

序説

新暗号化規格(AES:Advanced Encryption Standard)は連邦情報処理規格(FIPS)197として2001年に米国国立標準技術研究所によって確定された電子データの暗号化のための仕様です。これは電子データの暗号化と復号のために使用される対称塊暗号算法です。この応用記述はAtmel® ATmega328PBでのAES暗号化と復号の算法の例を提供します。この応用を実演するのにATmega328PB Xplained Miniキットが使用されます。AESの理論については[AT10764: AES-128暗号化と復号用ソフトウェア ライブラリ](#)を参照してください。

特徴

- FIPS公示197,新暗号化規格(AES:Advanced Encryption Standard)適合
- AES暗号化と復号の算法
- 128ビット暗号化鍵を支援
- FIPSで指定されたAESの5つの秘密性動作種別
 - 電子符号本動作 (ECB:Electronic Codebook mode)
 - 暗号塊連鎖動作 (CBC:Cipher Block Chaining mode)
 - 暗号回帰動作 (CFB:Cipher Feedback mode)
 - 出力回帰動作 (OFB:Output Feedback mode)
 - 計数器動作 (CTR)
- CFB動作で可能な8,16,32,64,128ビットのデータの大きさ

目次

序説	1
特徴	1
1. 事前必要条件	3
2. ATmega328PB Xplained Mini	3
2.1. 基板概要	3
2.2. 列挙と検出	3
3. ATmega328PBでのAES-128ソフトウェア例	4
3.1. 説明	4
3.2. 構成設定	4
4. 参照	5
5. 改訂履歴	5

1. 事前必要条件

この資料で検討される解決策は以下が必要です。

- Atmel Studio 7.0またはそれ以降
- ATmega328PB Xplained Miniキット
- [Atmel START](#)(開始)からダウンロードで入手可能な例ソースコード

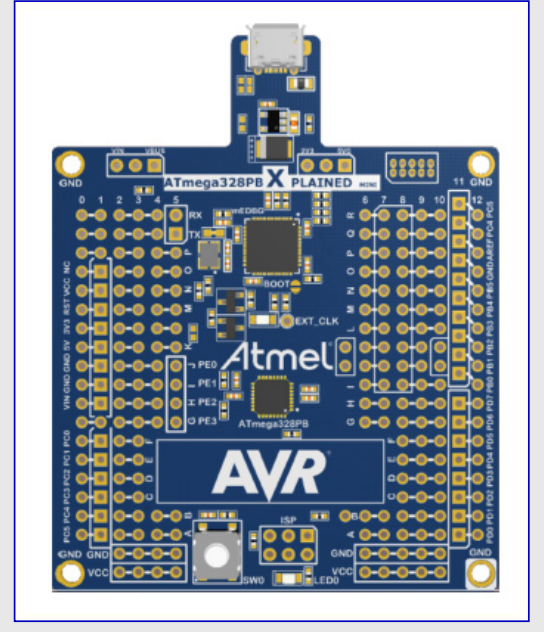
2. ATmega328PB Xplained Mini

2.1. 基板概要

ATmega328PB Xplained Mini評価キットはAtmel ATmega328PBマイクロコントローラを評価するためのハードウェア基盤です。この評価キットはAtmel Studio 7.0(とそれ以降版)との継ぎ目のない統合を提供する完全に統合されたデバッグと共にやって来ます。キットは独自設計でデバイスの容易な統合を許すATmega328PBの機能へのアクセスを提供します。

このキットについてのより多くの詳細に関しては、<http://www.atmel.com/Images/Atmel-42469-ATmega328PB-Xplained-Mini-User-Guide.pdf>で入手可能な「Atmel ATmega328PB Xplained Mini使用者の手引き」を参照してください。

図2-1. ATmega328PB Xplained Miniキット



2.2. 列挙と検出

ATmega328PB Xplained MiniキットがPCに接続されると、Windows®は装置を列挙(接続認証)して適切なドライバをインストールします。ドライバが成功裏にインストールされた場合、右の画面画像で示されるようにmEDBGはデバイスマネージャでポート下のmEDBG仮想COMポートとして一覧にされます。

