

Charm-crypto库安装记录



不懂球的2大业

关注

赞赏支持

Charm-crypto库安装记录



不懂球的2大业

关注

2019.11.18 19:26:00 字数 660 阅读 522

Charm-crypto简介

Charm-crypto 是一个框架,用于快速原型设计先进的密码系统。基于Python语言,它是从头设计的,减少开发时间和代码的复杂性,同时促进组件的重用。它支持基础密码库,包括对称加密方案,散列函数,PRNGs、数字签名、加密等。

安装过程

- 打开charm库的网址, <https://pypi.org/project/charm-crypto/0.43/>, 按照上面指示输入命令:

```
1 | pip install charm-crypto==0.43
```

然而不出所料,安装出错,显示如下:

```
building 'charm_core_math_pairing' extension
creating build/temp.linux-x86_64-3.6
creating build/temp.linux-x86_64-3.6/charm
creating build/temp.linux-x86_64-3.6/charm/core
creating build/temp.linux-x86_64-3.6/charm/core/math
creating build/temp.linux-x86_64-3.6/charm/core/math/pairing
creating build/temp.linux-x86_64-3.6/charm/core/math/pairing/module
creating build/temp.linux-x86_64-3.6/charm/core/math/pairing/module/pairingmodule.c
gcc -pthread -B /root/anaconda3/envs/gh/compiler_compat -Wl,--sysroot=/ -Wsign-compare -DNODEBUG -g -fwrapv -O3 -Wall
-ties/ -Icharm/core/math/pairing/module -I/root/anaconda3/envs/gh/include/python3.6m -c charm/core/math/pairing/module/pairingmodule.c -o
o
In file included from charm/core/math/pairing/module/pairingmodule.c:30:0:
charm/core/math/pairing/module/pairingmodule.h:37:17: fatal error: gmp.h: No such file or directory
compilation terminated.
error: command 'gcc' failed with exit status 1

ERROR: Command errored out with exit status 1: /root/anaconda3/envs/gh/bin/python -u -c 'import sys, setuptools, tokenize
py''''; __file__ = '/tmp/pip-install-bd712qj/charm-crypto/setup.py'''';f=getattr(tokenize, ''open'', open)(__
__).exec(code, __file__, ''exec'')' install --record /tmp/pip-record-kqmjmfv/install-record.txt --single-
d output.
```

安装charm报错

可以看到其中有一句: fatal error:gmp.h:No such file or directory。分析应该是缺少了某个库。继续阅读charm库的网址,发现需要依赖GMP库和PBC库。

- 安装GMP库: 打开GMP库网址<https://gmplib.org/#DOWNLOAD>, 选择GMP压缩文件下载, 这里我选择了gmp-6.1.2.tar.bz2文件下载, 下载完成后, 解压, 输入命令:

```
1 | tar -jxvf gmp-6.1.2.tar.bz2
```

解压得到gmp文件夹, 之后进入文件夹, 首先需要检查编译环境, 输入命令:

```
1 | ./configure
```

configure中, 发现报错提示:

```
1 | ...
2 | checking whether sscanf needs writable input... no
3 | checking for struct pst_processor.psp_iticksperclktick... no
4 | checking for suitable... configure: error: the variable 'M4' is $PATH or /usr/bin (see config.log)
```

写下你的评论...

评论0

赞

...

推荐阅读

你知道爱和喜欢的区别吗?

阅读 38,748

佛玲花开只为你第十三章

阅读 3,614

三生三世枕上书续写 (11) 去找燕

池悟、姬衡

阅读 11,307

《枕上书》番外五 家宴

阅读 9,986

最强之神 第六十二章

阅读 5,350

Charm-crypto库安装记录



不懂球的2大业

关注

赞赏支持

```
1 | sudo apt-get install m4
```

继续configure，没有报错，接着输入命令make和make install即可成功安装GMP库，接着进入/usr/local/lib查看是否安装成功，结果在/usr/local/lib下：

```
1 | libgmp.a libgmp.la libgmp.so libgmp.so.10 libgmp.so.10.3.2
```

显示有gmp的共享库，可以认为GMP库安装成功。

- 安装PBC库：打开PBC库的网址，<https://crypto.stanford.edu/ptb/download.html>，下载文件ptb-0.5.14.tar.gz，之后解压，解压命令：

```
1 | tar -zxvf ptb-0.5.14.tar.gz
```

