Google Cloud

Asymmetric versus symmetric encryption

So far, you've learned that encryption protects your data at rest, in use, and in transit. These states of data use encryption to convert data from a readable format to an encoded format. In this reading, you'll learn more about encryption and explore two types of cryptography: symmetric and asymmetric. You'll also learn how to use these processes to protect your data.

Cryptography

Cryptography is the process of transforming information into a form that unintended readers can't understand. Cryptography includes encryption and decryption techniques to keep your data secure. Encryption uses algorithms to encode messages, and decryption uses algorithms to decode messages. Symmetric and asymmetric encryption are two types of encryption used in cryptography.

Encryption at rest

Encryption at rest sometimes uses symmetric encryption to help protect data stored on a disk. This also includes data stored on a hard drive. But, encryption at rest can also use asymmetric encryption. Encryption at rest ensures that if an attacker accesses your data, they still need access to the encryption keys to use it. So, even though the attacker has the data, it's useless to them since it's still encrypted.

Encryption at rest also cuts out the lower layers of the hardware and software stack. Ideally, it works as a chokepoint, since centrally managed keys create a single place where access to data can be audited and enforced. This lets businesses focus their protection strategies on the encryption keys, which reduces the attack surface.

Encryption in transit

Encryption in transit sometimes uses symmetric encryption. But, it can also use asymmetric encryption. Encryption in transit is used to protect data if communications are intercepted. It achieves this by authenticating the endpoints, and encrypting the data before it's transmitted. Endpoint authentication verifies the identity of a user or a service connecting remotely to a network. So, once the data arrives at the endpoint, it decrypts the data and ensures the data wasn't modified.

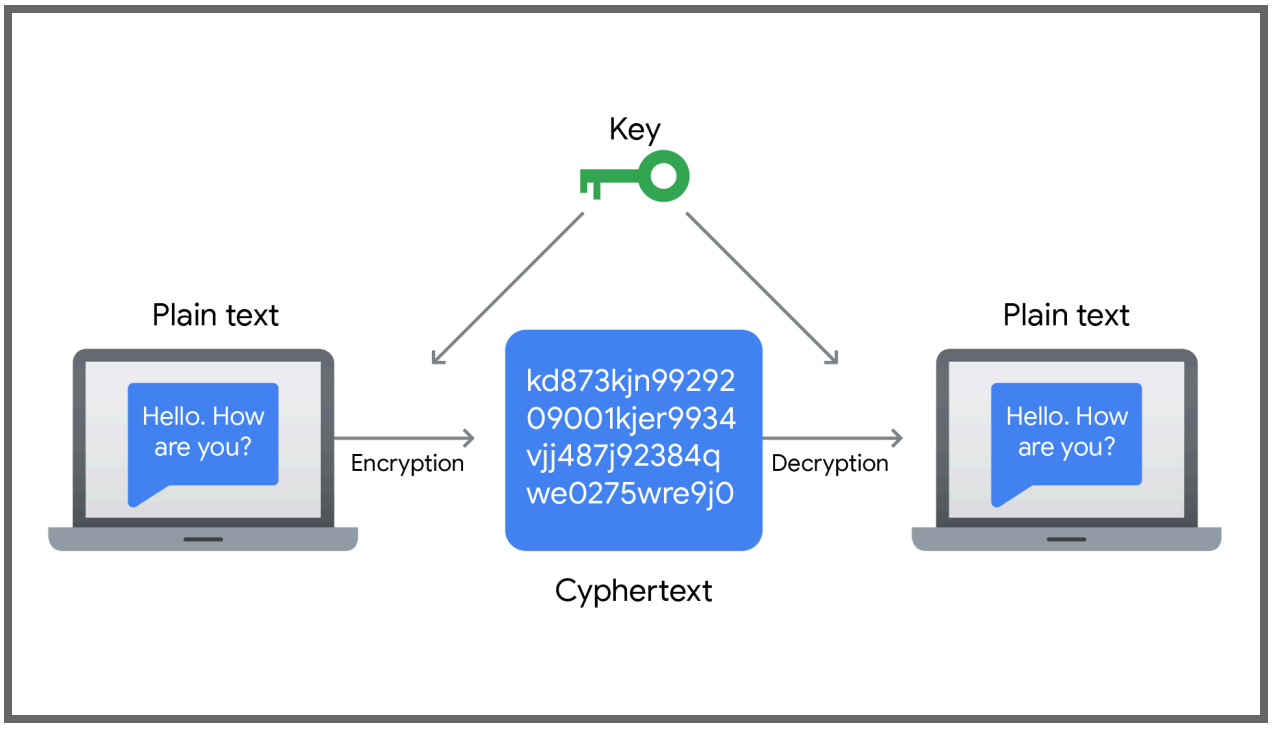
Like with encryption at rest, encryption in transit removes the need to trust the lower layers of the network, reduces the potential attack surface, and prevents attackers from accessing data if they intercept communications. Secure Socket Layer/Transport Layer Security (SSL/TLS) is

