NAME

hmac256 - Compute an HMAC-SHA-256 MAC

SYNOPSIS

hmac256 [**--binary**] *key [FILENAME]*

DESCRIPTION

This is a standalone HMAC-SHA-256 implementation used to compute an HMAC-SHA-256 message authentication code. The tool has originally been developed as a second implementation for Libgcrypt to allow comparing against the primary implementation and to be used for internal consistency checks. It should not be used for sensitive data because no mechanisms to clear the stack etc are used.

The code has been written in a highly portable manner and requires only a few standard definitions to be provided in a config.h file.

hmac256 is commonly invoked as

```
hmac256 "This is my key" foo.txt
```

This compute the MAC on the file '*foo.txt*' using the key given on the command line.

OPTIONS

hmac256 understands these options:

--binary

Print the MAC as a binary string. The default is to print the MAC encoded as lower case hex digits.

--version

Print version of the program and exit.

SEE ALSO

sha256sum(1)