

# My Project

Generated by Doxygen 1.9.8



---

<b>1 File Index</b>	<b>1</b>
1.1 File List . . . . .	1
<b>2 File Documentation</b>	<b>3</b>
2.1 libs/kem.h File Reference . . . . .	3
2.2 kem.h . . . . .	3
<b>Index</b>	<b>5</b>



# Chapter 1

## File Index

### 1.1 File List

Here is a list of all files with brief descriptions:

libs/ <a href="#">kem.h</a> . . . . .	3
---------------------------------------	---



# Chapter 2

## File Documentation

### 2.1 libs/kem.h File Reference

```
#include <stdint.h>
#include "params.h"
Include dependency graph for kem.h:
```

### 2.2 kem.h

[Go to the documentation of this file.](#)

```
00001 #ifndef KEM_H
00002 #define KEM_H
00003
00004 #include <stdint.h>
00005 #include "params.h"
00006
00007 // Definicije za velicine ključeva i druge parametre
00008 #define CRYPTO_SECRETKEYBYTES KYBER_SECRETKEYBYTES
00009 #define CRYPTO_PUBLICKEYBYTES KYBER_PUBLICKEYBYTES
00010 #define CRYPTO_CIPHERTEXTBYTES KYBER_CIPHERTEXTBYTES
00011 #define CRYPTO_BYTES          KYBER_SSBYTES
00019 #if (KYBER_K == 2)
00020 #define CRYPTO_ALGNAME "Kyber512"
00021 #elif (KYBER_K == 3)
00022 #define CRYPTO_ALGNAME "Kyber768"
00023 #elif (KYBER_K == 4)
00024 #define CRYPTO_ALGNAME "Kyber1024"
00025 #endif
00026
00027 // Deklaracije funkcija za KEM (Key Encapsulation Mechanism)
00028
00040 #define crypto_kem_keypair_derand KYBER_NAMESPACE(keypair_derand)
00041 int crypto_kem_keypair_derand(uint8_t* pk, uint8_t* sk, const uint8_t* coins);
00042
00053 #define crypto_kem_keypair KYBER_NAMESPACE(keypair)
00054 int crypto_kem_keypair(uint8_t* pk, uint8_t* sk);
00055
00067 #define crypto_kem_enc_derand KYBER_NAMESPACE(enc_derand)
00068 int crypto_kem_enc_derand(uint8_t* ct, uint8_t* ss, const uint8_t* pk, const uint8_t* coins);
00069
00081 #define crypto_kem_enc KYBER_NAMESPACE(enc)
00082 int crypto_kem_enc(uint8_t* ct, uint8_t* ss, const uint8_t* pk);
00083
00095 #define crypto_kem_dec KYBER_NAMESPACE(dec)
00096 int crypto_kem_dec(uint8_t* ss, const uint8_t* ct, const uint8_t* sk);
00097
00098 #endif // KEM_H
```





# Index

libs/kem.h, [3](#)