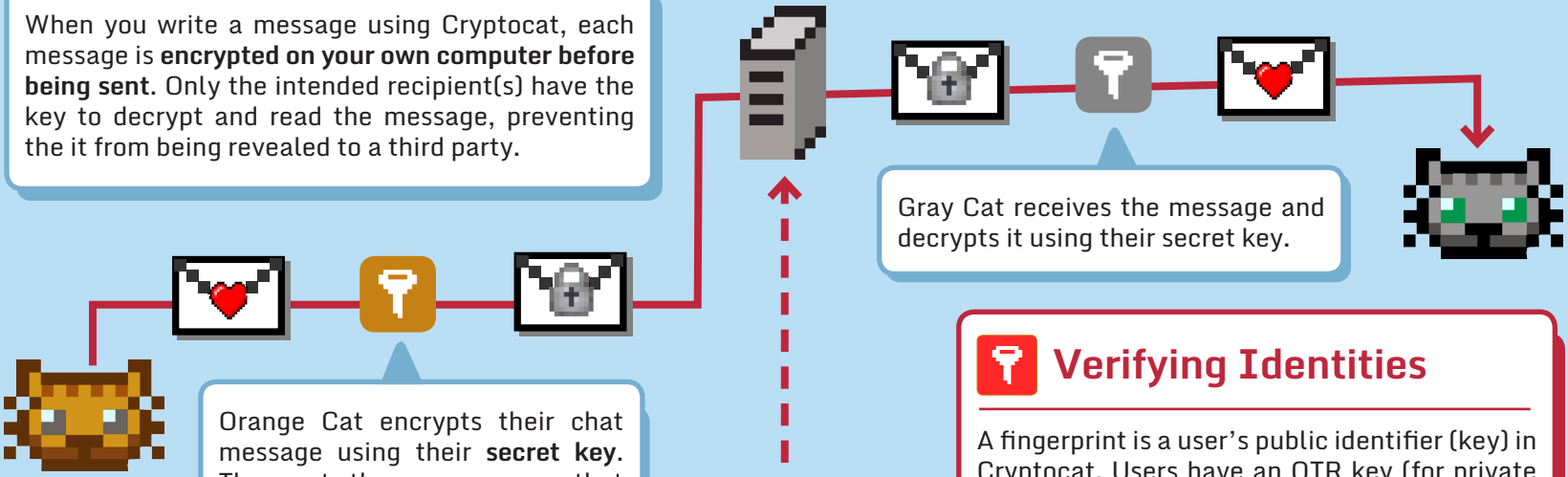
HOW CRYPTOCAT WORKS

When you write a message using Cryptocat, each message is **encrypted on your own computer before being sent.** Only the intended recipient(s) have the key to decrypt and read the message, preventing the it from being revealed to a third party.



Orange Cat encrypts their chat message using their **secret key**. They set the message so that **only Gray Cat can decrypt it** using Gray Cat's secret key. When the message passes through the server, it is already encrypted--if it's intercepted, Spy Dog can't read it.

Gray Cat receives the message and decrypts it using their secret key.

SPYDOG THWARTED!!

Verifying Identities

A fingerprint is a user's public identifier (key) in Cryptocat. Users have an OTR key (for private conversations) and a group conversation fingerprint. Confirming someone's key using a third channel (voice, DM) is one way to verify that the person you're talking to is who you think it is. **Every time you use Cryptocat, you get a new fingerprint set.** So you need to verify that identity every time.