将下载回来的压缩包解压，进入解压后的目录，即可使用 config 或 Configure 脚本进行配置。OpenSSL的配置脚本与大多数典型的软件包不同，它有自己的一套规则。详细的安装信息位于源码树下的 INSTALL Configure(特别是"PROCESS\_ARGS"段) Makefile.shared Makefile.org 文件中。安装后的使用与配置信息位于 doc 目录中， FAQ 文件也可以提供一些参考。

config 脚本检查系统环境并调用 Configure 完成配置，因此配置选项是通过 config 脚本向 Configure 传递的。事实上 config 脚本的作用相当于 config.guess ，所以如果你想直接调用 Configure 的话就一定要正确指定"操作系统-目标平台"(笔者推荐这个用法)。所有可用的目标机器列表可以使用"./Configure LIST"命令获取。Configure 脚本除了根据 Makefile.org 生成 Makefile 之外，还在 crypto/opensslconf.h 中定义了许多宏(基于 crypto/opensslconf.h.in)。

在 config 或 Configure 命令行上可以使用许多选项，大体上可以分为3类。

**全局选项**

第一类是全局性选项：

**--openssldir=OPENSSLDIR**

安装目录，默认是 /usr/local/ssl 。

**--prefix=PREFIX**

设置 lib include bin 目录的前缀，默认为 OPENSSLDIR 目录。

**--install\_prefix=DESTDIR**

设置安装时以此目录作为"根"目录，通常用于打包，默认为空。

**zlib  
zlib-dynamic  
no-zlib**

使用静态的zlib压缩库、使用动态的zlib压缩库、不使用zlib压缩功能。

**threads  
no-threads**

是否编译支持多线程的库。默认支持。

**shared  
no-shared**

是否生成动态连接库。

**asm  
no-asm**

是否在编译过程中使用汇编代码加快编译过程。

**enable-sse2  
no-sse2**

启用/禁用SSE2指令集加速。如果你的CPU支持SSE2指令集，就可以打开，否则就要关闭。

**gmp  
no-gmp**

启用/禁用GMP库

**rfc3779  
no-rfc3779**

启用/禁用实现X509v3证书的IP地址扩展

**krb5  
no-krb5**

启用/禁用 Kerberos 5 支持

**ssl  
no-ssl  
ssl2  
ssl3  
no-ssl2  
no-ssl3  
tls  
no-tls**

启用/禁用 SSL(包含了SSL2/SSL3) TLS 协议支持。

**dso  
no-dso**

启用/禁用调用其它动态链接库的功能。[提示]no-dso仅在no-shared的前提下可用。

[提示]为了安装Apache的mod\_ssl成功，SSLv2/SSLv3/TLS都必须开启。

**算法选项**

第二类用于禁用crypto目录下相应的子目录(主要是各种算法)。虽然理论上这些子目录都可以通过"no-\*"语法禁用，但是实际上，为了能够最小安装libcrypto,libssl,openssl，其中的大部分目录都必须保留，实际可选的目录仅有如下这些：

**no-md2,no-md4,no-mdc2,no-ripemd**

这些都是摘要算法，含义一目了然。

**no-des,no-rc2,no-rc4,no-rc5,no-idea,no-bf,no-cast,no-camellia**

这些都是对称加密算法，含义一目了然。"bf"是"Blowfish"的意思。

**no-ec,no-dsa,no-ecdsa,no-dh,no-ecdh**

这些都是不对称加密算法，含义一目了然。

**no-comp**

数据压缩算法。因为目前实际上并没有压缩算法，所以只是定义了一些空接口。

**no-store**

对象存储功能。更多细节可以查看 crypto/store/README 文件。

[提示]OpenSSH 只依赖于该软件包的加密库(libcrypto)，而带有 HTTPS 支持的 Apache 则依赖于该软件包的加密库和 SSL/TLS 库(libssl)。因此，如果你不打算使用 HTTPS 的话，可以只安装加密库(no-ssl no-tls)；更多介绍可以查看 README 文件的"OVERVIEW"部分。事实上，为了能够让OpenSSH安装成功，ripemd,des,rc4,bf,cast,dsa,dh目录不能被禁 止。

**编译器选项**

第三类是编译器选项。大多数软件包都是通过在运行 configure 脚本的时候定义 CPPFLAGS CFLAGS LDFLAGS 环境变量来设置编译选项的，但是OpenSSL却不是这样。OpenSSL的 Configure 脚本允许你在命令行上直接输入 CPPFLAGS CFLAGS 的内容。比如：-DDEVRANDOM='"/dev/urandom"' 可以用来指定随机设备， -DSSL\_FORBID\_ENULL 则可以用于禁止使用NULL加密算法。`echo $CFLAGS` 则可以将 CFLAGS 变量添加上来。另一方面，LDFLAGS却是无法通过Configure进行设置的。因为Configure会强制清空Makefile中的 LDFLAGS，所以在运行完Configure之后，可以使用一个sed修改所有Makefile中的 LDFLAGS(用于连接openssl)和SHARED\_LDFLAGS(用于连接libcrypto,libssl库)。

比如笔者就经常这样使用 Configure 进行配置：

./Configure ... -DSSL\_FORBID\_ENULL -DDEVRANDOM='"/dev/urandom"' `echo $CFLAGS`

find . -name "Makefile\*" -exec sed -r -i -e"s|^(SHARED\_)?LDFLAGS=|& $LDFLAGS |" {} \;

[提示]不能省略find命令内"Makefile\*"两边的引号。