Course 3_Lab 5: Create symmetric and asymmetric keys

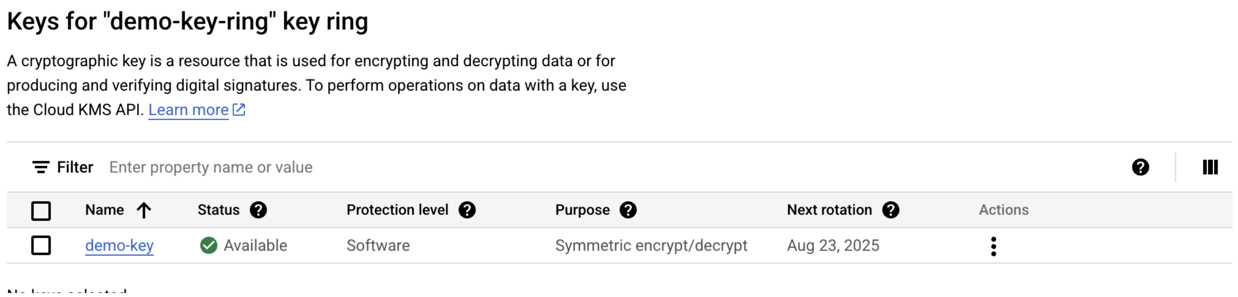
Scenario

Cymbal Bank stores and processes large amounts of sensitive customer data including financial transactions and personally identifiable information (PII). The CISO, Javier, wants to protect the confidentiality, integrity, and availability of this data while it's at rest, in transit, and in use. Cymbal Bank wants to transfer a large volume of its data from its on-premises servers to the cloud. Your team lead, Chloe, has suggested using a cloud key management system to create and manage encryption keys to facilitate the secure transmission of this data. You have been tasked with creating a symmetric key and an asymmetric key to support this data transmission.

Here's how you'll do this task: **First**, you'll create a symmetric key. **Then**, you'll create an asymmetric key.

MY WORK:
Task 1: Create a symmetric key

In this lab I used Key Management in Google Cloud Platform to create a symmetric key. The lab encompassed setting a location, key rotation period, and protection level for the key.

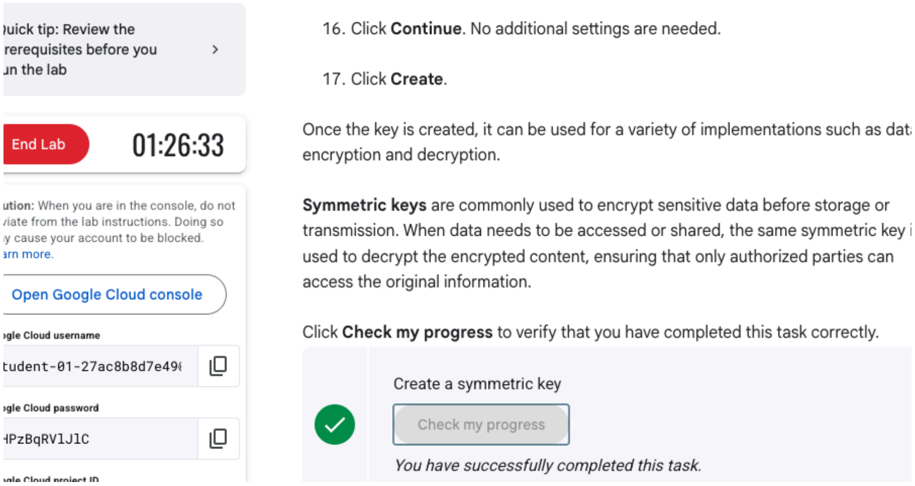


Keys for "demo-key-ring" key ring

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

Filter Enter property name or value

□	Name ↑	Status	Protection level	Purpose	Next rotation	Actions
□	demo-key	✓ Available	Software	Symmetric encrypt/decrypt	Aug 23, 2025	⋮



16. Click **Continue**. No additional settings are needed.

17. Click **Create**.

Once the key is created, it can be used for a variety of implementations such as dat encryption and decryption.

Symmetric keys are commonly used to encrypt sensitive data before storage or transmission. When data needs to be accessed or shared, the same symmetric key i used to decrypt the encrypted content, ensuring that only authorized parties can access the original information.

