**Caesar cipher**

**How it was used**

A Caesar substitution cipher takes the alphabet and maps it onto the alphabet with an agreed shift of a number of letters. Caesar encoded his private letters by shifting it three letters.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  alphabet | 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 |
| Ciphertext  alphabet | 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 |

The message can then be encoded by converting letters from the top row to the bottom.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | I | L | O | V | E | Y | O | U | C | A | L | L | M | E |
| Ciphertext  message | f | i | l | s | b | v | l | r | z | x | i | i | j | b |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Once the ciphertext message has been given to somebody it can easily be decoded if they know the shift.

**Decoding challenge**

This message has been encoded with a shift of 12 letters.

Decode this message

ksfsohvcigobrawzsgtfcaqcatcfh

**Extension**

How would you go about trying to crack a code if you were not told the shift?

Gh hgx phnew atox uxebxoxw bg max etlm rxtkl hy max gbgxmxxgma vxgmnkr matm mabl phkew ptl uxbgz ptmvaxw dxxger tgw vehlxer ur bgmxeebzxgvxl zkxtmxk matg ftg'l tgw rxm tl fhkmte tl abl hpg

**Keyword cipher**

**How it was used**

A keyword substitution cipher takes the alphabet and maps it onto the alphabet mixed up, beginning with the keyword (avoid repeated letters), with the remainder of the alphabet backwards.

For example, using the keyword ‘cornflakes’

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  alphabet | 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 |
| Ciphertext  alphabet | c | o | r | n | f | l | a | k | e | s | z | y | x | w | v | u | t | q | p | m | j | i | h | g | d | b |

The message can then be encoded by converting letters from the top row to the bottom.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | A | T | T | A | C | K | A | T | N | I | N | E | T | O | M | O | R | R | O | W |
| Ciphertext  message | c | m | m | c | r | z | c | m | w | e | w | f | m | v | x | v | q | q | v | h |

Once the ciphertext message has been given to somebody it can easily be decoded if they know the keyword.

**Decoding challenge**

This message has been encoded using the keyword 'whiteboards'.

Decode this message

jawmjvlztrtvjrmafvlpnywpmyvlma

**Extension**

How would you go about trying to crack a code if you were not told the keyword?

**Transposition cipher**

**How it was used**

This does not change the letters, only the order of the letters.

Pick a short word with no repeats and then write your message underneath it in the table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **T** | **R** | **A** | **I** | **N** |
| 20 | 18 | 1 | 9 | 14 |
| T | H | E | B | O |
| M | B | I | S | I |
| N | T | H | E | R |
| O | S | E | G | A |
| R | D | E | N | X |

The columns are then read per-column based upon the position of the letter in the alphabet in the original word (A=1, B=2, etc).

So, in this case the ciphertext is: eihee bsegn oirax hbtsd tmnor

**Decoding challenge**

This message has been encoded using the keyword 'hurt'

Decode this message

igerwioomtmzaataiscytbtytheahmus

**Extension**

How would you go about trying to crack a code if you were not told the keyword?

**Vigenère square**

**How it was used**

This clever method uses multiple shifts, depending upon an initial keyword.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |

So, if you want to encode a message using the keyword ‘SAND’ you encode your first letter using the ‘S’ row, and the second letter using ‘A’.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | W | I | L | L | Y | O | U | M | A | R | R | Y | M | E |
| Repeated keyword | **S** | **A** | **N** | **D** | **S** | **A** | **N** | **D** | **S** | **A** | **N** | **D** | **S** | **A** |
| Ciphertext  message | o | i | y | o | q | o | h | p | s | r | e | b | e | e |

**Decoding challenge**

This message has been encoded using the keyword 'rosebud'

Decode this message

nvwrzixizwktxrehosse

**Extension**

How might you go about trying to decode this if you did not have the keyword?

**Caesar cipher**

**Answer**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  alphabet | 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 |
| Ciphertext  alphabet | 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 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | W | E | R | E | A | T | H | O | U | S | A | N | D | M | I | L | E | S | F | R | O | M | C | O | M | F | O | R | T |
| Ciphertext  message | k | s | f | s | o | h | v | c | i | g | o | b | r | a | w | z | s | g | t | f | c | a | q | c | a | t | c | f | h |

The decoded message is

‘We’re a thousand miles from comfort.’

