Google Cloud

Cryptographic keys for data protection

So far, you've learned that encryption is the process of converting data from a readable format to an encoded format. You've also learned there are different types of encryption, including symmetric and asymmetric encryption. Both of these encryption types require keys to decrypt the encrypted information. It's like using keys to open a locked door or box. In this reading, you'll learn more about keys, and review an example of a key being made and used.

What are keys and how do they work?

Keys are values you use to control cryptographic operations like decryption and encryption. Cryptographic algorithms substitute characters for other characters, and transpose letters by moving them around in a message. To accomplish this, the cryptographic algorithms generate keys and use them to encrypt and decrypt user information.

Here's an example of how keys are made, using public key cryptography. Imagine you're a data professional who is sending a message to a colleague. In public key cryptography, you have two keys: a public key and a private key. The public key is available for anyone to use, but the private key is kept secret. First, take a plain text message: "Hello." Now you encrypt the message with a key. For example, you decide to use "jd8932kd8" for the key. Now, your message now reads "X5xJCSycg14=". The message is now locked behind this data, and appears to be nonsense to anyone trying to access it without a key. Trying to read that message is like trying to find out what's behind a locked door by simply turning the knob. Only the private key can be used to decrypt the nonsense message and show you the "Hello." message instead.

What is key management?

Having a secure key management system is vital. Think about what happens when someone loses the key to their home. Now they can't get in. The same thing happens if an organization loses its keys to data. They're locked out of their data. The management of cryptographic keys in a cryptosystem is called **key management**. Cloud providers usually offer key management solutions to their users, and offer services that help you manage your keys the same way you do with on-premises environments.

Pro tip: Immediately revoke access to any key version that you suspect is compromised.

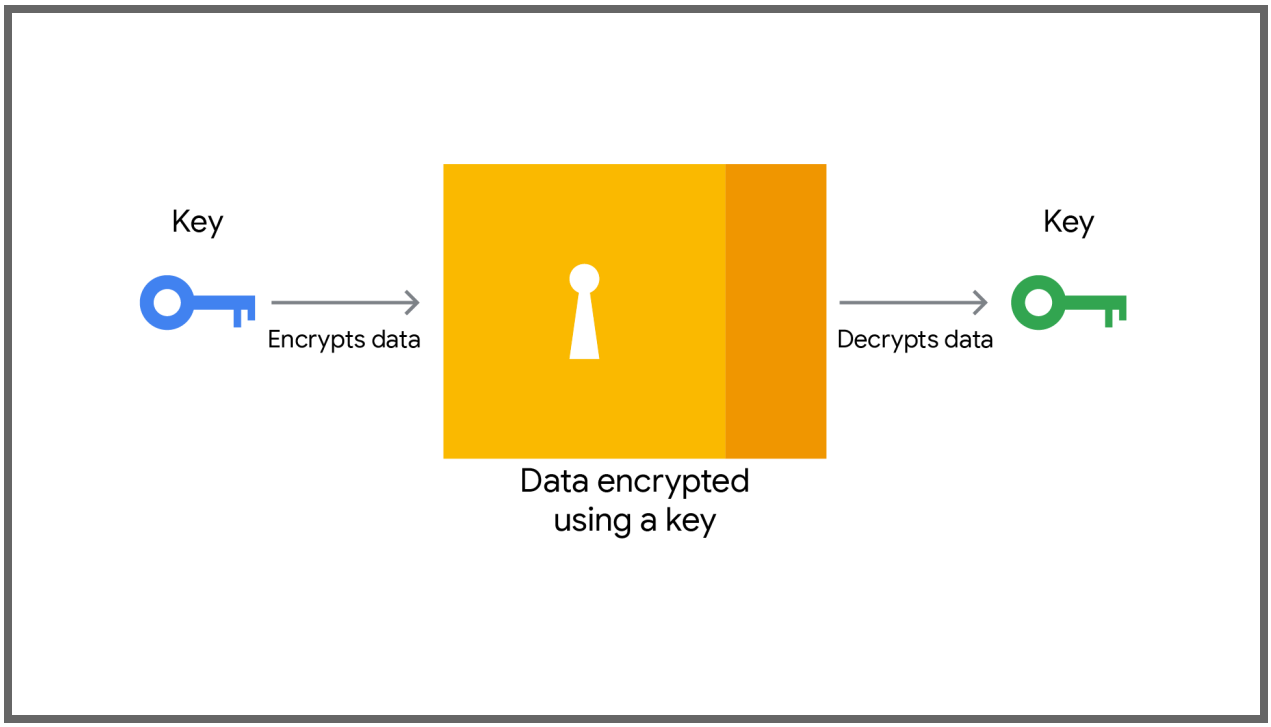
Note: Automatic key rotation is an effective security practice, but you may need to rotate keys manually if:

- You suspect that a key has been compromised
- You are migrating an application to a stronger key algorithm and your security guidelines require you to manually rotate the key

Key rotation benefits

You need to set rotation periods when you create keys. The benefits to key rotation include:

- It helps prevent attackers from deciphering coded messages by limiting the number of encrypted messages using the same key. This process is called cryptanalysis, or the process of deciphering coded messages. By rotating keys regularly, you limit the number of encrypted messages that use the same key. This makes it more difficult for attackers to decrypt your data.
- It reduces the impact of a key compromise. If a key is compromised, rotating keys regularly limits the amount of data that can be accessed by attackers.
- It also ensures your system is resilient to manual rotation. Key rotation may be necessary because of security incidents or algorithm updates. Rotating keys regularly ensures that your system is prepared for manual rotation.



Envelope encryption

Key management can use multiple layers of keys for encrypted data. An example of this is envelope encryption. **Envelope encryption** is the process of encrypting a key with another key. In this process, a **data encryption key** (**DEK**) encrypts the data. The data encryption key

itself is then encrypted by a **key encryption key** (**KEK**).

To use envelope encryption, first you need to generate a data encryption key locally to encrypt the data. Next, use a key encryption key to wrap the data encryption key. Finally, store the encrypted data and the wrapped data encryption key.

Two primary benefits of envelope encryption include:

1. Easier key rotation: For example, this includes rotating only one KEK instead of re-encrypting all the data that is encrypted with the DEKs.
2. Asymmetric encryption: For example, asymmetric encryption can be used for the KEK while still efficiently encrypting large amounts of data using a symmetric DEK.

When you are finished with keys

When you're finished, you can disable a key. Once your key is disabled, you can't access the data encrypted with that key unless you enable it again. Disabling a key may take some time. You can also destroy a key if you know you'll never need it again. In Google Cloud Key Management, the key stays in the **scheduled for destruction** state for a while just in case.

Key takeaways

Keys are created using encryption algorithms. You can use keys to encrypt and decrypt data, so that it's secure, and only accessible to those with the key. This keeps your data safe and confidential. Key management allows you to manage your keys, and most cloud providers offer key management solutions.When you make keys, you should set rotation periods for them. Once you're finished with your keys, you can either disable them temporarily, so you can enable them again later, or destroy them. If you disable them, you won't be able to access your data.