**JWT**

JSON Web Token is a proposed Internet standard for creating data with optional signature and/or optional encryption whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a public/private key.



jwt-go

Useful links:

1. <https://pkg.go.dev/github.com/dgrijalva/jwt-go>
2. <https://jwt.io/introduction>
3. <https://github.com/golang-jwt/jwt>

What is JWT?

JSON web token (JWT), pronounced “jot”, is **an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object**. Again, JWT is a standard, meaning that all JWTs are tokens, but not all tokens are JWTs.

Is JWT a cryptography?

JWT, or JSON Web Token, is an open standard used to share security information between two parties --- a client and a server. Each JWT contains encoded JSON objects, including a set of claims. **JWTs are signed using a cryptographic algorithm** to ensure that the claims cannot be altered after the token is issued.

How exactly JWT works?

How it works? Basically **the identity provider ( IdP ) generates a JWT certifying user identity and Resource server decodes and verifies the authenticity of the token using secret salt / public key**. User sign-in using username and password or google/facebook.

What is JWT vs TLS?

TLS Mutual Authentication

The difference between the two approaches is, **in JWT-based authentication, the JWS can carry both the end user identity as well as the upstream service identity**. With TLS mutual authentication, the end user identity has to be passed at the application level.

Is JWT private or public key?

**The jwt token is signed using private key**. The auth server provides the public key publicly on a url in the form of JSON Web Key Set(JWKS). During verification public keys are fetched.

**HMAC**

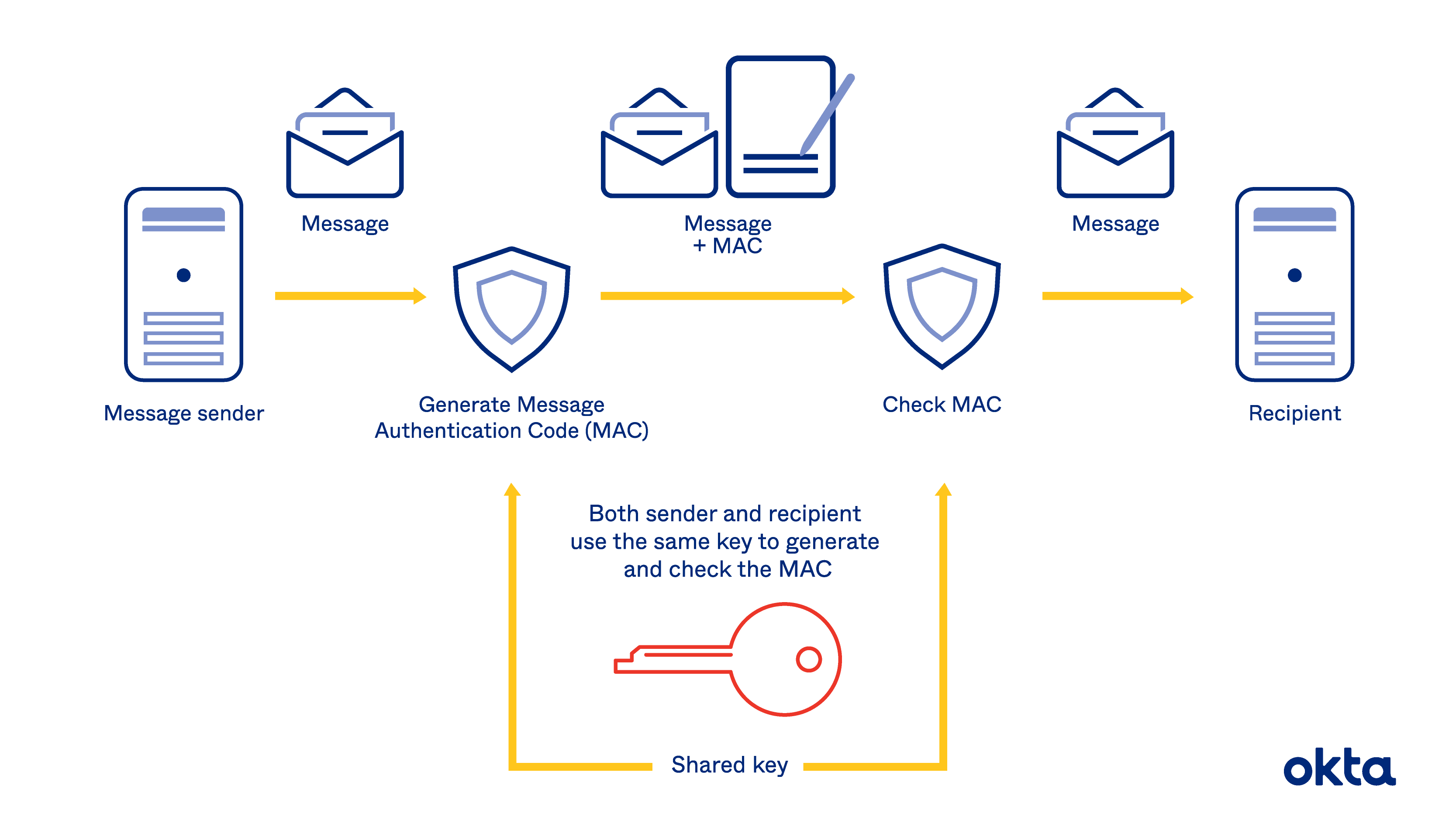
Hash-based message authentication code (or HMAC) is **a cryptographic authentication technique that uses hash function and a secret key**. With HMAC, you can achieve authentication and verify that data is correct and authentic with shared secrets, as opposed to approaches that use signature and asymmetric cryptography.

