

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 לנו יהוה לא-לנו כי-לשמך תן כבוד על-המרהך 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

סת-רפ מצפצ כת-כרפ למ-כביל אמ ללמק 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
```

