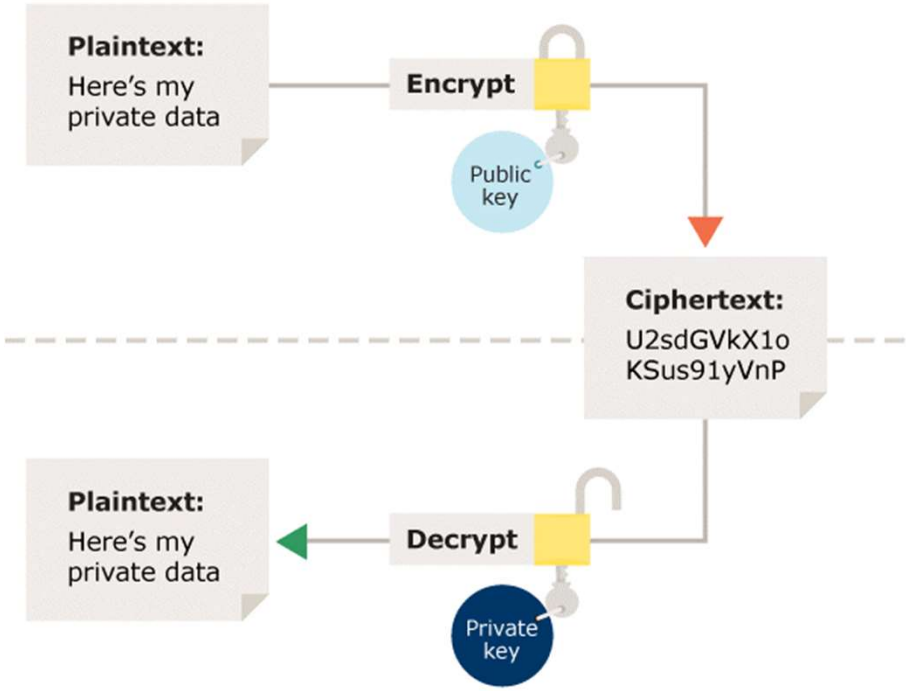
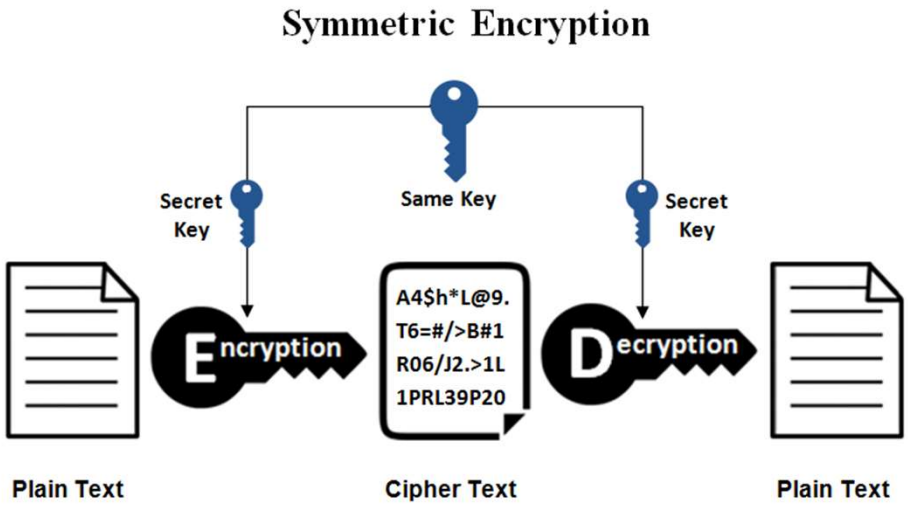
ENCRYPTION

- Do you notice when accessing some websites e.g. Instagram via a web browser there is a lock pad image in the address bar
  - What does it mean?
  - Websites that use http:// and https://, what are the differences?
- Encryption means changing data to be not understandable
  - Using an encryption key to change data (plain text) to be unreadable called cipher text
  - Using an decryption key to restore back the encrypted data back to original data (plain text)



METHOD OF ENCRYPTION

- Symmetric encryption
  - Using same key to encrypt and decrypt data
  - Senders and receivers must agree what key to be used
  - If the key is intercepted between sending, hackers can decrypt the encrypted data
  - Example of this method is Caesar cipher



METHOD OF ENCRYPTION

- Symmetric encryption
  - Caesar cipher
  - It is named after Julius Caesar who encrypted messages in the following way
  - The letters of the alphabet are shifted a set number of places
    - A positive shift moves the letters to the right
    - A negative shift moves to the left
    - For example, a key +2 the alphabet would be changed to this
      - Plain text: A SECRET
      - Cipher text: C UGETIX

Plain text (input)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher text (output)	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

METHOD OF ENCRYPTION

- Asymmetric encryption
  - Use different key to encrypt and decrypt data
  - Public key is used to encrypt
  - Private key is used to decrypt
  - Private key is safe to be sent in the internet