

**NAME**

gnutls\_sec\_param\_to\_pk\_bits - API function

**SYNOPSIS**

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

```
unsigned int gnutls_sec_param_to_pk_bits(gnutls_pk_algorithm_t algo, gnutls_sec_param_t param);
```

**ARGUMENTS**

gnutls\_pk\_algorithm\_t algo  
is a public key algorithm

gnutls\_sec\_param\_t param  
is a security parameter

**DESCRIPTION**

When generating private and public key pairs a difficult question is which size of "bits" the modulus will be in RSA and the group size in DSA. The easy answer is 1024, which is also wrong. This function will convert a human understandable security parameter to an appropriate size for the specific algorithm.

**RETURNS**

The number of bits, or (0).

**SINCE**

2.12.0

**REPORTING BUGS**

Report bugs to <bugs@gnutls.org>.

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

**COPYRIGHT**

Copyright (C) 2001- 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

gnutls\_sec\_param\_to\_pk\_bits(3)

gnutls

gnutls\_sec\_param\_to\_pk\_bits(3)

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