Encryption

Encryption

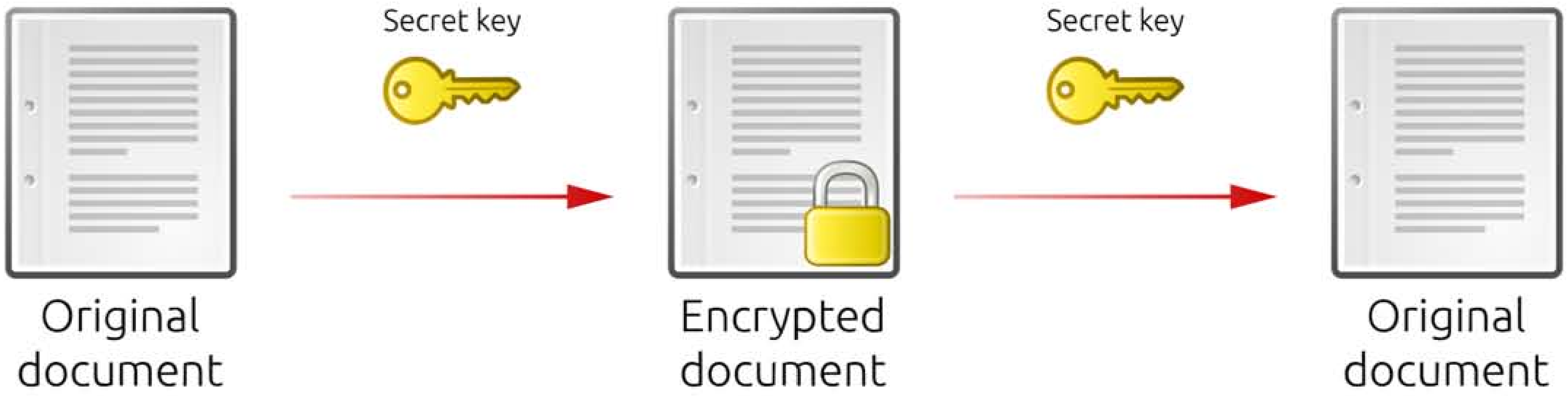
Encryption is the process of transforming data into a form that is unreadable – this allows it to be stored and transmitted securely.

A special key is required in order to decrypt the message in order to make it readable.

The original message is known as plain text and the encrypted text is known as cypher text.

