现代密码学课程设计任务书

姓名：　杨礼珍

2019年

目　录

第一章　课程设计任务

1.1 如何提交及其他

- 提交时间：开学前提交
- 提交方式：
  - 统一发到我的邮箱：yanglizhen_exe@163.com
- 任务书下载email: yanglizhen_course@163.com，密码：tongjics

1.2 提交文档

1. 课程设计报告。需是.ps或者.pdf文档（如何转成.ps或.pdf文档见第2章附录），不接收word或其它类型的文档。
2. 源代码。要求编程语言为C++，编译器为VC6.0或VS2003。
3. 可运行程序。

1.3 准备工作

阅读《密码学原理与实践》7.1节、7.3节、9.1节、9.3节、12.1－12.3.1节（P.351-357）。

1.4 编程基本要求和任务

基本要求：

- 公钥密码中用到的高精度计算使用开源代码库NTL（官网：http://www.shoup.net/ntl/ ），不接受使用其他代码库。该库使用简单友好。源码库网站上有使用说明书，中文网上也有不少使用介绍。
- 程序的输入友好，不能有大量手工控制台输入。
- 注意代码的可读性、可扩展性和可重用性，禁止使用全局变量。
- 方案和协议中涉及到的传输过程不需要实际的网络通信。
- 主函数不包含具体细节的实现代码，只调用其他功能模块。
- 不要求可视化，控制台程序亦可。

编程任务：

1. 实现《密码学原理与实践》7.1节的RSA签名方案，基于NTL库实现。其中素数p, q要求为512比特。
2. 实现《密码学原理与实践》7.3节的ElGamal签名方案（密码体制7.2），基于NTL库实现。其中素数p取为1024比特。素数p和本原元α生成过程：
   (a) 产生素数$p = 2q_0 + 1$，q_0为大素数。使用NTL中的素性测试算法。
   (b) 产生模p本原元α：产生随机数$\alpha \in \mathbb{Z}_p^*$，根据以下定理判定$\alpha$是否为本原元。如果不是则产生其它随机数继续测试。

   定理 1.1: *如果$p > 2$是素数，且$\alpha \in \mathbb{Z}_p^*$。那么$\alpha$是模$p$的本原元当且仅当*

$$\alpha^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}, \text{对所有素数} q|p-1$$

3. 实现《密码学原理与实践》9.3.1节的基本证书方案的改进版（和9.3.1节的证书的区别是证书增加了TA的ID和签名算法标志，相应地签名和验证的输入也需加入这两项，具体见下），包含证书颁发（协议9.5的改进版）和证书验证。

   证书颁发协议 TA向Alice颁发证书

   1. TA形成一个串，记为ID(Alice)，其中ID(Alice)为Alice的姓名或email。

   2. TA生成Alice的秘密签名密钥sig_{Alice}和相应的公开验证密钥ver_{Alice}。Alice的签名密钥对支持RSA和ElGamal两种签名密钥。如果是RSA签名密钥对，则设置$flag_{Alice} = 0$，如果是ElGamal签名密钥对，则设置$flag_{Alice} = 1$。

   3. TA生成对Alice的ID、Alice的验证密钥、TA的ID和签名算法标识的签名s，即

$$s = sig_{TA\text{的私钥}}(ID(Alice)||ver_{Alice}||ID(TA)||flag_{Alice}||flag_{TA})$$

   把证书(为txt格式)

$$Cert(Alice) = (ID(Alice)||ver_{Alice}||ID(TA)||flag_{Alice}||flag_{TA})$$

   连同Alice的私钥sig_{Alice}一起传给Alice。其中ver_{Alice}表示Alice的公钥；$flag_{TA}$为TA使用的签名算法的标识，如果使用RSA签名，则$flag_{TA} = 0$，如果使用ElGamal签名，则$flag_{TA} = 1$。

   证书验证算法 Bob通过以下等式来验证Alice的证书

$$ver_{TA\text{的公钥}}(ID(Alice)||ver_{Alice}||ID(TA)||flag_{Alice}||flag_{TA}, s) = true$$

