Cryptography 2

Lets learn about Substitution ciphers

Mary queen of scots

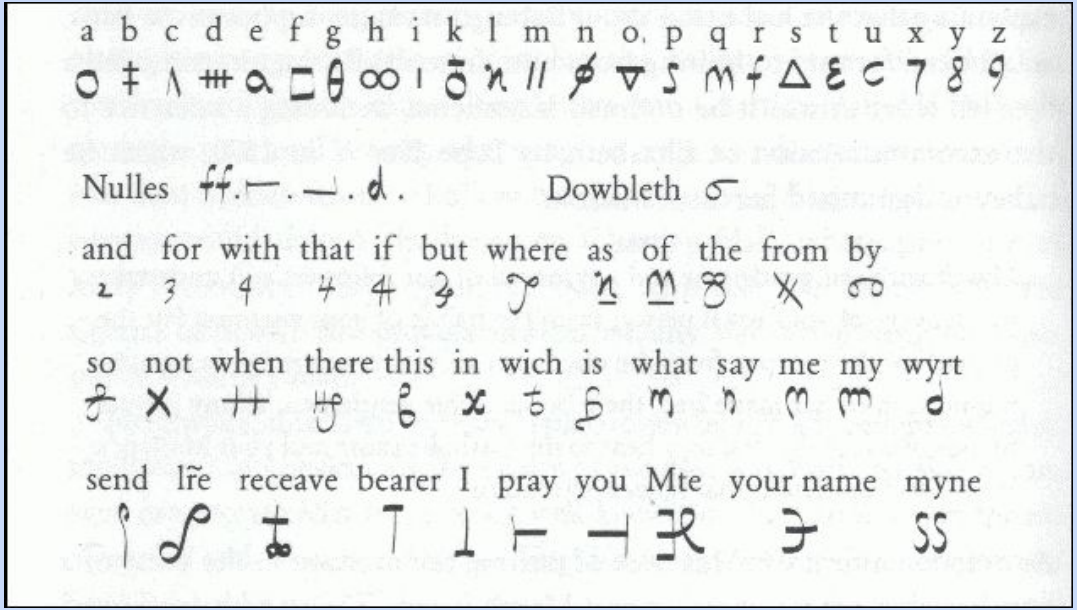
When To prove the importance of secure ciphers, here is the tragic story of Mary Queen of Scots, who was foolish enough to use a weak cipher in the 16th century.

Mary wanted to assassinate Queen Elizabeth I, and began exchanging messages with her co-conspirators, in particular Anthony Babington. This was dubbed the Babington Plot. Their messages were so treacherous that they were encrypted, so that they could not be read if they fell into the wrong hands.

Mary queen of scots

The cipher that Mary used is shown below. It has a cipher alphabet, with substitutions for each letter from A to Z. The cipher also contains some code symbols for the most common words, and some more sophisticated symbols.

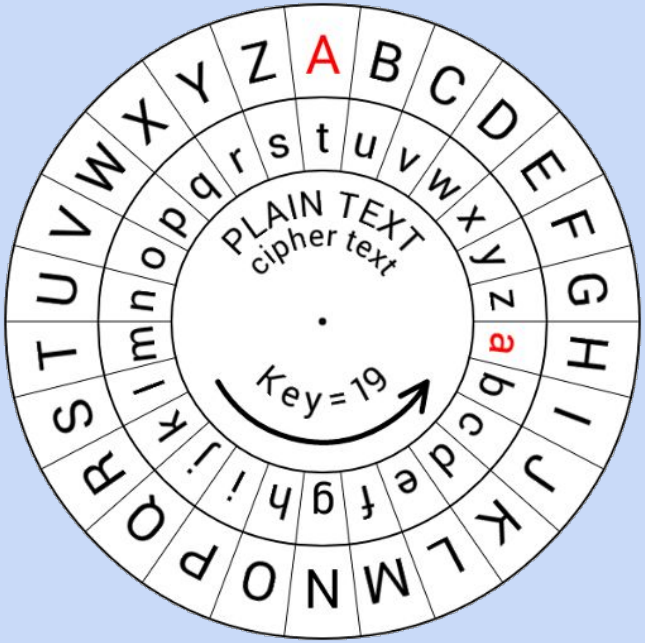
Mary's messages were captured by Elizabeth's spies and they were cracked by her chief code breaker. Mary was immediately arrested, put on trial and the deciphered messages were used as evidence of her treachery. She was found guilty and was executed in 1587 ... all because her cipher was cracked.



Substitution ciphers

A substitution cipher is one in which letters are represented by other letters; it can be deciphered by someone knowing the order of the cipher alphabet used.

One method of hiding messages in this way was invented by Julius Caesar, Roman Emperor over two thousand years ago. It is known as the **Caesar Cipher**.



Caesar Cipher - Encryption

Usually we would use a caesar cipher wheel to encrypt and decrypt messages. But as we don't have any we will do it without them.

EXAMPLE

To encrypt the message 'A B C' we need the KEY.

The KEY is **6.**

For each letter in the message we move 6 spaces (KEY) in the alphabet.

A + 6 = G
B + 6 = H
C + 6 = I

The encrypted message is now 'GHI'

Another example

[PLAIN TEXT MESSAGE]

Hello there

Using a caesar cipher with a key of 6 the PLAIN TEXT “Hello there” would be encrypted as “NKRRU ZNKXK”

Task 1 - Encrypt the messages

If you reach the end of the alphabet continue from the start! “X” with a key of 3 becomes “A”.

It might be helpful to look at the alphabet on slide 12

1. **Message to encrypt “I love ice cream”**

Key value: 2

Encrypted message:

2. **Message to encrypt “I wish i was in Wales”**

Key Value: 3

Encrypted message:

3. **Message to encrypt “Computing is the best”**

Key value: 4

Encrypted message:

4. **Message to encrypt “A picnic at the beach on a rainy day is a bad idea”**

Key value: 8

Encrypted message:

Caesar Cipher - Decryption

This time we need to decrypt the message so it makes sense.

EXAMPLE

To encrypt the message ‘G H I’ we need the KEY.

The KEY is **6.**

For each letter in the message we move 6 spaces backwards (KEY) in the alphabet.

G - 6 = A
H - 6 = B
C - 6 = C

The decrypted message is now ‘ABC’

Another example

[CIPHER TEXT MESSAGE]

DTZ FWE WJFID

Using a caesar cipher with a key of 5 the Cipher TEXT “Hello there” would be decrypted as “You are ready”

Task 1 - Decrypt the messages

If you convert the letter “X” by 3 letters then it becomes “A”. When you reach the end of the alphabet start again!

It might be helpful to look at the alphabet on slide 12

1. **Message to decrypt “K JCVG OQPFCAU”**

Key value: 2

Decrypted message:

2. **Message to decrypt “D EDNHUV GRCHQ”**

Key Value: 3

Decrypted message:

3. **Message to decrypt “XLI ERKVC HSK FEVOIH”**

Key value: 4

Decrypted message:

4. **Message to decrypt “QB EIA I EQTL OWWAM KPIAM”**

Key value: 8

Decrypted message:

Extension - Create your own caesar cipher

Choose your KEY

Write the encrypted message here


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