Click **Check my progress** to verify that you have completed this task correctly.

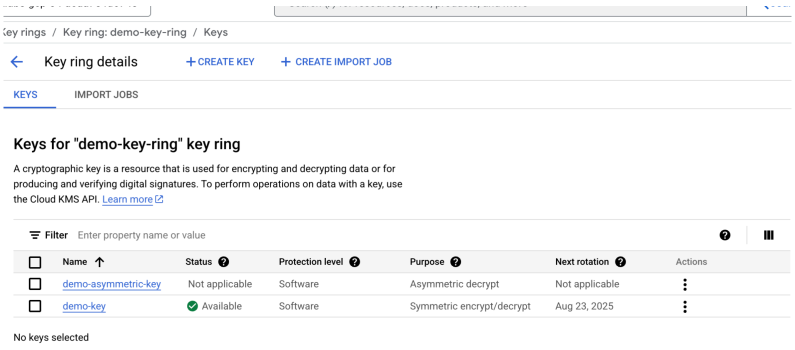
Create a symmetric key

Check my progress

You have successfully completed this task.

Task 2: Create an asymmetric key

In task 2, I created an asymmetric key in Google Cloud Platform. With the exception of a few steps,, the process was the same. Some different steps in the formation of the key included, considering the algorithm and version values, while not inputting a region, or key rotation period for the key.



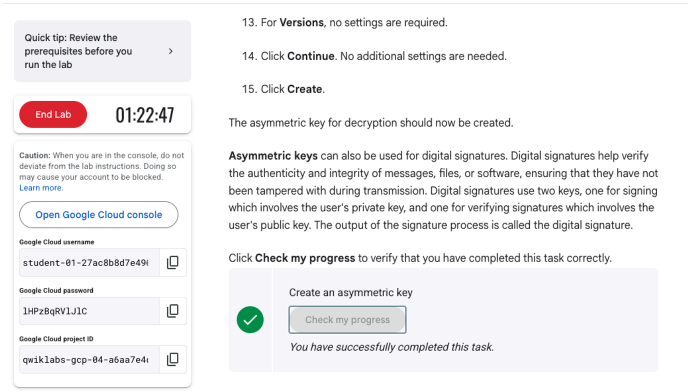
Keys for "demo-key-ring" key ring

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

Filter Enter property name or value

□	Name	Status	Protection level	Purpose	Next rotation	Actions
□	demo-asymmetric-key	Not applicable	Software	Asymmetric decrypt	Not applicable	⋮
□	demo-key	✓ Available	Software	Symmetric encrypt/decrypt	Aug 23, 2025	⋮

No keys selected



Quick tip: Review the prerequisites before you run the lab
End Lab
01:22:47

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username: student-01-27ac8b8d7e49

Google Cloud password: 1HPzBqRV1J1C

Google Cloud project ID: qwiklabs-gcp-04-a6aa7e4

13. For **Versions**, no settings are required.
14. Click **Continue**. No additional settings are needed.
15. Click **Create**.

The asymmetric key for decryption should now be created.

Asymmetric keys can also be used for digital signatures. Digital signatures help verify the authenticity and integrity of messages, files, or software, ensuring that they have not been tampered with during transmission. Digital signatures use two keys, one for signing which involves the user's private key, and one for verifying signatures which involves the user's public key. The output of the signature process is called the digital signature.

Click **Check my progress** to verify that you have completed this task correctly.

✓ Create an asymmetric key

You have successfully completed this task.

My Assessment

In this lab I created a symmetric and asymmetric key that can be used to encrypt data.

What are encryption keys: To start, encryption is the process of securing data through ciphertext so it is not accessed by unauthorized users. Encryption keys are a random string of bits used to convert plain text to ciphertext and can also be used for decryption by an authorized user with the key.

Symmetric Key- This type of key allows data to be encrypted and decrypted with the same key if the user has access. This key is commonly used for data at rest (storage/stored data) and data in transit (traversing between locations).

Asymmetric Key - This type of key allows data to be encrypted with one key (public) and decrypted by another key (private). The private key must remain private in order for the data to remain secure.