AVR 8-bit Microcontrollers

AVR284: Software Library for AES-128 Encryption and Decryption on megaAVR

APPLICATION NOTE

Introduction

Advanced Encryption Standard (AES) is a specification for encryption of electronic data established by National Institute of Standards and Technology (NIST) in 2001 as Federal Information Processing Standards (FIPS) 197. This is a symmetric block cipher algorithm used for the encryption and decryption of electronic data. This application note provides an example of AES encryption and decryption algorithm on the Atmel® ATmega328PB. An ATmega328PB Xplained Mini kit is used to demonstrate this application. For the theory of AES, refer to AT10764: Software Library for AES-128 Encryption and Decryption.

Features

- Compliant with FIPS Publication 197, Advanced Encryption Standard (AES)
- AES encryption and decryption algorithm
- 128-bit cryptographic key supported
- Five confidentiality modes of operation of AES specified in FIPS
  - Electronic Codebook mode (ECB)
  - Cipher Block Chaining mode (CBC)
  - Cipher Feedback mode (CFB)
  - Output Feedback mode (OFB)
  - Counter mode (CTR)
- 8, 16, 32, 64, and 128-bit data sizes possible in CFB mode

Table of Contents

1. Prerequisties

The solution discussed in this document requires:

- Atmel Studio 7.0 or later
- ATmega328PB Xplained Mini kit
- Example Source Code available for download from Atmel START

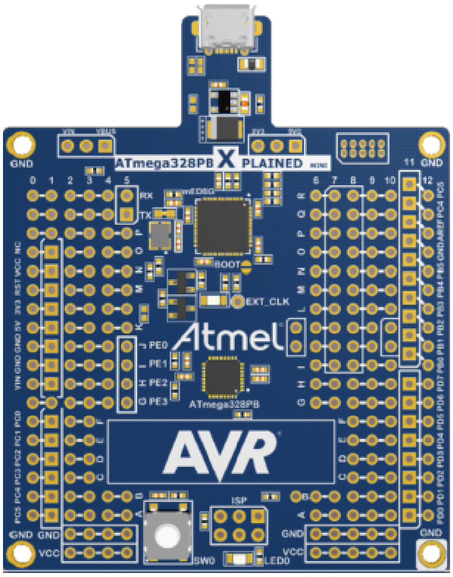
2. ATmega328PB Xplained Mini

2.1. Board Overview

The ATmega328PB Xplained Mini evaluation kit is a hardware platform to evaluate the Atmel ATmega328PB microcontroller. The evaluation kit comes with a fully integrated debugger that provides seamless integration with Atmel Studio 7.0 (and later version). The kit provides access to the features of the ATmega328PB enabling easy integration of the device in a custom design.

For more details about this kit, refer to the Atmel ATmega328PB Xplained Mini user guide available at http://www.atmel.com/Images/Atmel-42469-ATmega328PB-Xplained-Mini_User-Guide.pdf.

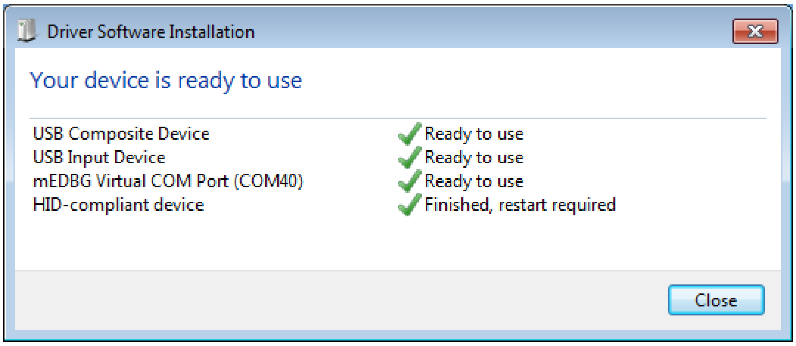
Figure 2-1. ATmega328PB Xplained Mini Kit



2.2. Enumeration and Detection

When the ATmega328PB Xplained Mini kit is connected to the PC, Windows® will enumerate the device and the install appropriate driver. If the driver installed successfully, mEDBG will be listed in the Device Manager as mEDBG Virtual COM port under Ports, as shown in the following screen-shots.