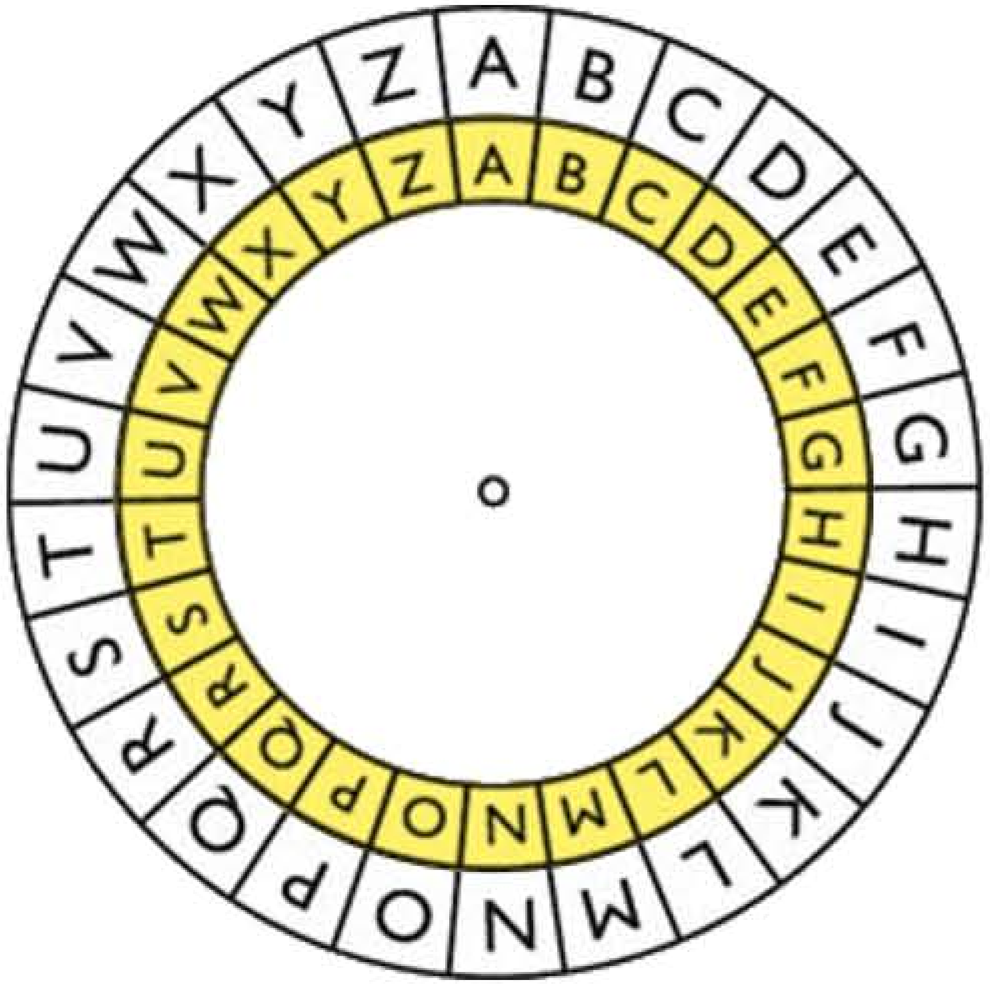
Symmetric Encryption

In symmetric encryption a single key is used to both encrypt and decrypt the message.



One of the earliest forms of encryption was the Caesar cypher. It is said that it was developed by Julius Caesar and is a form of symmetric encryption. It works by shifting the letters in the alphabet by a set amount.