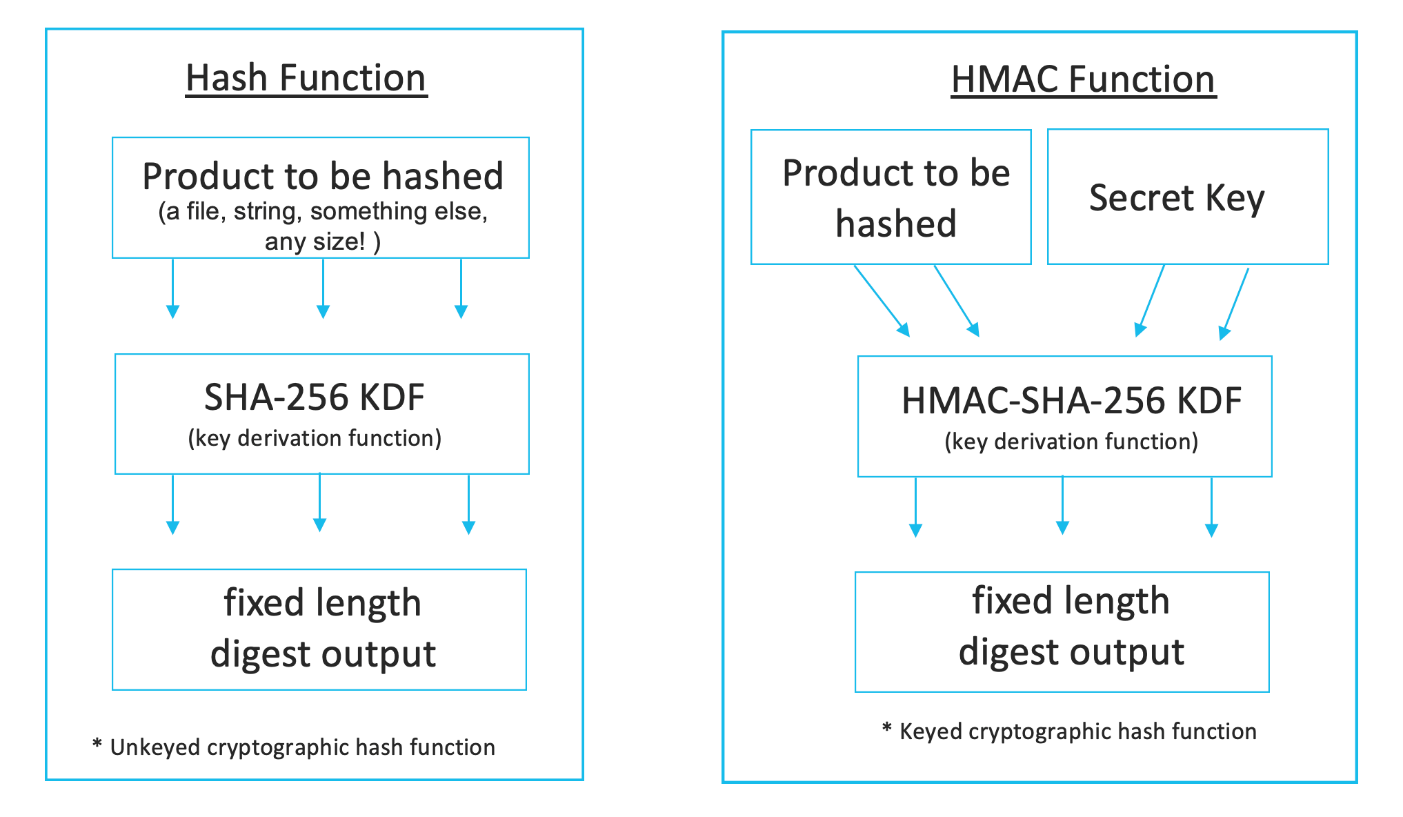
In cryptography, an HMAC is a specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and authenticity of a message.

