

NAME

gnutls_cipher_decrypt2 - API function

SYNOPSIS

```
#include <gnutls/crypto.h>
```

```
int gnutls_cipher_decrypt2(gnutls_cipher_hd_t handle, const void * ctext, size_t ctext_len, void * ptext, size_t ptext_len);
```

ARGUMENTS

gnutls_cipher_hd_t handle
is a **gnutls_cipher_hd_t** type

const void * ctext
the data to decrypt

size_t ctext_len
the length of data to decrypt

void * ptext the decrypted data

size_t ptext_len
the available length for decrypted data

DESCRIPTION

This function will decrypt the given data using the algorithm specified by the context. For block ciphers the *ctext_len* must be a multiple of the block size. For the supported ciphers the plaintext data length will equal the ciphertext size.

Note that in AEAD ciphers, this will not check the tag. You will need to compare the tag sent with the value returned from **gnutls_cipher_tag()**.

RETURNS

Zero or a negative error code on error.

SINCE

2.12.0

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.

Home page: <https://www.gnutls.org>

COPYRIGHT

Copyright (C) 2001-2023 Free Software Foundation, Inc., and others.

Copying and distribution of this file, with or without modification, are permitted in any medium without royalty provided the copyright notice and this notice are preserved.

SEE ALSO

The full documentation for **gnutls** is maintained as a Texinfo manual. If the `/usr/local/share/doc/gnutls/` directory does not contain the HTML form visit

<https://www.gnutls.org/manual/>