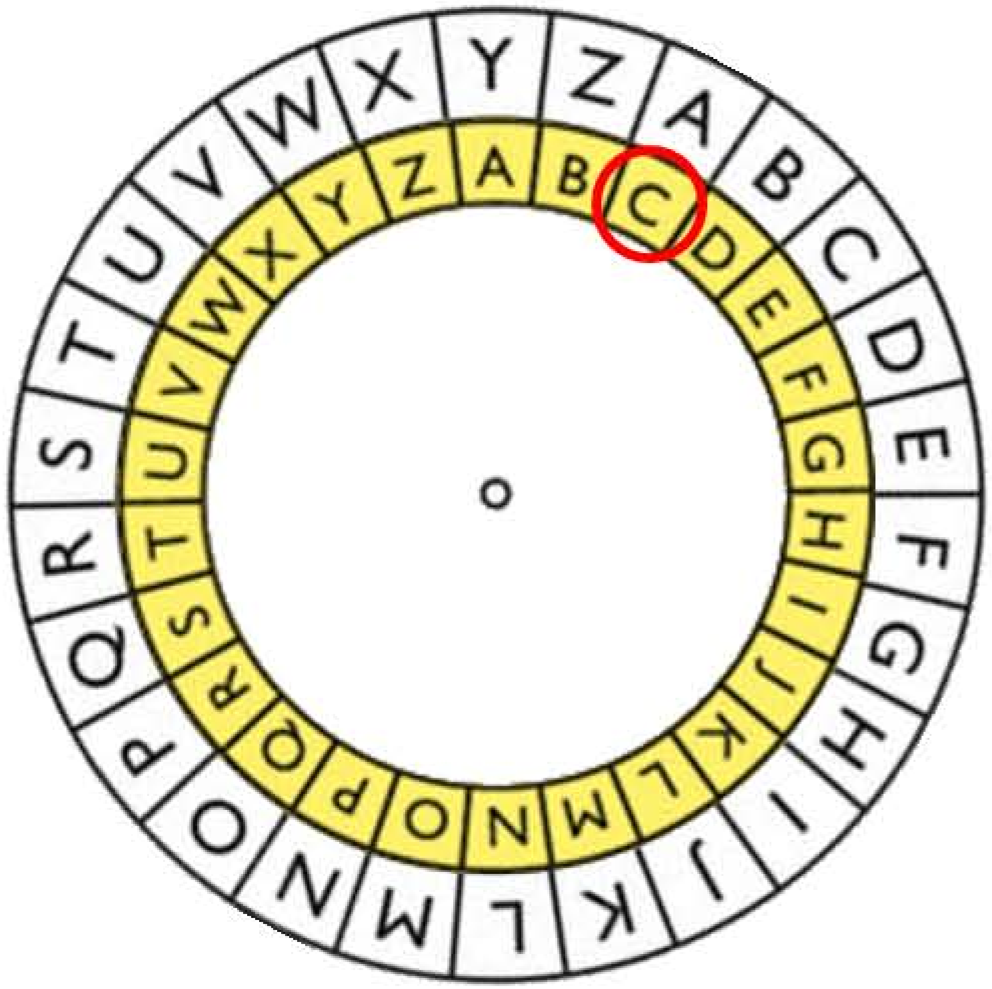
Caesar Cypher


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
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

This is a Caesar cypher wheel.

For a shift of +2 we turn the outer wheel clockwise two places.

Caesar Cypher


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
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

This is a Caesar cypher wheel.

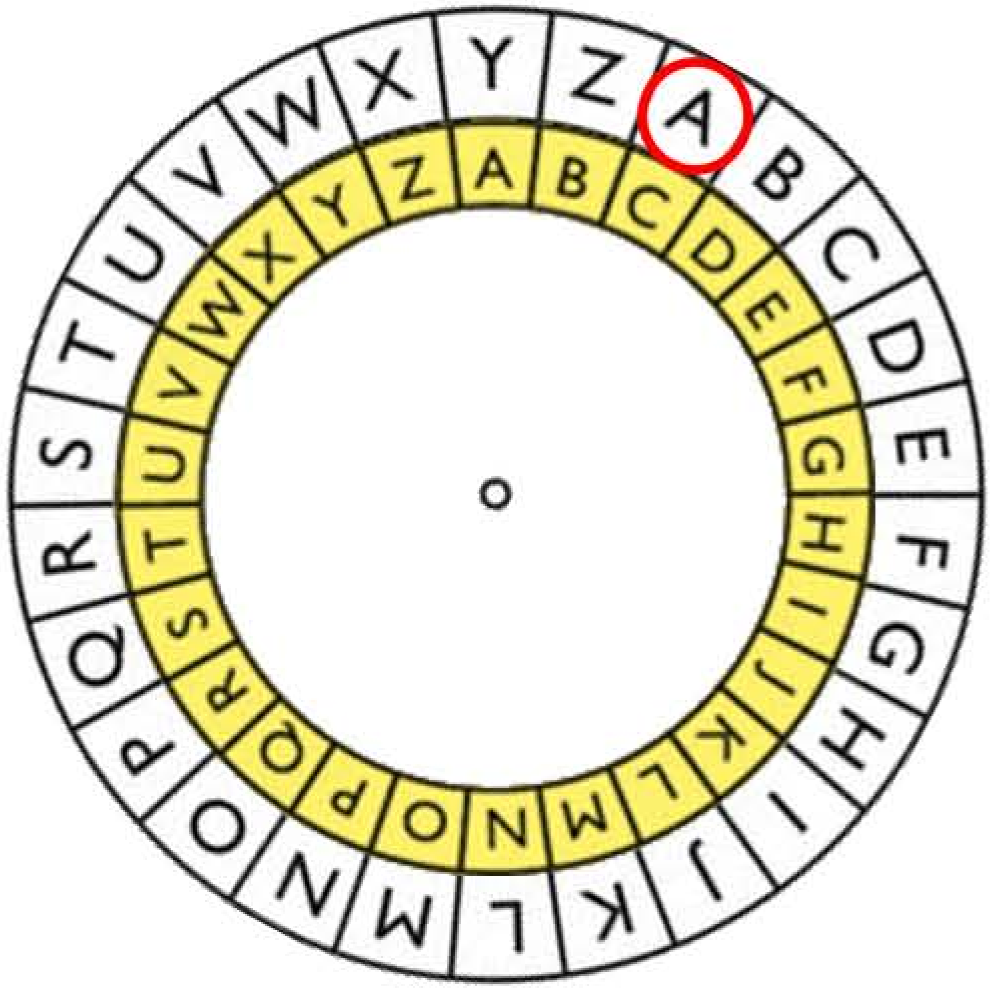
For a shift of +2 we turn the outer wheel clockwise two places.

