

**NAME**

gnutls\_privkey\_decrypt\_data2 - API function

**SYNOPSIS**

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

```
int gnutls_privkey_decrypt_data2(gnutls_privkey_t key, unsigned int flags, const gnutls_datum_t *  
ciphertext, unsigned char * plaintext, size_t plaintext_size);
```

**ARGUMENTS**

gnutls\_privkey\_t key

Holds the key

unsigned int flags

zero for now

const gnutls\_datum\_t \* ciphertext

holds the data to be decrypted

unsigned char \* plaintext

a preallocated buffer that will be filled with the plaintext

size\_t plaintext\_size

in/out size of the plaintext

**DESCRIPTION**

This function will decrypt the given data using the algorithm supported by the private key. Unlike with **gnutls\_privkey\_decrypt\_data()** this function operates in constant time and constant memory access.

**RETURNS**

On success, **GNUTLS\_E\_SUCCESS** (0) is returned, otherwise a negative error value.

**SINCE**

3.6.5

**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/>