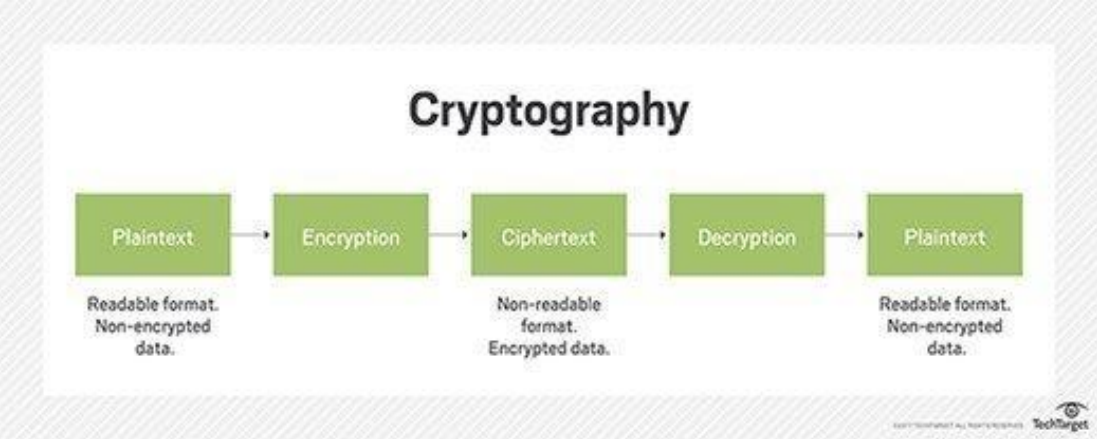
Encryption

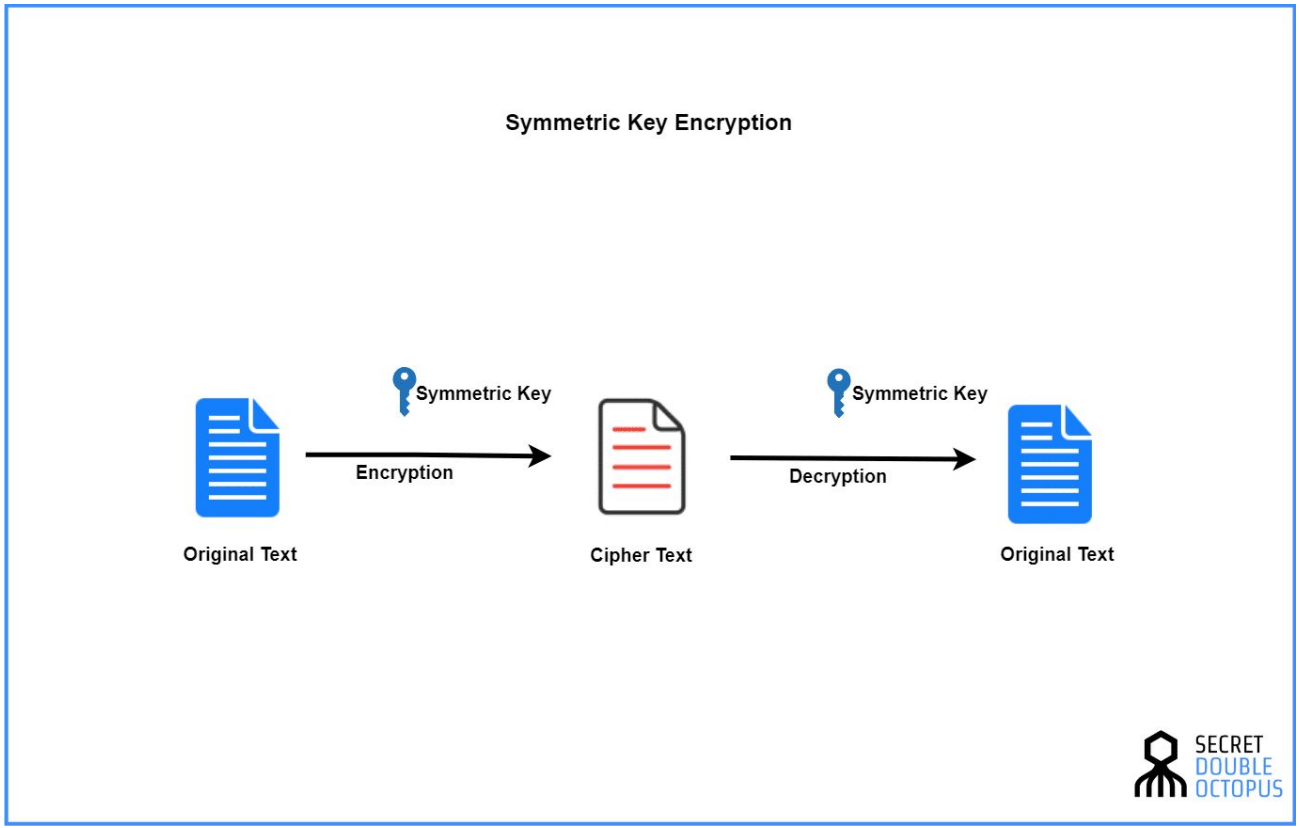
By: Isaac Chang

Importance of encryption

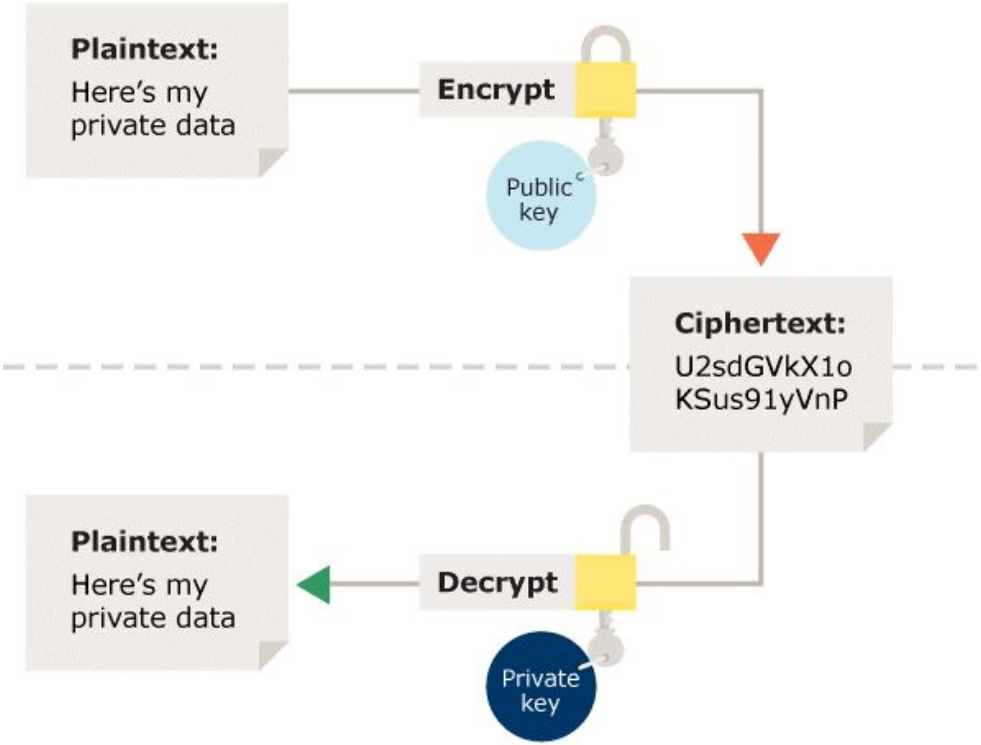
- Without encryption, anyone can read data
- If you wanted to keep a message a secret, you have to encrypt the contents
- No one can read your message unless they decrypt the contents



Symmetric Encryption



Asymmetric Encryption

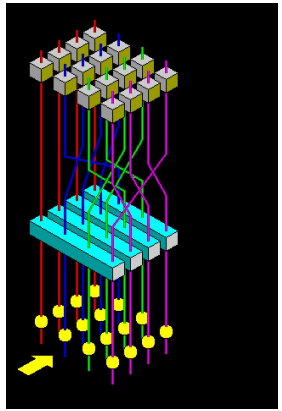


What can you encrypt?

- Text files
- Video files
- Folders
- Directories

Two common encryption methods

- RSA
- AES



RSA

- Oldest and most secure(atm) encryption system
- Concept: Multiplies two very large prime numbers together with an extra value

- Allows people to encrypt any files with the encryption key but only those who know the two prime numbers can decrypt
