My Project

Generated by Doxygen 1.9.8

Chapter 1

File Index

1.1 File List

Here is a list of all files with brief descriptions:

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.

```
#ifndef KEM_H
#define KEM_H

#include <stdint.h>
#include "params.h"

// Definicije za veli?ine klju?eva i druge parametre
#define CRYPTO_SECRETKEYBYTES  KYBER_SECRETKEYBYTES
#define CRYPTO_PUBLICKEYBYTES  KYBER_PUBLICKEYBYTES
#define CRYPTO_CIPHERTEXTBYTES KYBER_CIPHERTEXTBYTES
#define CRYPTO_BYTES           KYBER_SSBYTES
#if   (KYBER_K == 2)
#define CRYPTO_ALGNAME "Kyber512"
#elif (KYBER_K == 3)
#define CRYPTO_ALGNAME "Kyber768"
#elif (KYBER_K == 4)
#define CRYPTO_ALGNAME "Kyber1024"
#endif

 // Deklaracije funkcija za KEM (Key Encapsulation Mechanism)

#define crypto_kem_keypair_derand KYBER_NAMESPACE(keypair_derand)
int crypto_kem_keypair_derand(uint8_t* pk, uint8_t* sk, const uint8_t* coins);

#define crypto_kem_keypair KYBER_NAMESPACE(keypair)
int crypto_kem_keypair(uint8_t* pk, uint8_t* sk);

#define crypto_kem_enc_derand KYBER_NAMESPACE(enc_derand)
int crypto_kem_enc_derand(uint8_t* ct, uint8_t* ss, const uint8_t* pk, const uint8_t* coins);

#define crypto_kem_enc KYBER_NAMESPACE(enc)
int crypto_kem_enc(uint8_t* ct, uint8_t* ss, const uint8_t* pk);

#define crypto_kem_dec KYBER_NAMESPACE(dec)
int crypto_kem_dec(uint8_t* ss, const uint8_t* ct, const uint8_t* sk);

#endif  // KEM_H
```

Index