如果等式成立则通过Alice的证书验证，否则不通过。

4. 实现《密码学原理与实践》12.3.1节中的严格层次PKI系统的简易版本，要求如下：

   (a) 包含一个根CA（CA_{root}），根CA的证书由自己签名，自己给自己颁发。
   (b) 根CA下有2个下级CA（CA_1, CA_2），它们的证书由根CA签名和颁发。
   (c) CA_1, CA_2下是用户。用户证书由CA_1或CA_2签名和颁发。
   (d) 各个CA生成证书后，把证书存储到证书库中。
   (e) 实现一个可公开查询的证书库。该证书库存储了该PKI系统的所有证书。证书库的功能有：
      i. 只存储CA发来的证书。
      ii. 对任何人提出的查询申请（申请内容为证书所属者的ID），返回证书路径。如Bob发送申请为ID(Alice)，而Alice的证书由CA_1颁发，则证书库返回的证书路径是

      $$CA_{root}\text{的证书}, CA_1\text{的证书}, Alice\text{的证书}$$

   (f) 实现该证书系统的一个使用例子：
      i. Alice向CA_1或CA_2申请证书，CA生成Alice的证书，并把Alice的证书存储到系统的证书库中供以后查询。
      ii. Bob也向CA_1或CA_2申请证书，CA生成Bob的证书，并把Bob的证书存储到系统的证书库中。
      iii. Eve也向CA_1或CA_2申请证书，CA生成Eve的证书，并把Eve的证书存储到系统的证书库中。
      iv. Alice向Bob发送消息和该消息的签名。
      v. Bob在证书库中查询Alice的证书，证书库向Bob返回Alice的证书路径（或称为证书链）（包含根CA的证书、给Alice颁发证书的CA的证书及Alice的证书）。
      vi. Bob验证Alice的证书路径是否正确，如果正确，那么用ALice的证书中的公钥验证Alice发来的签名是否正确。

5. 对以上1－4的方案和协议均有独立的测试函数。
6. 不同对象（如TA、CA、证书库、Alice和Bob）完成的任务都应用独立的模块完成。注意，独立的模块不是用几个程序完成。

1.5 课程设计报告组成

1. 封面，包含学号，姓名
2. 软件设计说明书，包括基本数据结构说明，功能模块说明（包含每个函数的功能说明）。
3. 软件使用说明书，必须包含输入格式说明及例子。

1.6 评分准则

根据任务完成程度和代码的质量评分。代码的质量根据代码的可读性、可扩展性、可重用性和软件使用友好度判断。

第二章　附录：如何转化成.ps和.pdf文档

2.1 .ps和.pdf文档阅读器

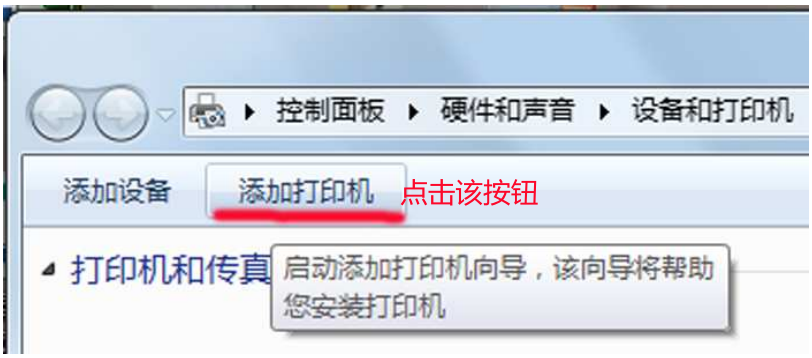
- GSView：.ps文档阅读器，为免费软件，可网上搜索下载（如：http://www.onlinedown.net/soft/6218.htm）
- Adobe Reader：.pdf文档阅读器，可网上搜索下载