Is sha256 a HMAC?

HMACSHA256 is a type of keyed hash algorithm that is constructed from the SHA-256 hash function and used as a Hash-based Message AuthenticationCode(HMAC)

HMACMD5 is a type of keyed hash algorithm that is constructed from the Message Digest Algorithm 5 (MD5) hash function and used as a Hash-based Message Authentication Code (HMAC)

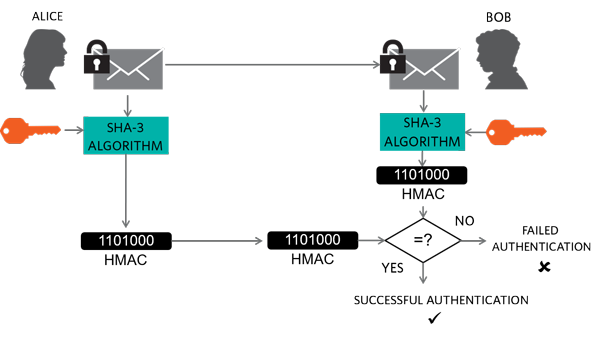




HASH – A hash lets you verify only the authenticity of the data (I,. e., that the data you received is what was originally sent).

HMAC – An HMAC lets you verify both the authenticity and the originator of the data.

More info: **https://www.ietf.org/rfc/rfc2104.txt**



**CRYPTOGRAPHY**

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect, data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