Clean Bandit, *Rather Be (feat. Jess Glynne)*

**Extension**

The Caesar cipher is very easy to crack.

You can check every possible shift, but you do not have to try the whole message; you can check the first few letters and see if it makes sense.

It is also very susceptible to an attack by frequency analysis. In this example ‘a’, ‘c’, ‘f’ and ‘s’ all appeared three or more times. It is very likely that one of those will be an ‘e’.

**Extension decrypted**

‘No one would have believed in the last years of the nineteenth century that this world was being watched keenly and closely by intelligences greater than man's and yet as mortal as his own.’

H.G. Wells, *War of the Worlds*

**Keyword cipher**

**Answer**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  alphabet | 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 |
| Ciphertext  alphabet | w | h | i | t | e | b | o | a | r | d | s | z | y | x | v | u | q | p | n | m | l | k | j | g | f | c |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | W | H | A | T | W | O | U | L | D | I | D | O | W | I | T | H | Y | O | U | R | S | M | A | R | T | M | O | U | T | H |
| Ciphertext  message | j | a | w | m | j | v | l | z | t | r | t | v | j | r | m | a | f | v | l | p | n | y | w | p | m | y | v | l | m | a |

The decoded message is

'What would I do with you smart mouth?'

John Legend, *All of Me*

**Extension**

Although a lot more complicated than the Caesar cipher it is still relatively easy to crack.

If the message is long enough it will be victim to frequency analysis attack. In this case the letters ‘a’, ‘j’, ‘p’, ‘q’ and ‘v’ all appear more often than the other letters – this can be compared with the most common letters used in English.

Knowing the most common letter pairs are ‘TH HE AN RE ER IN ON AT ND ST ES EN OF TE ED OR TI HI AS TO’, and the most common doubled letters are ‘LL EE SS OO TT FF RR NN PP CC’ will also help.

A modern computer could run through all possible initial words and test the outputs to see if they make sense.

**Transposition cipher**

**Answer**

|  |  |  |  |
| --- | --- | --- | --- |
| h | u | r | t |
| 8 | 21 | 18 | 20 |
| i | t | m | i |
| g | h | t | s |
| e | e | m | c |
| r | a | z | y |
| w | h | a | t |
| i | m | a | b |
| o | u | t | t |
| o | s | a | y |

The decoded message is

'It might seem crazy what I’m about to say'

Pharrell Williams, *Happy*

**Extension**

Unlike with the transposition ciphers a frequency analysis will not reveal anything interesting about this problem – as the most common letters will show up here as being the most common.

To start to crack one of these codes, it make sense to try out writing the message in different sized-grids to determine how many letters were in the keyword used. There were 32 letters, so it was likely to be 4x8, 8x4, 2x16 or 16x2. Using squared paper can help.

**Vigenère square**

**Answer**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext  message | w | h | e | n | y | o | u | r | l | e | g | s | d | o | n | t | w | o | r | k |
| Keyword | **R** | **O** | **S** | **E** | **B** | **U** | **D** | **R** | **O** | **S** | **E** | **B** | **U** | **D** | **R** | **O** | **S** | **E** | **B** | **U** |
| Ciphertext  message | n | v | w | r | z | i | x | i | z | w | k | t | x | r | e | h | o | s | s | e |

The message is

'When your legs don't work [like they used to before]'

Ed Sheeran, *Thinking Out Loud*

**Extension**

This is much harder to break than a simple Caesar cipher, especially with a short length message like this, which is why it was generally thought to be uncrackable for around three centuries.

The first stage is to try to determine the length of the keyword that was used. This can be done by trying frequency analysis on different length keywords. You can also search for repeating patterns of letters, to give you an indication of length of keyword used.

If you can determine a length of keyword then you can solve each one separately as a Caesar cipher. This will be time consuming for a human, but a computer could do this very quickly.

A computer could also test a range of different plausible keywords.