This page describes how to use your own encryption key, referred to as a *customer-supplied encryption key*, with Cloud Storage. For details about this feature, including countries where it's available, see Customer-Supplied Encryption Keys (/storage/docs/encryption/customer-supplied-keys). For other encryption options in Cloud Storage, see Data Encryption Options (/storage/docs/encryption).

There are many ways to generate a Base64-encoded (https://tools.ietf.org/html/rfc4648#section-4) AES-256 encryption key. Here are several examples:

To use customer-supplied encryption keys to upload an object:

To download an object stored in Cloud Storage that is encrypted with a customer-supplied encryption key:

To rotate a customer-supplied encryption key:

Rotating encryption keys involves overwriting data. Nearline Storage, Coldline Storage, and Archive Storage objects h
eletion (/storage/pricing#archival-pricing) charges if they are overwritten less than 30 days, 90 days, or 365 days fr
reation time, respectively.