To encrypt a message we read from the outer ring to the inner ring.

A becomes C with a shift of +2.

Decrypting Messages

To decrypt a message you set the position of the wheel in the same way we did when encrypting.

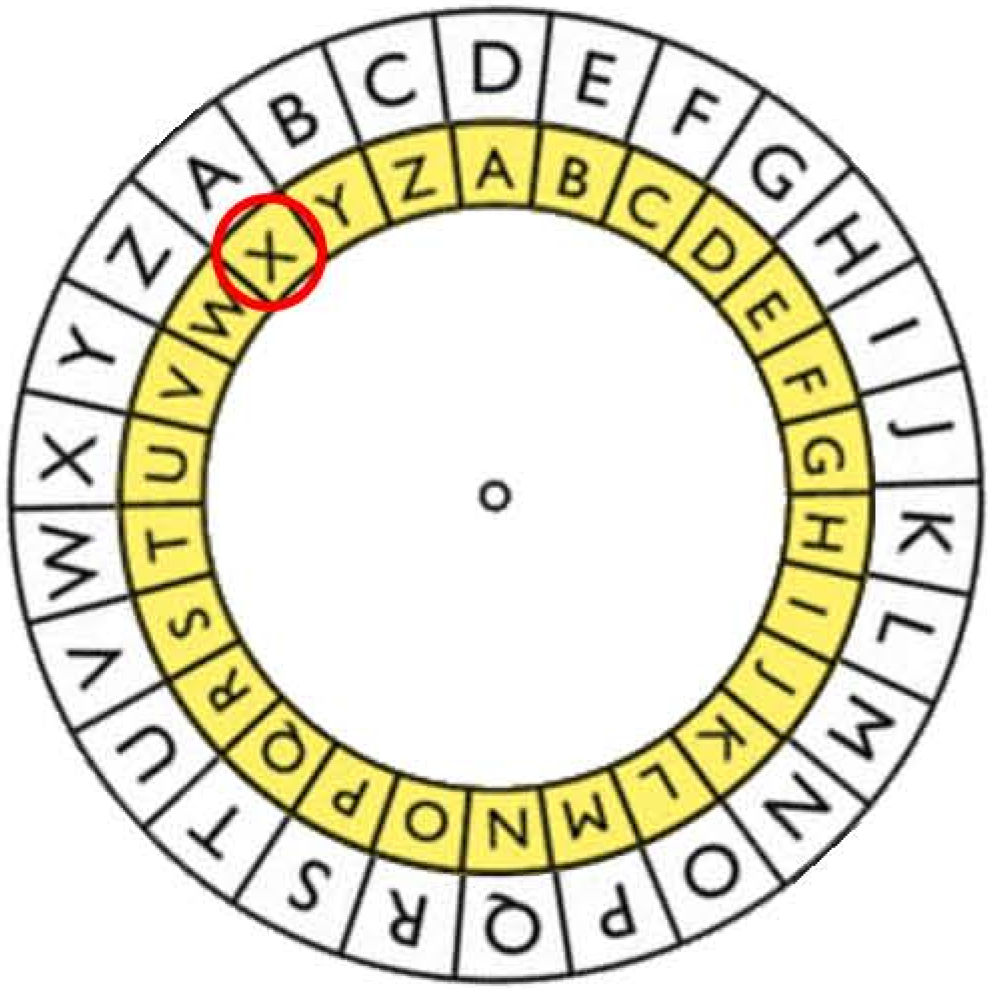

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The only difference is we read from the inner ring to the outer ring.

So, when decrypting with a shift of +2, C becomes A.

Negative Shifts

If a shift is negative (e.g. –3), we move the outer ring counter-clockwise.


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
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

So, with a shift of –3, A becomes X.

Encryption Strength

The Caesar cypher is a very simple and weak example of symmetric encryption.

More complex forms of symmetric encryption use keys with multiple digits or characters.

In these forms of encryption increasing the length of the key increases the strength of the encryption.

Secure Socket Layer

Secure Socket Layer (SSL) is a form of encryption used to keep data safe when being transferred over the internet.

The SSL key is kept secret during transmission by encrypting the key itself.