図2-3. 成功したmEDBGドライバインストール

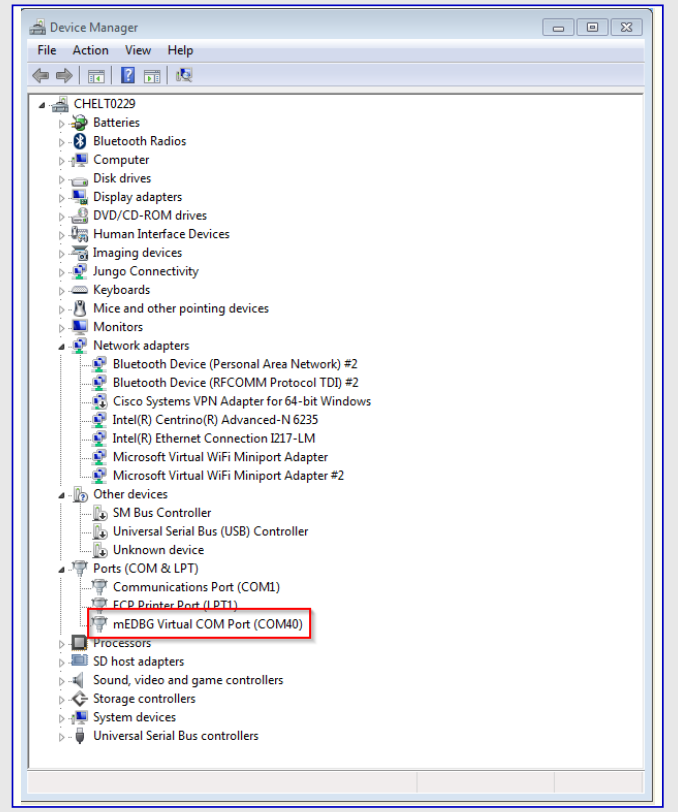
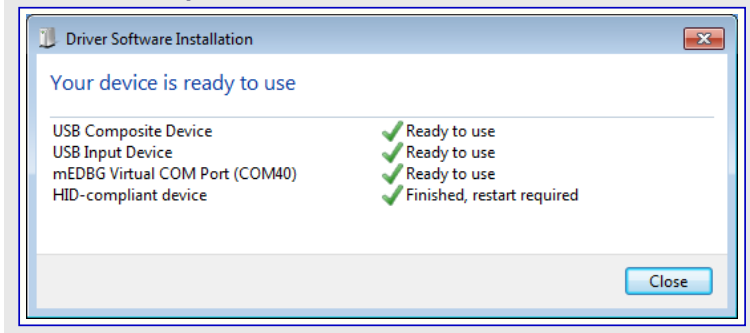


図2-2. ツール列挙



3. ATmega328PBでのAES-128ソフトウェア例

この応用記述はATmega328PBでのAES暗号化と復号の算法の例を提供します。ソースコードはAtmel START(開始)からのダウンロードで入手可能です。

3.1. 説明

本項は5つ全ての動作種別を網羅するAES-128の例についての短い説明を与えます。

- AES-128と5つの秘密性動作種別は2つのレベルで実装されます。AES算法は[aes.c/aes.h](#)のファイルで実装されます。
- 5つの秘密性動作種別は[crypt.c/crypt.h](#)のファイルで実装されます。
- 例は全ての動作種別を独立して用いて64バイト(即ち、16入力塊)の平文が暗号化されて復号されるように実装されます。
- 復号しているメッセージは端末ウィンドウで見ることができます。
- 復号されたデータが平文と同じ場合の結果から、これは各動作種別の動きと一致します。
- 動作種別は下で示されるように[conf_example.h](#)で独立して許可または禁止することができます。既定では全ての動作種別が許可されます。

```
/* 各々の動作種別を許可するにはtrueに設定してください。
 * 各々の動作種別を許可するにはfalseに設定してください。
 */
// ECB動作 許可/禁止
#define AES_ECB true

// CBC動作 許可/禁止
#define AES_CBC true

// CFB動作 許可/禁止
#define AES_CFB true

// OFB動作 許可/禁止
#define AES_OFB true

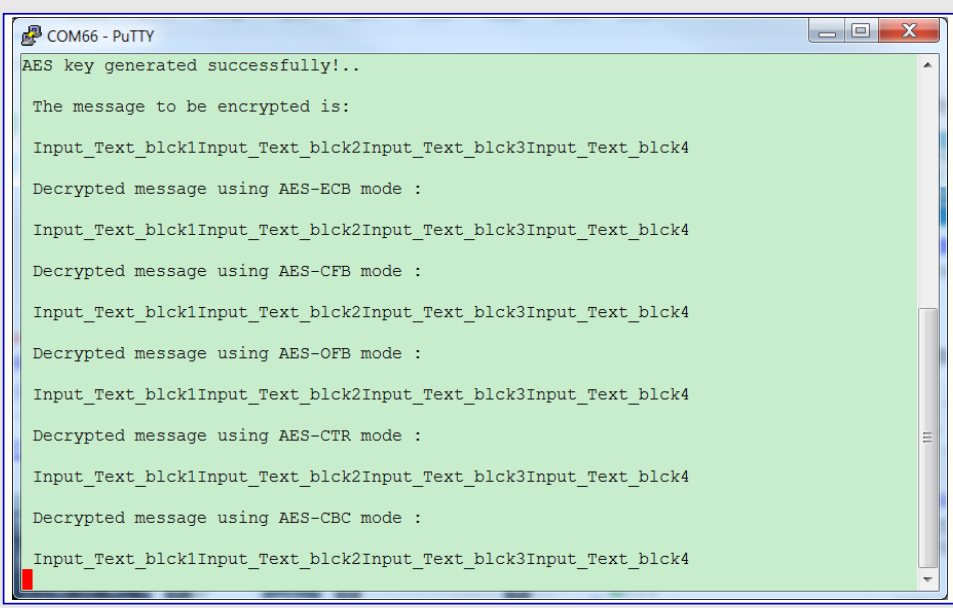
// CTR動作 許可/禁止
#define AES_CTR true
```