Figure 2-2. Tool Enumeration

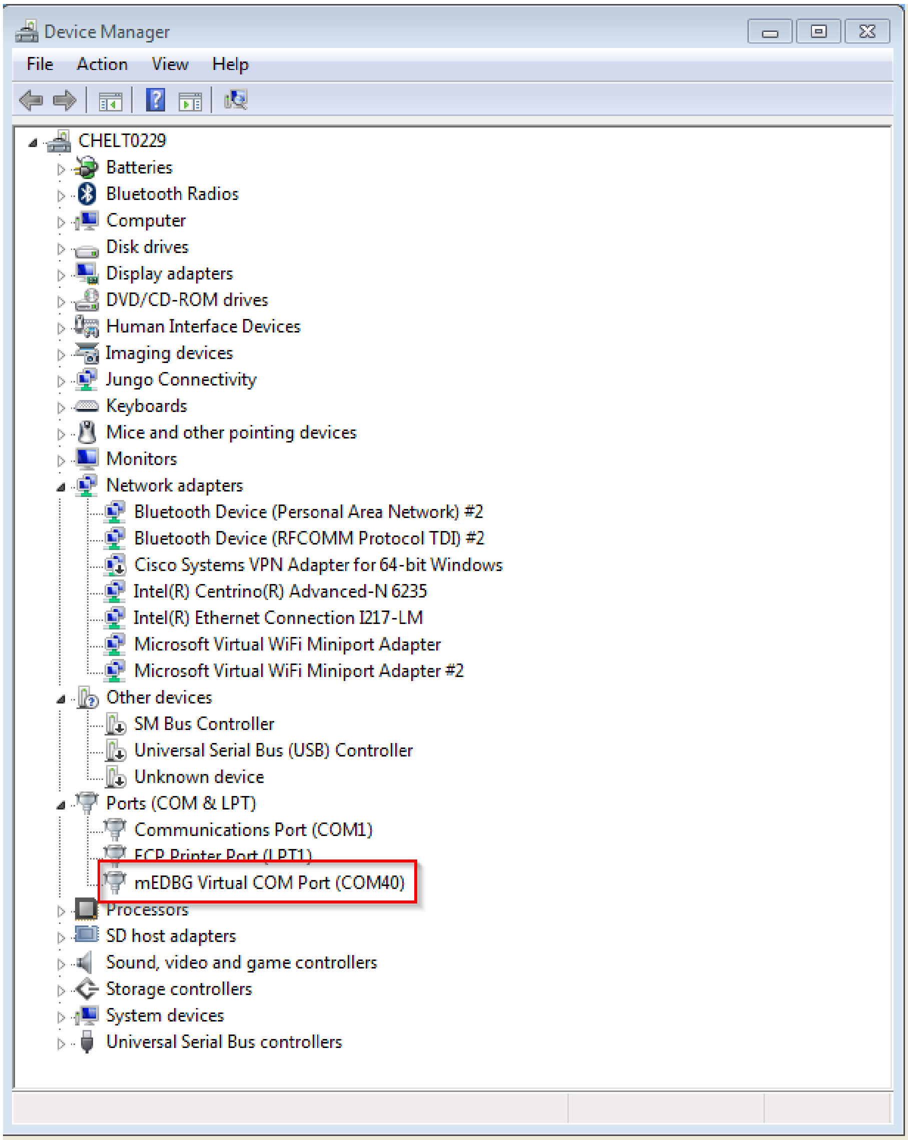


Driver Software Installation

Your device is ready to use

USB Composite Device	✓ Ready to use
USB Input Device	✓ Ready to use
mEDBG Virtual COM Port (COM40)	✓ Ready to use
HID-compliant device	✓ Finished, restart required

Figure 2-3. Successful mEDBG Driver Installation



```
CHELT0229
    Batteries
    Bluetooth Radios
    Computer
    Disk drives
    Display adapters
    DVD/CD-ROM drives
    Human Interface Devices
    Imaging devices
    Jungo Connectivity
    Keyboards
    Mice and other pointing devices
    Monitors
    Network adapters
        Bluetooth Device (Personal Area Network) #2
        Bluetooth Device (RFCOMM Protocol TDI) #2
        Cisco Systems VPN Adapter for 64-bit Windows
        Intel(R) Centrino(R) Advanced-N 6235
        Intel(R) Ethernet Connection I217-LM
        Microsoft Virtual WiFi Miniport Adapter
        Microsoft Virtual WiFi Miniport Adapter #2
    Other devices
        SM Bus Controller
        Universal Serial Bus (USB) Controller
        Unknown device
    Ports (COM & LPT)
        Communications Port (COM1)
        ECP Printer Port (LPT1)
        mEDBG Virtual COM Port (COM40)
    Processors
    SD host adapters
    Sound, video and game controllers
    Storage controllers
    System devices
    Universal Serial Bus controllers
```

3. AES-128 Software Example on ATmega328PB

This application note provides an example of AES encryption and decryption algorithm on ATmega328PB. The source code is available for download from Atmel START.

3.1. Description

This section gives short a description about the example of AES-128, covering all five modes.