进入解压后的文件夹，与GMP一样，首先检查编译环境，输入命令./configure，结果报错：

```
1 | ...
2 | checking how to run the C preprocessor... gcc -E
3 | checking whether ln -s works... yes
4 | checking whether make sets $(MAKE)... (cached) yes
5 | checking for flex... no
6 | checking for lex... no
7 | *****
8 | flex not found
9 | *****
```

提示缺少flex库，继续安装flex库：

```
1 | sudo apt-get install flex
```

安装成功后，继续configure，结果报错：

```
1 | checking whether yytext is a pointer... yes
2 | checking for bison... no
3 | checking for yacc... no
4 | *****
5 | bison not found
```

提示缺少bison库，继续安装bison库：

```
1 | sudo apt-get install bison
```

安装成功后，继续configure，接着输入make，make install即可安装，接着进入/usr/local/lib查看安装情况：

```
libgmp.so libgmp.so.10 libgmp.so.10.3.2 libptb.a libptb.la libptb.so libptb.so.1 libptb.so.1.0.0
```

文件夹存在ptb的共享库，可以认为ptb正确安装。

- 在安装好GMP和PBC库的情况下，再安装charm，依然报错：

推荐阅读

你知道爱和喜欢的区别吗？

阅读 38,748

佛玲花开只为你第十三章

阅读 3,614

三生三世枕上书续写（11）去找燕

池悟、姬衡

阅读 11,307

《枕上书》番外五 家宴

阅读 9,986

最强之神 第六十二章

阅读 5,350

写下你的评论...

评论0

赞

...

Charm-crypto库安装记录



不懂球的2大业

关注

赞赏支持

```
3 | compilation terminated.  
4 | error: command 'gcc' failed with exit status 1
```

显示缺少openssl/objects.h文件。在网上查找原因，
<https://blog.csdn.net/shakeme/article/details/80911441>，按照网页说明输入命令：

```
1 | sudo apt-get install libssl-dev
```

再次安装输入pip install charm-crypto==0.43没有报错即可。若还报错,输入：

```
1 | sudo apt-get install libssl1.0-dev
```

验证安装成功与否

打开python，输入：

```
1 | import charm
```

没有报错即可。

0人点赞 >

课题记录

"小礼物走一走，来简书关注我"

赞赏支持

还没有人赞赏，支持一下



不懂球的2大业 盖文章,经国之大业,不朽之盛事。
总资产2 (约0.21元) 共写了8697字 获得10个赞 共5个粉丝

关注

写下你的评论...

全部评论 0 只看作者

按时间倒序 按时间正序

推荐阅读

CP-ABE库安装步骤

初学CP-ABE库的安装，遇到了不少弯，现总结如下：- cp-abe依赖pbc，pbc依赖gmp，gmp依赖M4...

mxhxtfh 阅读 615 评论 0 赞 0

更多精彩内容 >

```
1 | tar -xvf libhomq-0.9.tar.gz  
2 | cd libhomq-0.9  
3 | ./configure  
4 | make  
5 | make install  
  
然后安装cpabe  
1 | tar -xvf cpabe-0.11.tar.gz  
2 | cd cpabe-0.11  
3 | ./configure  
4 | make  
5 | make install
```

写下你的评论...

评论0 赞

Charm-crypto库安装记录



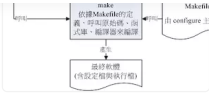
不懂球的2大业

关注

赞赏支持



Zhang21 阅读 4,131 评论 0 赞 10



12C CDB模式下RMAN备份与恢复_3

背景: 阅读新闻 12C CDB模式下RMAN备份与恢复 [日期:2016-11-29] 来源:Linux社区 作...



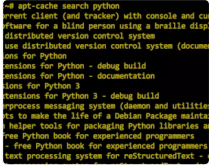
阳屯okyepd 阅读 1,614 评论 0 赞 5

极迅云课（服务端教案）

一、Python简介和环境搭建以及pip的安装 4课时实验课主要内容 【Python简介】： Python 是一个...



小老虎 阅读 3,573 评论 0 赞 5



Charm安装指南（Linux）

1、了解Charm之前的相关依赖 ---Python2.7 or Python3 ---Pyparsing 基于P...



未央的I 阅读 168 评论 0 赞 1

推荐阅读

你知道爱和喜欢的区别吗？

阅读 38,748

佛玲花开只为你第十三章

阅读 3,614

三生三世枕上书续写（11）去找燕

池悟、姬衡

阅读 11,307

《枕上书》番外五 家宴

阅读 9,986

最强之神 第六十二章

阅读 5,350

写下你的评论...

评论0

赞

...