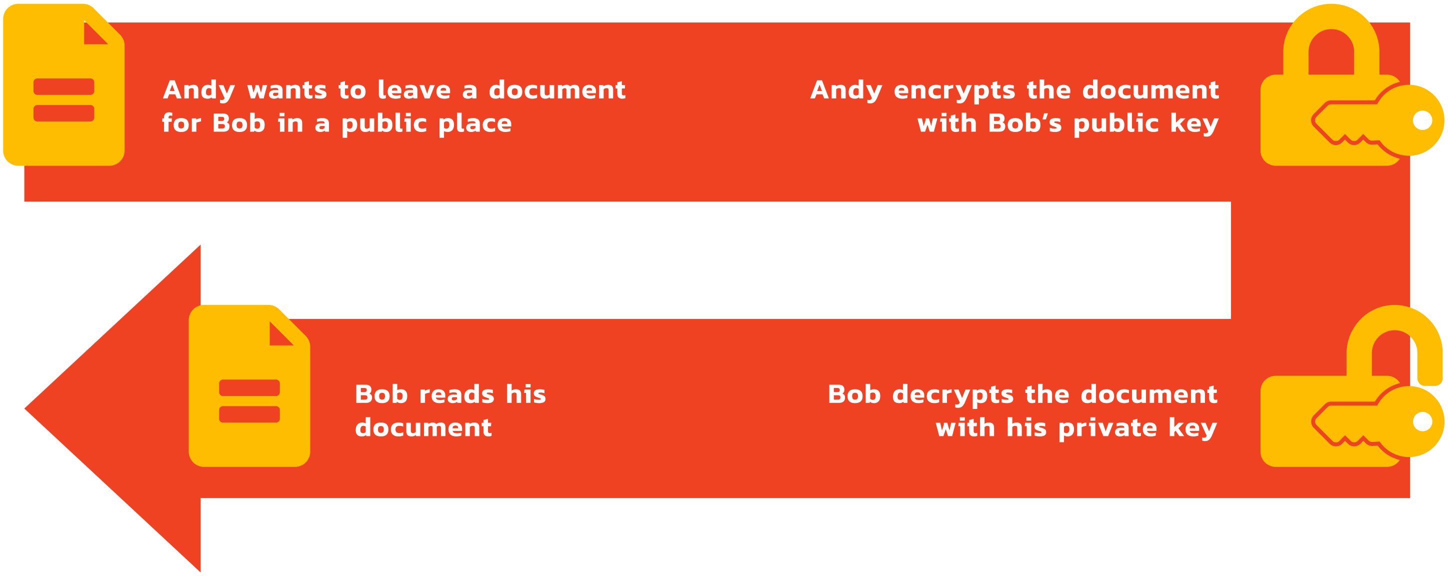
we teach blockchain

4649 N BROADWAY AVE CHICAGO, IL 60640
WETEACHBLOCKCHAIN.ORG
INFO@WETEACHBLOCKCHAIN.ORG

WHAT IS ASYMMETRICAL ENCRYPTION?

Asymmetrical Encryption is a complex method of encryption. It incorporates two cryptographic keys to implement data security: the **public key** and the **private key**. The public key is available to everyone who wishes to send a message. The private key is known only to the owner of a public key. The public key can be used to encrypt information in such a way that it can only be decrypted with the corresponding private key



Andy wants to leave a document for Bob in a public place

Andy encrypts the document with Bob's public key

Bob decrypts the document with his private key

Bob reads his document

	SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
FUNCTIONALITY	Useful for storing data which will be retrieved by the same party	Useful for storing data in public so that it can only be retrieved by the intended party.
EFFICIENCY	These relatively simple operations are executed differently.	Decrypts slowly due to greater overhead (Better for small amounts of data)
KEY SIZE	128 bt keys, private, fast and secure	At least 1000 bits for secure, public storage
HARDWARE	Performs simple algorithms, requires relatively inexpensive hardware.	Implements complex and time-consuming algorithms that require better hardware
SECURITY	Security is based on the strength of the algorithm and the size of the key. Good algorithms exist for both encryption methods and key size effectiveness.	