the most common protocol used for encryption in transit.

Symmetric encryption

Symmetric encryption is the use of a single key to exchange information. Symmetric encryption is also known as the shared or private key algorithm because it needs one key to encrypt and decrypt information. Two benefits of symmetric encryption are its ability to handle high rates of data and use less computational power. For example, banks and banking apps handle millions of transactions a day, so they use symmetric encryption to handle large amounts of data.

Despite these benefits, ensuring a secure exchange of the shared key can be a challenge. Anyone who gains access to a key, including a malicious actor, can decrypt anything sent between the parties. This includes any messages or data. So, the shared key transfer needs to be adequately secured. This can be accomplished by encrypting it with a different type of cryptographic key.



Common symmetric models

Symmetric encryption has evolved over time. Advanced Encryption Standard (AES) is the most widely used form of symmetric encryption. AES allows for fast encryption and decryption, and can be implemented easily.

Asymmetric encryption

Asymmetric encryption uses both a public and private key for encrypting and decrypting data. The public key encrypts the data being sent, and the private key decrypts the data. Anyone with the public key can send encrypted messages. But only those who have the private key can decrypt the sent messages. With a public and private key pair, you can use your own private key to digitally sign data. Using the public key, the authenticity and integrity of this data can be verified.

For example, a public key is like a bank account number that can be shared with anyone. Sharing the number won't give anyone access to the account holder's financial information. In contrast, a private key is like an ATM PIN number. A PIN number should never be shared with anyone. If shared, the person with the PIN will have access to financial information that gives them direct access to your bank account. This is something to avoid.

Common asymmetric model

One common method of asymmetric encryption is Rivest-Shamir-Adelman (RSA). This is one of the original forms of asymmetric encryption where two prime numbers are factored and an auxiliary value is added to create a public key. Anyone can use the public key to encrypt data, but only someone with the prime number code can decrypt the data. The keys can be very large, with 2,048 and 4,096 bits as two examples of typical sizes.

Note: Because the keys used for asymmetric encryption can be very large, it requires more computing power. So, this type of encryption is not suited for large packets of data.

Symmetric and asymmetric encryption in action

Both symmetric and asymmetric encryption are used for data encryption. Different situations call for different types of encryption.

Symmetric encryption is used by businesses like financial institutions because it can encrypt large amounts of information in bulk. For example, a bank decides to provide an app for customers to pay for services and products using their mobile devices. The bank deals with millions of transactions, so they need bulk encryption. The app uses symmetric encryption to verify users are who they claim to be, and to protect the users' Personal Identifying Information (PII).

The bank then decides to create its own messaging app for its users. The app uses end-to-end encryption to protect their users, and to authenticate them. The two types of encryption work together for this task. If a user wants to communicate with the bank, a symmetric key is created in the user's app. This symmetric key is encrypted with the bank's public key. So, the symmetric key can be securely transferred to the bank. The bank decrypts the symmetric key with its

private key. Now, both parties have access to the same symmetric key, so they can exchange larger volumes of data to leverage the more efficient symmetric encryption model.

Key takeaways

Cryptography is an essential part of protecting data from being read by unauthorized individuals. Symmetric encryption uses one key to exchange information, while asymmetric encryption uses a public and private key to encrypt and decrypt data. While the encryption types differ in how information is exchanged, they both ensure only authorized users can read the data. As a cloud security professional, you'll likely use asymmetric and symmetric encryption to secure data in a variety of situations. With an understanding of what they do, you'll be better prepared to use them.