- RSA is so successful because it is extremely hard to find the two prime numbers

Why is it so hard to break RSA?

- We will look only at the factoring problem of RSA and not the other reasons
- If you have two prime numbers multiplied together, you get a huge number.
-

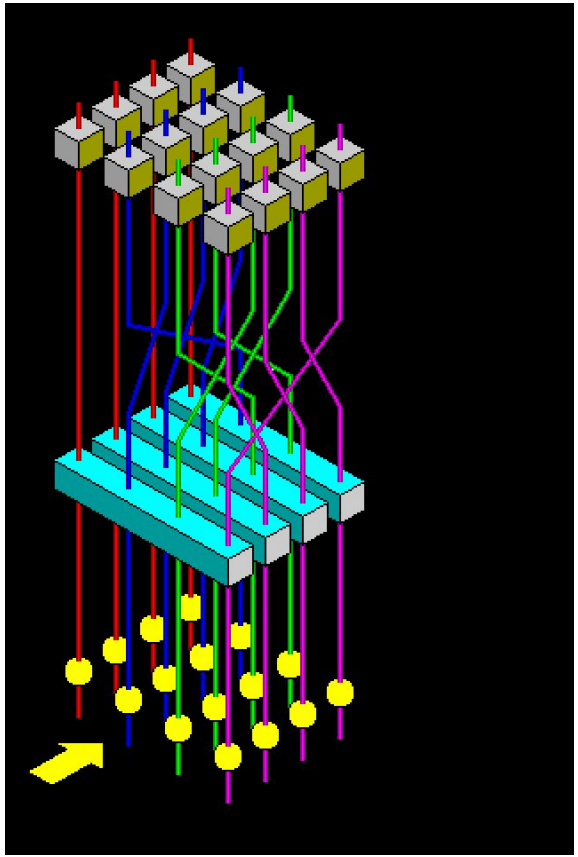
Example: 4057*15679=63609703

Imagine how you usually find factors of 24:

1,2,3,4,6,8,24

Imagine that for 63609703

AES:



How to crack encryption

- Brute force attacks
- Phishing attacks

Resources to learn more:

More about the mathematics behind RSA: https://en.wikipedia.org/wiki/RSA_(cryptosystem)#:~:text=An%20RSA%20user%20creates%20and,who%20knows%20the%20prime%20numbers.

Thanks for listening!

Next meeting will most likely be next Monday

We will do a hands on coding tutorial for an encryption method, most likely RSA!