- AES-128 and five confidentiality modes are implemented at two levels. The AES algorithm is implemented in the aes.c/aes.h file.
- The five confidentiality modes are implemented in the crypt.c/crypt.h file
- The example is implemented in a way that 64 bytes (i.e. 16 input blocks) of plain text are encrypted and decrypted using all modes separately
- The decrypting message can be viewed in the terminal window
- From the result if the decrypted data is the same as the plain text, this conforms the working of each mode
- The modes can be independently enabled or disabled in the conf_example.h as shown below. By default all the modes are enabled.

```
/* Set to true to enable respective mode
 * set to false to disable the respective mode
 */
//Enable/Disable ECB mode
#define AES_ECB    true

//Enable/Disable CBC mode
#define AES_CBC    true

//Enable/Disable CFB mode
#define AES_CFB    true

//Enable/Disable OFB mode
#define AES_OFB    true

//Enable/Disable CTR mode
#define AES_CTR    true
```

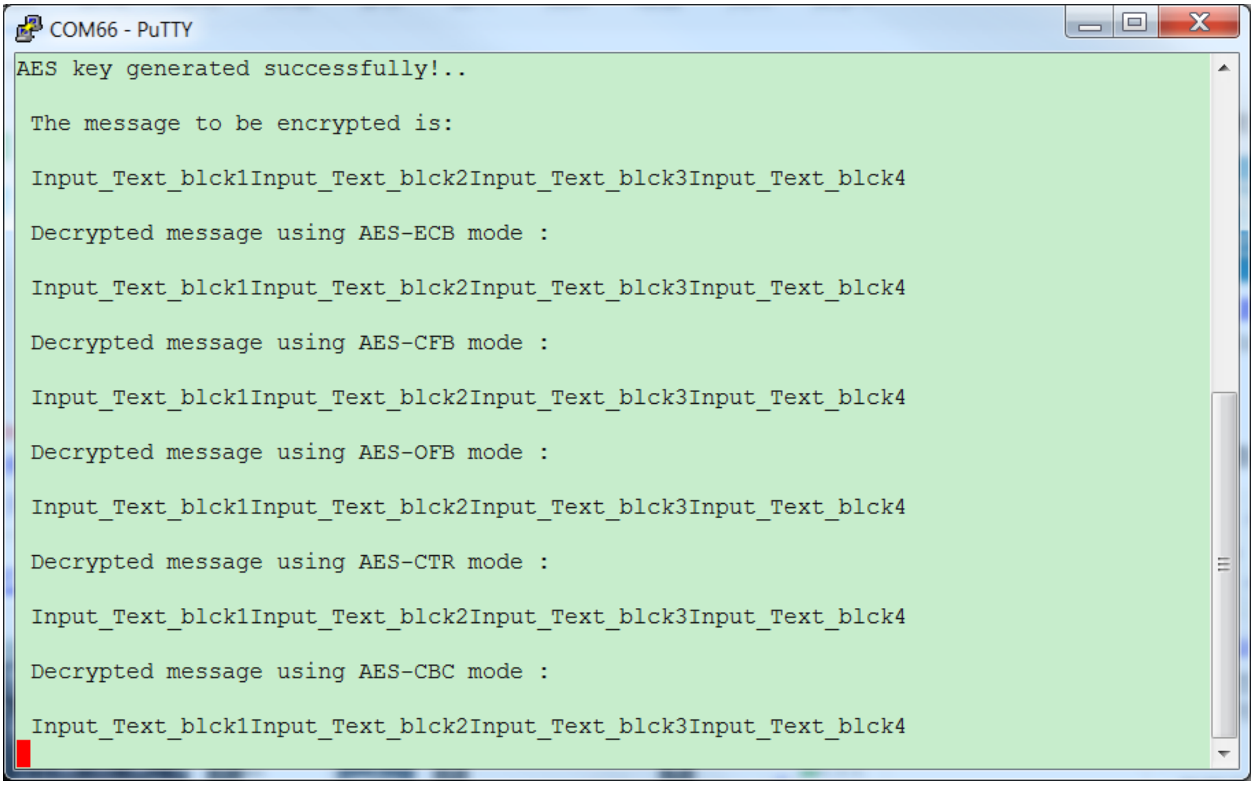
3.2. Setup

This example uses the USART0 module to print the message. PD0 is used to receive data, and PD1 is used to transmit data. In this example the USART0 will be configured with the following settings:

- Asynchronous mode
- 38400 Baudrate
- 8-bits, No Parity, and one Stop Bit

If everything is OK, in the terminal window the decrypted and actual input message can be viewed as below.

Figure 3-1. Running Results



```
AES key generated successfully!..

 The message to be encrypted is:

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4

 Decrypted message using AES-ECB mode :

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4

 Decrypted message using AES-CFB mode :

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4

 Decrypted message using AES-OFB mode :

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4

 Decrypted message using AES-CTR mode :

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4

 Decrypted message using AES-CBC mode :

 Input_Text_blck1Input_Text_blck2Input_Text_blck3Input_Text_blck4
```

4. References

- ATmega328PB datasheet (http://www.atmel.com/devices/ATMEGA328PB.aspx)
- ATmega328PB Xplained Mini kit (http://www.atmel.com/tools/MEGA328PB-XMINI.aspx)
- Atmel Studio (http://www.atmel.com/tools/atmelstudio.aspx?tab=overview)
- Atmel START (http://start.atmel.com)
- AT10764 (http://www.atmel.com/images/atmel-42508-software-library-for-aes-128-encryption-and-decryption_applicationnote_at10764.pdf)

5. Revision History

Doc Rev.	Date	Comments
42784A	09/2016	Initial document release

Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**

DISCLAIMER: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death (“Safety-Critical Applications”) without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.