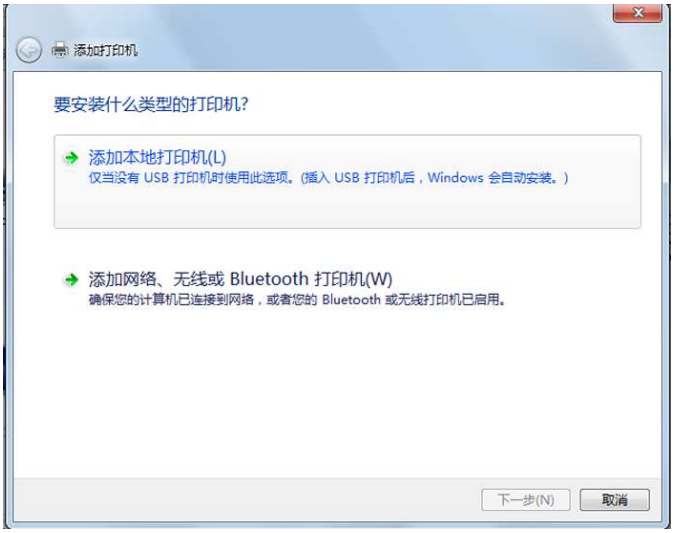
2.2 如何转化成.ps文档

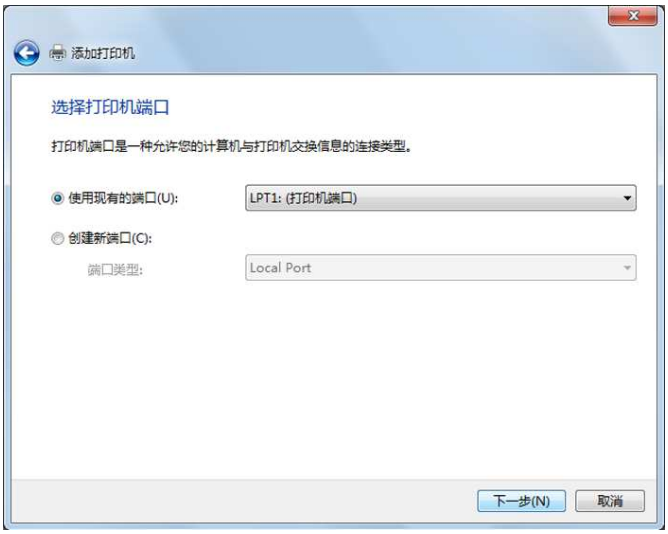
1. 安装postscript虚拟打印机驱动，以win7为例步骤如下：

   (a) 点击“添加打印机”对话框：点击开始菜单–>设备和打印机。 在打开的

“设备和打印机”页面，点击“添加打印机”按钮。

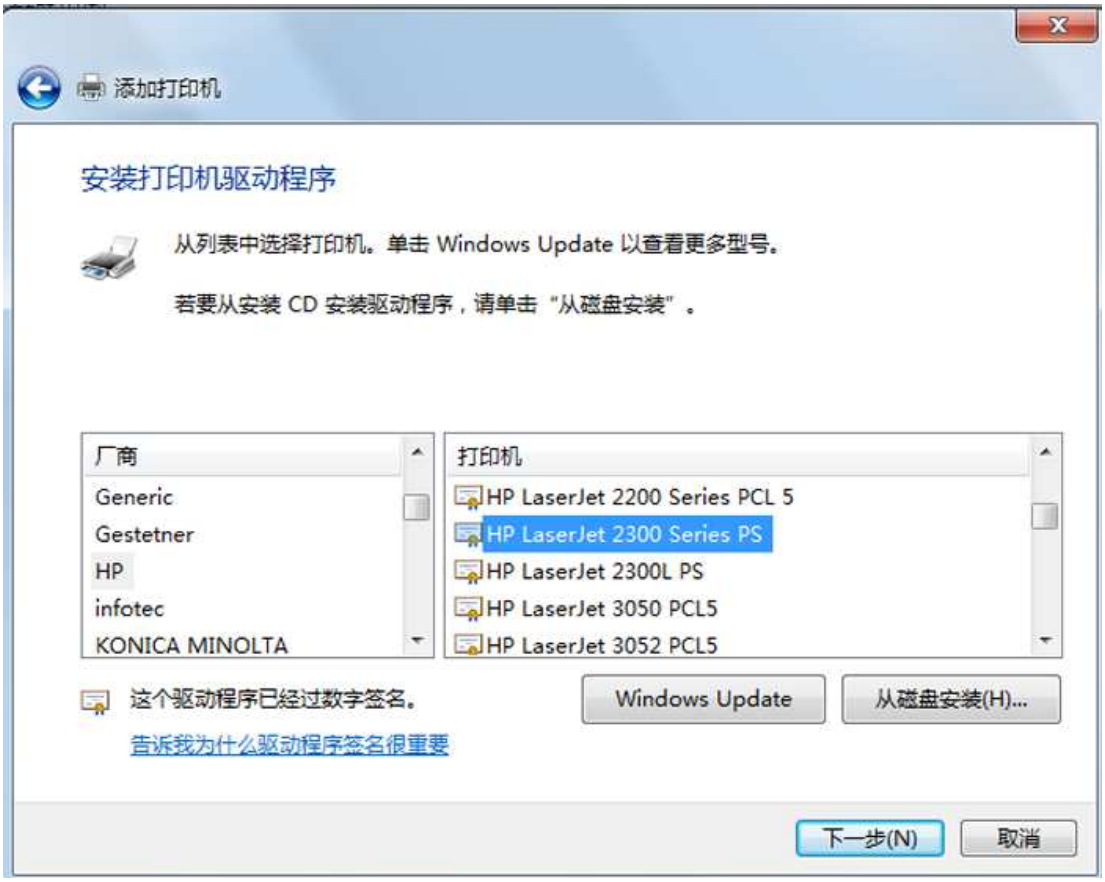






(b) 在“添加打印机”对话框中点击“添加本地打印机”。在“选择打印机端口”页面，点击“下一步”按钮。在“安装打印机驱动程序”页面，从打印机列表中选择postscript 打印机（很多厂商都提供有postscript打印机驱动，大部分为系统自带有），例如选择HP的HP LaserJet 5/5M PostScript、LaserJet 2300 Series PS打印机。如果电脑中没

有postscript打印机驱动，可在网上搜索，如Adobe提供的postscript打印驱动：http://www.adobe.com/support/downloads/product.jsp?product=44platform=Windows



