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

- Introduction ......................................................................................................................1
- Features .......................................................................................................................... 1
  1. Prerequisites ..............................................................................................................3
  2. ATmega328PB Xplained Mini .................................................................................... 4
     2.1. Board Overview .......................................................................................................4
     2.2. Enumeration and Detection ...................................................................................4
  3. AES-128 Software Example on ATmega328PB ......................................................... 6
     3.1. Description ..............................................................................................................6
     3.2. Setup ...................................................................................................................... 6
  4. References ................................................................................................................ 8
  5. Revision History ........................................................................................................9
1. **Prerequisites**

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.


![Figure 2-1. ATmega328PB Xplained Mini Kit](image)

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](image)
Atmel AVR284: Software Library for AES-128 Encryption and Decryption on megaAVR [APPLICATION NOTE]

Figure 2-3. Successful mEDBG Driver Installation
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.

```c
/* Set to true to enable respective mode
   set to false to disable the respective mode */
#define AES_ECB    true
#define AES_CBC    true
#define AES_CFB    true
#define AES_OFB    true
#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 START (http://start.atmel.com)
5. Revision History

<table>
<thead>
<tr>
<th>Doc Rev.</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>42784A</td>
<td>09/2016</td>
<td>Initial document release</td>
</tr>
</tbody>
</table>