

# ATBASH

Atbash is a simple substitution very similar in nature to the Caesar Substitution. Whereas the Caesar substitution was Roman in origin, Atbash is Jewish in origin.

לא לגו יהוה לא-לגו כי-לשמך תן כבוד על-המרחק על-אמתך:

11	10	9	8	7	6	5	4	3	2	1
כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
12	13	14	15	16	17	18	19	20	21	22

כתרפ מצפצ כת-כרפ למ-כביל אמ ללמך זכ-ציגל זכ-תיאל:

In Atbash, the last letter represents the first, the second to last represents the second and so on:

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

Atbash is even simpler to solve than the Caesar Substitution as there is only one solution to try!

You may start to wonder how we could start to solve a monoalphabetic substitution if we do not know whether the cipher alphabet is atbash, caesar, some combination of the two or just random! This will be addressed later when I discuss monoalphabetic substitution. In the meantime, can you decode the following atbash? I've provided a key to save some legwork.

Blf ziv mlg z Qvwr bvg (Wzigs Ezwvi gl Ofpv Hpbdzopvi)

You shouldn't have had a problem with this, it's fairly easy!

Atbash can also be combined with a caesar shift, to produce a Reversed Caesar substitution.

An example is shown below.

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

