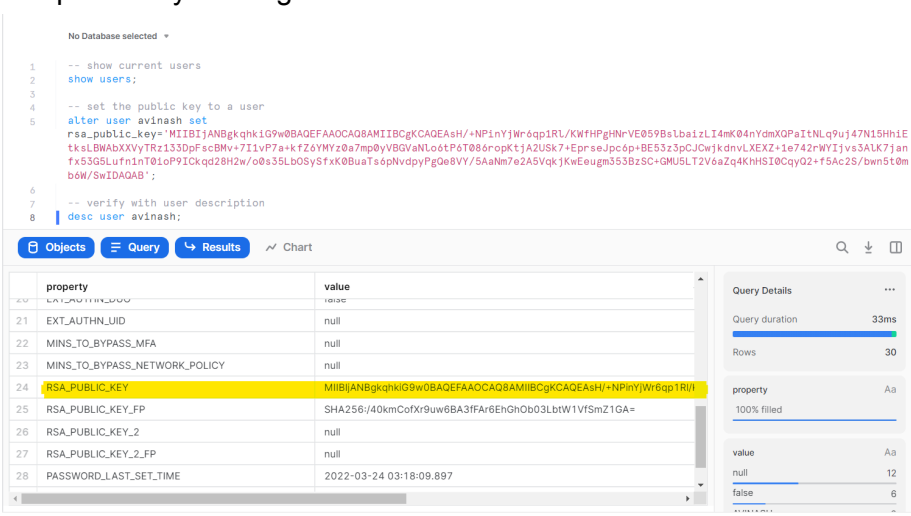
1. Public and Private keys are generated using OpenSSL. The encrypted private key is stored in the rsa_key.p8 file and the public key is stored in the rsa_key.pub file.



2. The public key is assigned to the Snowflake user.



3. The Snowflake configuration file is modified to include the file path to the private key. Notice that we don't need to reveal our account credentials with this approach.

```
config
C: > Users > Avinash Akella > .snowsql > config
[connections]
# *WARNING* *WARNING* *WARNING* *WARNING* *WARNING* *WARNING*
#
# The Snowflake user password is stored in plain text in this file.
# Pay special attention to the management of this file.
# Thank you.
#
# *WARNING* *WARNING* *WARNING* *WARNING* *WARNING* *WARNING*

#If a connection doesn't specify a value, it will default to these
#
#accountname = defaultaccount
#region = defaultregion
#username = defaultuser
#password = defaultpassword
#dbname = defaultdbname
#schemaname = defaultschema
#warehousename = defaultwarehouse
#rolename = defaultrolename
#proxy_host = defaultproxyhost
#proxy_port = defaultproxyport

private_key_path = C:\Users\Avinash Akella\.snowsql\rsa_key.p8
```

4. To decrypt the encrypted private key, we set the SNOWSQL_PRIVATE_KEY_PASSPHRASE in the command prompt using the 'set' command in windows. This is used to decrypt the private key. We can then connect to Snowflake without having to enter the credentials.

```
Command Prompt - snowsql  -a xt67644.ca-central-1.aws -u Avinash
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Avinash Akella>set SNOWSQL_PRIVATE_KEY_PASSPHRASE=snowflakeproject

C:\Users\Avinash Akella>snowsql -a xt67644.ca-central-1.aws -u Avinash
* SnowSQL * v1.2.21
Type SQL statements or !help
Avinash#COMPUTE_WH@(no database).(no schema)>
```