CC32xx DES Demo Application

Return to CC31xx & CC32xx Home Page

Return to CC31xx Sample Applications

Overview

The DES module provides hardware-accelerated data encryption and decryption functions. The module runs either the single DES or the triple DES (3DES) algorithm in compliance with the FIPS 46-3 standard and supports the following operating modes:

- Electronic codebook (ECB)
- Cipher block chaining (CBC)
- Cipher feedback (CFB)

The DES module is based on a symmetric algorithm, meaning that the encryption and decryption keys are identical. To encrypt data means to convert it from plain text to an unintelligible form called cipher text. Decrypting cipher text converts previously encrypted data back to its original plain text form.

Application details

The application is a reference to usage of DES DriverLib functions on CC3200. Developer/User can refer to this simple application and re-use the functions in their applications. This application can be used with or without "Uart Terminal".

If the user wishes to use "Uart Terminal" to give some inputs and follow the execution path prints, then they might do so by defining "USER-INPUT" in the des_main.c file.

- **desdemo**: This command allows the user to excercise the DES funcitonality on CC3200. The command needs a parameter, des-mode.

  - des-mode is the DES algorithm that user can choose, the value can be ECB or CBC or CFB or TECB or TCBC or TCFB.

Further, user will be prompted for more inputs for "key" and "plain text input"

Not defining or un-defining the USER-INPUT will allow the user to follow the execution path on the IAR or CCS IDE, in the "debugging" mode and no input is needed to be given by the user.

Source Files briefly explained

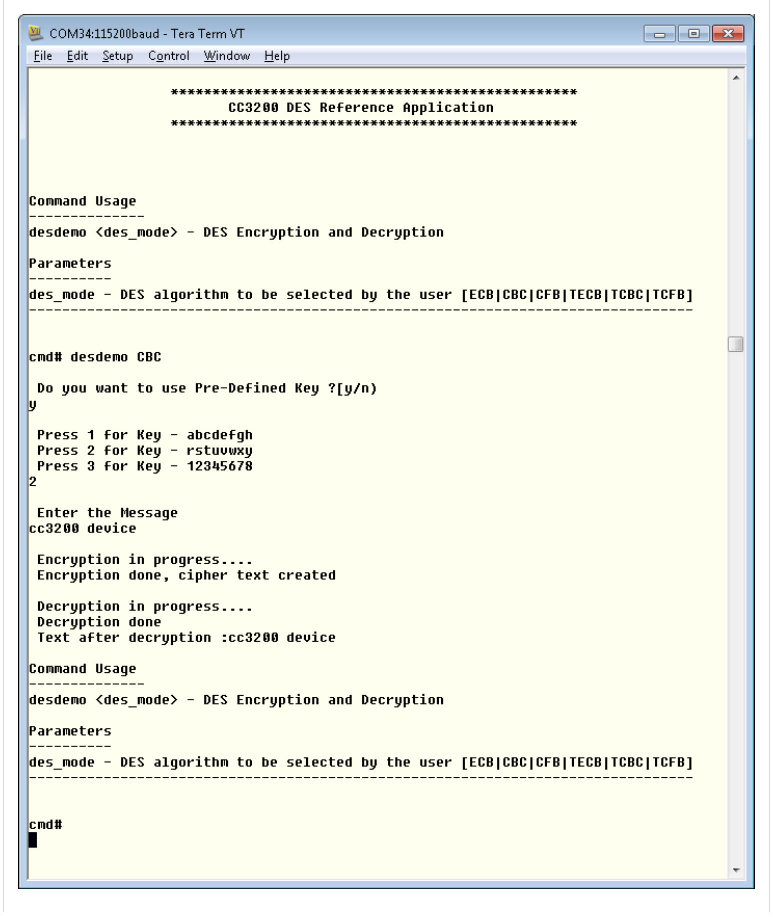
- **main.c** - The main file that contains the core-logic for encryption and decryption. The functions in the file uses DriverLib calls to perform encryption and decryption.

Supporting files

- **des_userinput.c** - This file is used in the USER-INPUT mode. The function in the file reads the input from the user, parses the input string and feed the core-logic functions in the des_main.c
- **pinmux.c** - Generated by the PinMUX utility. UARTA0 pins are brought out in this file.
- **startup_ccs.c** - CCS related functions
- **startup_ewarm.c -** IAR related functions
- **uart_logger.c -** Functions to display information on UART

Usage

1. Setup a serial communication application (HyperTerminal/TeraTerm). For detail info visit Terminal setup
   On the host PC, open a hyperterminal, with the following settings
   - **Port:** Enumerated COM port
   - **Baud rate:** 115200
   - **Data:** 8 bit
   - **Parity:** None
   - **Stop:** 1 bit
   - **Flow control:** None
2. Run the reference application (/IAR/CCS)
   - Flash the bin
   - Open the project in IAR/CCS. Build and download the application to the board
3. On the Hyperterminal, a prompt appears
   - The DES commands need to be issued and the results can be seen


COM34:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
                 *************************************************
                        CC3200 DES Reference Application
                 *************************************************



Command Usage
--------------
desdemo <des_mode> - DES Encryption and Decryption

Parameters
----------
des_mode - DES algorithm to be selected by the user [ECB|CBC|CFB|TECB|TCBC|TCFB]
--------------------------------------------------------------------------------


cmd# desdemo CBC

 Do you want to use Pre-Defined Key ?[y/n)
y

 Press 1 for Key - abcdefgh
 Press 2 for Key - rstuvwxy
 Press 3 for Key - 12345678
2

 Enter the Message
cc3200 device

 Encryption in progress....
 Encryption done, cipher text created

 Decryption in progress....
 Decryption done
 Text after decryption :cc3200 device

Command Usage
--------------
desdemo <des_mode> - DES Encryption and Decryption

Parameters
----------
des_mode - DES algorithm to be selected by the user [ECB|CBC|CFB|TECB|TCBC|TCFB]
--------------------------------------------------------------------------------


cmd#
```

Limitations/Known Issues

None

Article Sources and Contributors

CC32xx DES Demo Application *Source*: http://processors.wiki.ti.com/index.php?oldid=180751 *Contributors*: A0221015, Codycooke, Jitgupta, Malokyle

Image Sources, Licenses and Contributors

File:Cc31xx cc32xx return home.png *Source*: http://processors.wiki.ti.com/index.php?title=File:Cc31xx_cc32xx_return_home.png *License*: unknown *Contributors*: A0221015

File:Cc32xx return sample apps.png *Source*: http://processors.wiki.ti.com/index.php?title=File:Cc32xx_return_sample_apps.png *License*: unknown *Contributors*: A0221015

Image:CC3200 des terminal runScreen.png *Source*: http://processors.wiki.ti.com/index.php?title=File:CC3200_des_terminal_runScreen.png *License*: unknown *Contributors*: Codycooke