

## NAME

aes - encrypts or decrypts a file using the Rijndael AES-256 cipher

## SYNOPSIS

```
aes [-help] <-e | -d> <-k key> <input-file> <output-file>
```

## DESCRIPTION

The akiwi aes program encrypts or decrypts an input file using the Rijndael AES-256 cipher given a 64 character secret key.

## OPTIONS

The option flags may occur in any order on the command line, but only once. For option flags with arguments, there must be at least one space between the option flag and its argument.

- help Prints a short summary of the command line syntax and options.
- e Encrypt the input file.
- d Decrypt the input file.
- k Specifies the encryption or decryption secret key.

The secret key can only consist of hexadecimal characters in the range [0-9a-fA-F].

For maximum encryption strength the secret key should be 64 characters in length. If a shorter secret key is provided, it is padded out to 64 characters.

### **WARNING!**

If you loose your secret key, there is no way to recover the contents of the encrypted file.

## EXAMPLES

### **Example 1**

```
aes -e -k 01234567890abcdefABCDEF foo.txt foo.enc
```

Encrypts the file 'foo.txt' using the specified secret key and writes the result out to a file named 'foo.enc'.

**Example 2**

```
aes -d -k 01234567890abcdefABCDEF foo.enc foo.dec
```

Decrypts the file 'foo.enc' using the specified secret key and writes the result out to a file named 'foo.dec'.

**COPYRIGHT**

Copyright (C) 2013. By akiwi. All Rights Reserved.