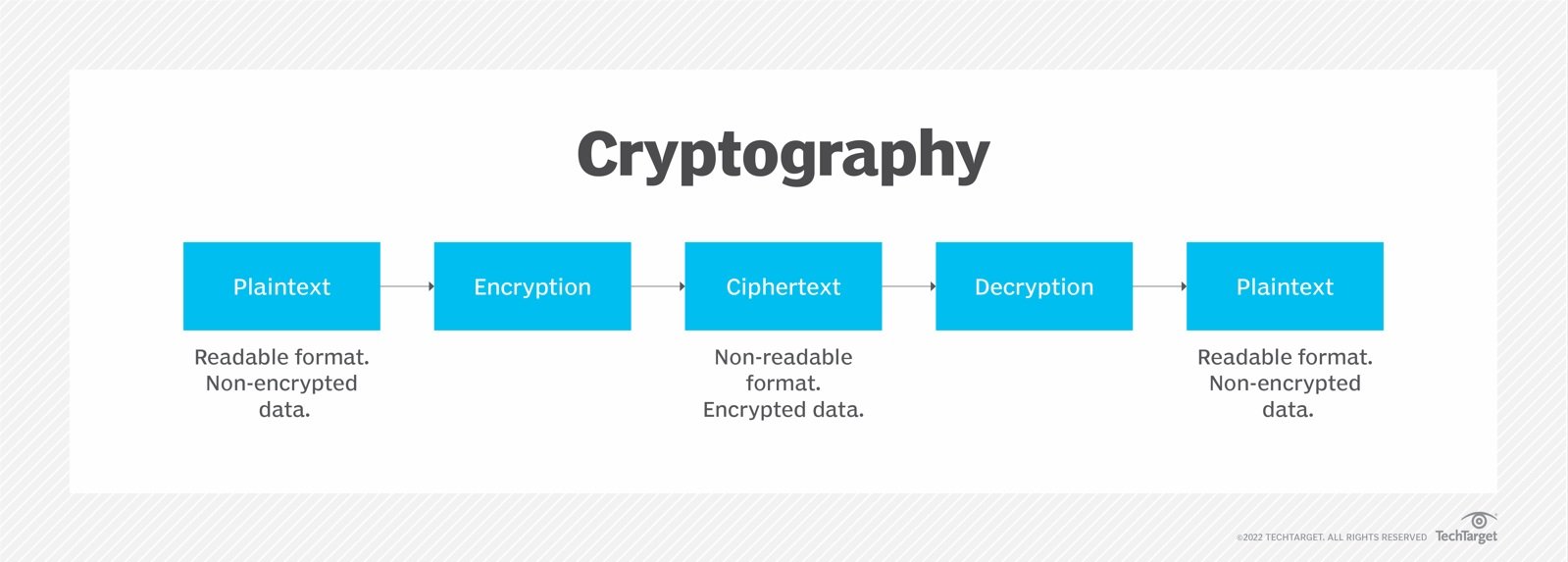
**Cryptography techniques**

Cryptography is closely related to the disciplines of **cryptology** and **cryptanalysis**. It includes techniques such as a microdots, merging words with image and other ways to hide information in storage or transit. However, in today’s computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality.** The information cannot be understood by anyone for whom it was unintended.
2. **Integrity.** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3. **Non-repudiation.** The creator/sender of the information cannot deny at a later stage their intention in the creation or transmission of the information.
4. **Authentication.** The sender and receiver can confirm each other’s identity and the origin/destination of the information.

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also includes the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems and not discussing sensitive procedures with outsiders.

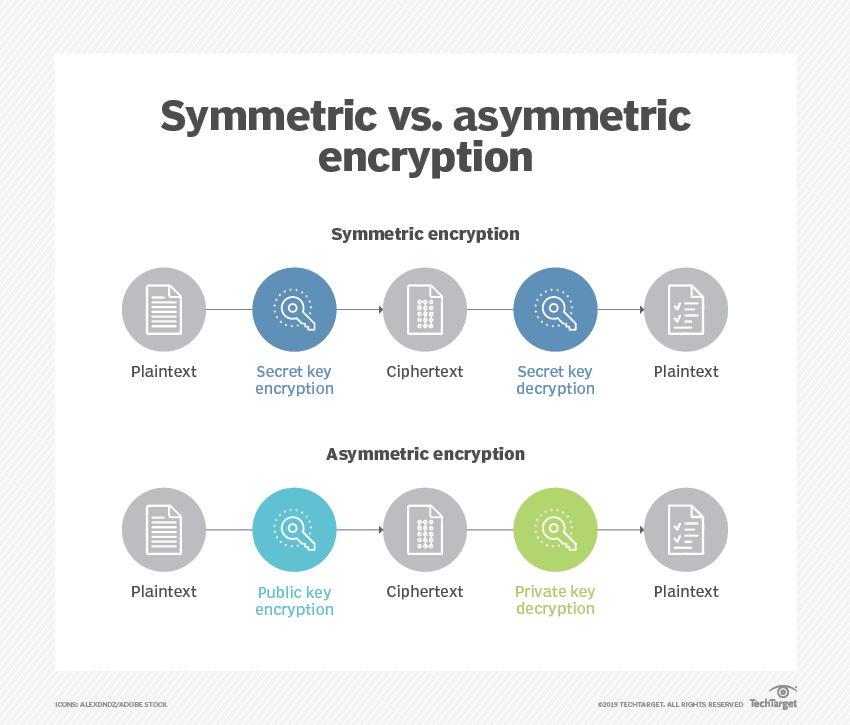


**Cryptographic algorithms**

Cryptosystems use a set of procedures known as cryptographic algorithm, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices and applications.

