# Kerberos V5 Data Encryption Standard library
## DRAFT

## 1   DES functions

The DES functions conform to the encryption interface required by the Kerberos version 5 library, and provide an encryption mechanism based on the DES Cipher-block chaining mode (CBC), with the addition of a cyclical redundancy check (CRC-32) for integrity checking upon decryption.

The functions have the same signatures as those described by the main library document; the names are:

**mit_des_encrypt_func**()

**mit_des_decrypt_func**()

**mit_des_process_key**()

**mit_des_finish_key**()

**mit_des_string_to_key**()

**mit_des_init_random_key**()

**mit_des_finish_random_key**()

**mit_des_random_key**()

The **krb5_cryptosystem_entry** for this cryptosystem is `mit_des_cryptosystem_entry`.