3.2. 構成設定

この例はメッセージを出力するのにUSART0単位部を使用します。データを受け取るのにPD0が使用され、データを送るのにPD1が使用されます。この例でのUSART0は以下の設定で形態設定されます。

- 非同期動作
- 38400bpsのボーレート
- 8ビットデータ、パリティなし、1停止ビット

全てがOKなら、実際の入力メッセージと復号は端末ウィンドウで下のように見ることができます。



```
COM66 - PuTTY
AES key generated successfully!..

The message to be encrypted is:

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4

Decrypted message using AES-ECB mode :

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4

Decrypted message using AES-CFB mode :

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4

Decrypted message using AES-OFB mode :

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4

Decrypted message using AES-CTR mode :

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4

Decrypted message using AES-CBC mode :

Input_Text_blk1Input_Text_blk2Input_Text_blk3Input_Text_blk4
```

4. 参照

- ATmega328PBデータシート (<http://www.atmel.com/devices/ATMEGA328PB.aspx>)
- ATmega328PB Xplained Miniキット (<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. 改訂履歴

資料改訂	日付	注釈
42784A	2016年9月	初版資料公開

Atmel®, Atmelロゴとそれらの組み合わせ、Enabling Unlimited Possibilities®, AVR®, megaAVR®とその他は米国及び他の国に於けるAtmel Corporationの登録商標または商標です。Windows®は米国及び他の国に於けるMicrosoft Corporationの登録商標です。他の用語と製品名は一般的に他の商標です。

お断り: 本資料内の情報はAtmel製品と関連して提供されています。本資料またはAtmel製品の販売と関連して承諾される何れの知的所有権も禁反言あるいはその逆によって明示的または暗示的に承諾されるものではありません。Atmelのウェブサイトに表示する販売の条件とAtmelの定義での詳しい説明を除いて、商品性、特定目的に関する適合性、または適法性の暗黙保証に制限せず、Atmelはそれらを含むその製品に関連する暗示的、明示的または法令による如何なる保証も否認し、何ら責任がないと認識します。たとえAtmelがそのような損害賠償の可能性を進言されたとしても、本資料を使用できない、または使用以外で発生する(情報の損失、事業中断、または利益と損失に関する制限なしの損害賠償を含み)直接、間接、必然、偶然、特別、または付随して起こる如何なる損害賠償に対しても決してAtmelに責任がないでしょう。Atmelは本資料の内容の正確さまたは完全性に関して断言または保証を行わず、予告なしでいつでも製品内容と仕様の変更を行う権利を保留します。Atmelはここに含まれた情報を更新することに対してどんな公約も行いません。特に別の方法で提供されなければ、Atmel製品は車載応用に対して適当ではなく、使用されるべきではありません。Atmel製品は延命または生命維持を意図した応用での部品としての使用に対して意図、認定、または保証されません。

安全重視、軍用、車載応用のお断り: Atmel製品はAtmelが提供する特別に書かれた承諾を除き、そのような製品の機能不全が著しく人に危害を加えたり死に至らしめることがかなり予期されるどんな応用(“安全重視応用”)に対しても設計されず、またそれらとの接続にも使用されません。安全重視応用は限定なしで、生命維持装置とシステム、核施設と武器システムの操作用の装置やシステムを含みます。Atmelによって軍用等級として特に明確に示される以外、Atmel製品は軍用や航空宇宙の応用や環境のために設計も意図もされていません。Atmelによって車載等級として特に明確に示される以外、Atmel製品は車載応用での使用のために設計も意図もされていません。

© HERO 2016.

本応用記述はAtmelのAVR284応用記述(Rev.42784A-09/2016)の翻訳日本語版です。日本語では不自然となる重複する形容表現は省略されている場合があります。日本語では難解となる表現は大幅に意識されている部分もあります。必要に応じて一部加筆されています。頁割の変更により、原本より頁数が少なくなっています。

必要と思われる部分には()内に英語表記や略称などを残す形で表記しています。

青字の部分はリンクとなっています。一般的に赤字の0,1は論理0,1を表します。その他の赤字は重要な部分を表します。