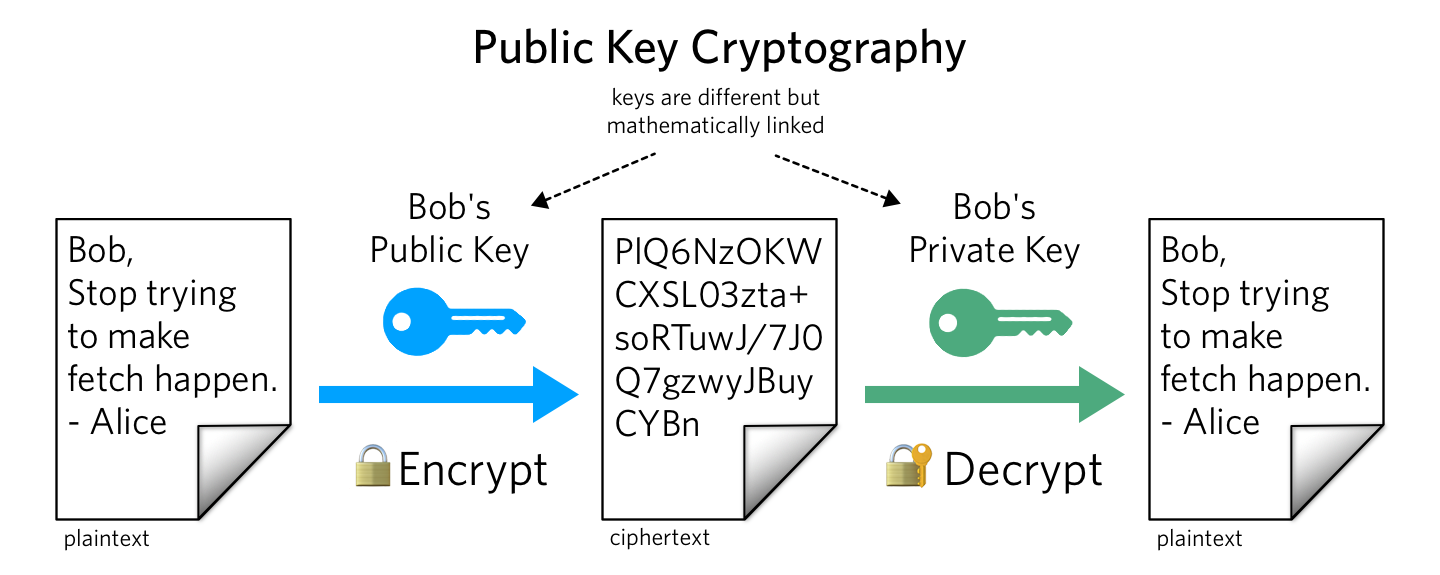
A cipher suite uses one algorithm for encryption, another algorithm for message authentication and another for key exchange. This process, embedded in protocols and written in software that run on operating systems and networked computer systems.

**Types of cryptography**

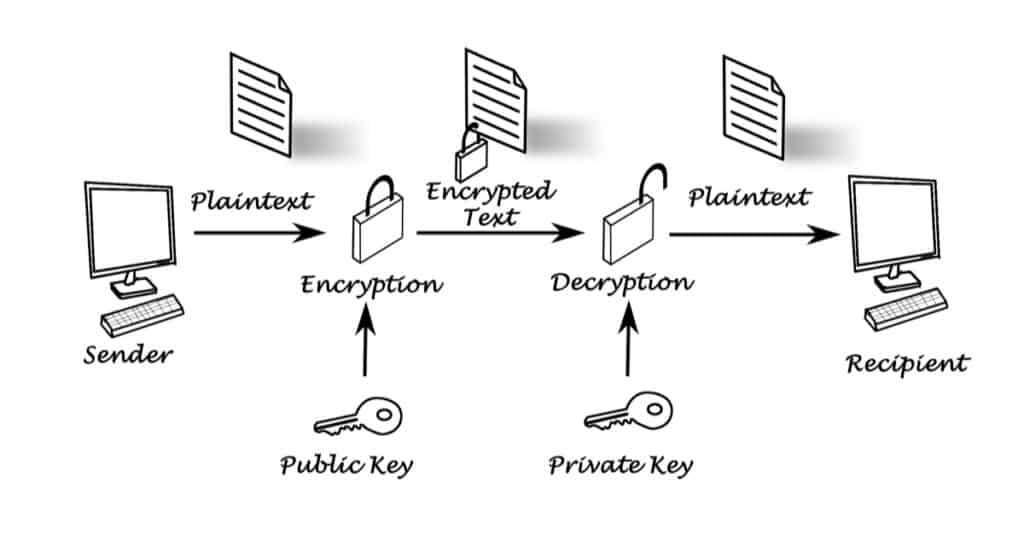


**Examples**

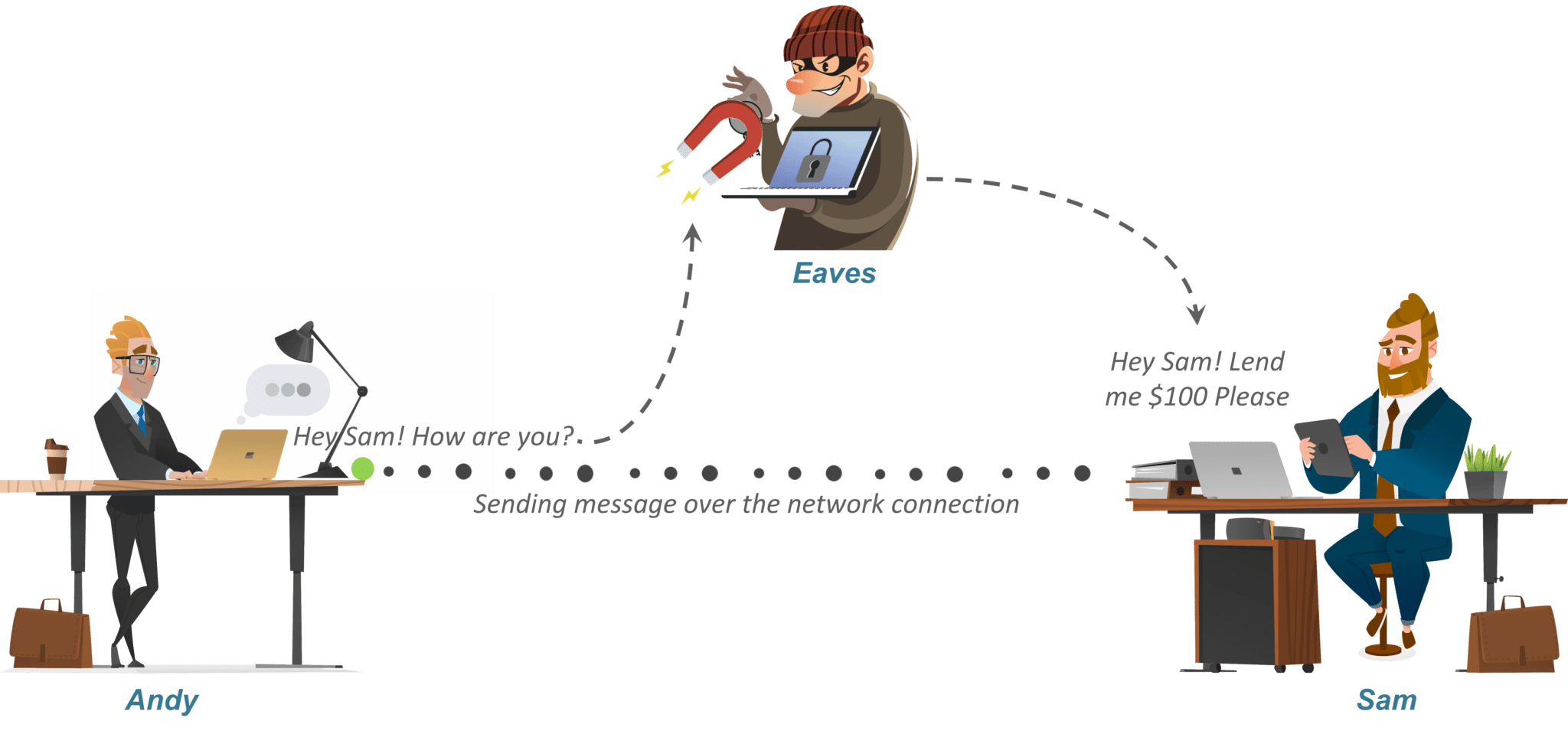
**1**



**2**



**3**



**4**