(c) 后面步骤请按照个人喜好设置

2. 把编辑好的文档（如word文档）用postscript打印机打印成.ps文档

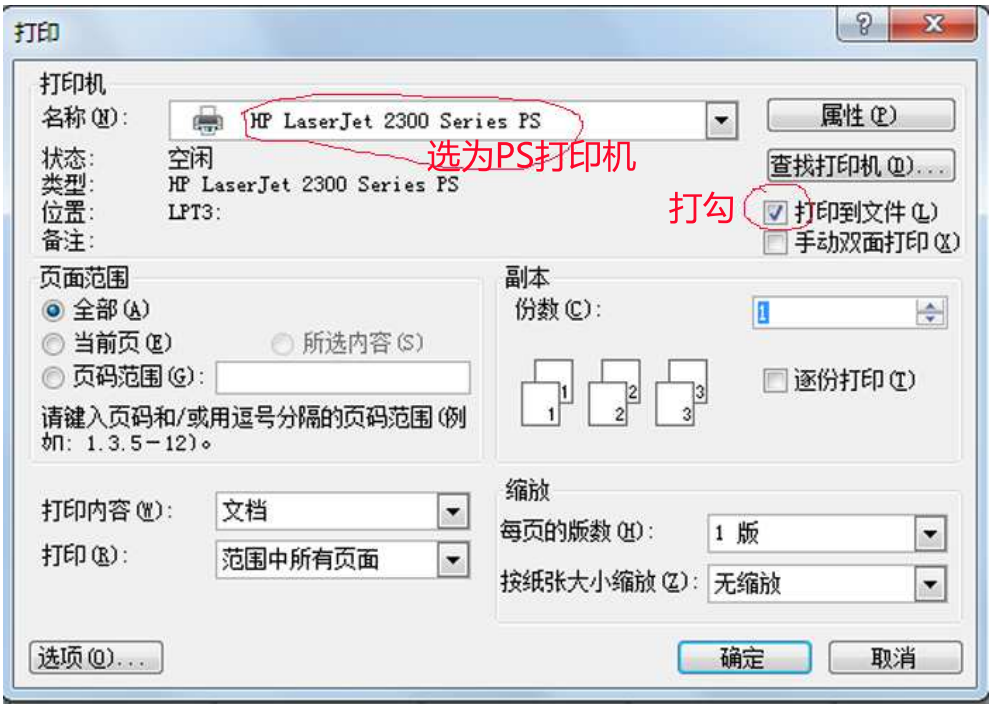
(a) 打开打印页面

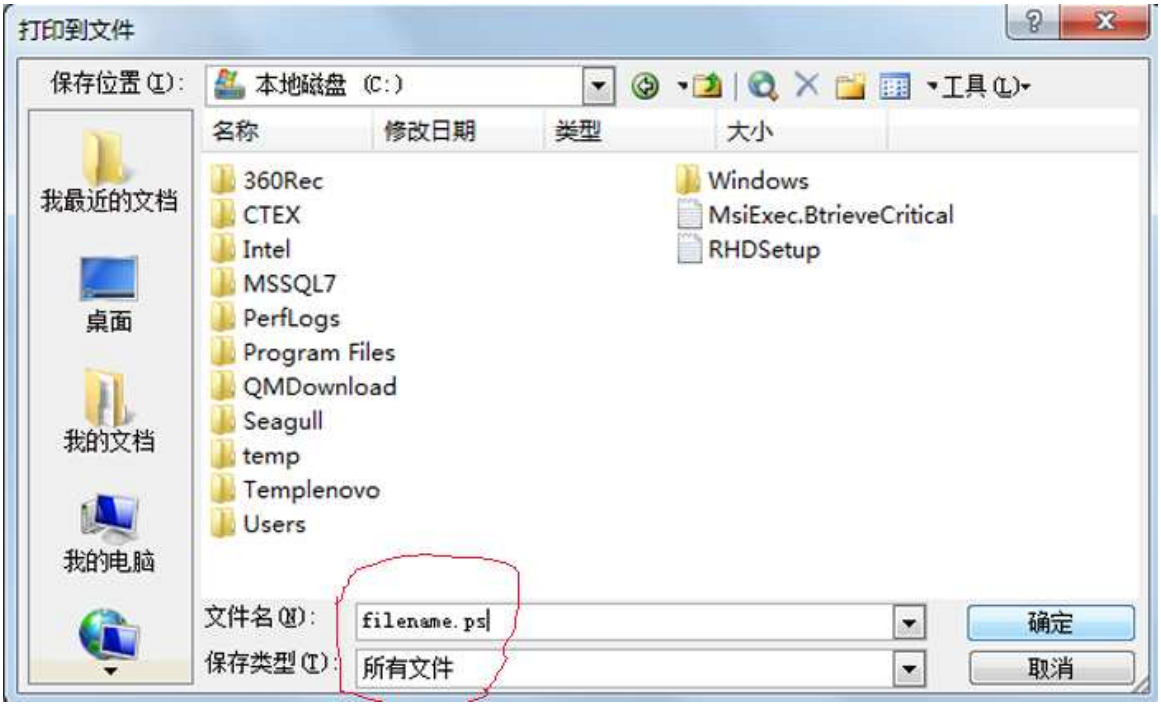
(b) 打印机名称选择为已安装的postscript打印机，对“打印到文件”选择框打勾，点击“打印”按钮后打开“保存到文件...”对话框

(c) “保存到文件...”对话框中：选择保存目录，保存类型选择为“所有文件(*.*)”，文件名称为：名称.ps，最后点击“保存”按钮。（如文件类型选择为“打印机文件(.prn)”，则生成文档名称后会加上后缀“.prn”，则需要手动删掉文档名称后的“.prn”后缀。）

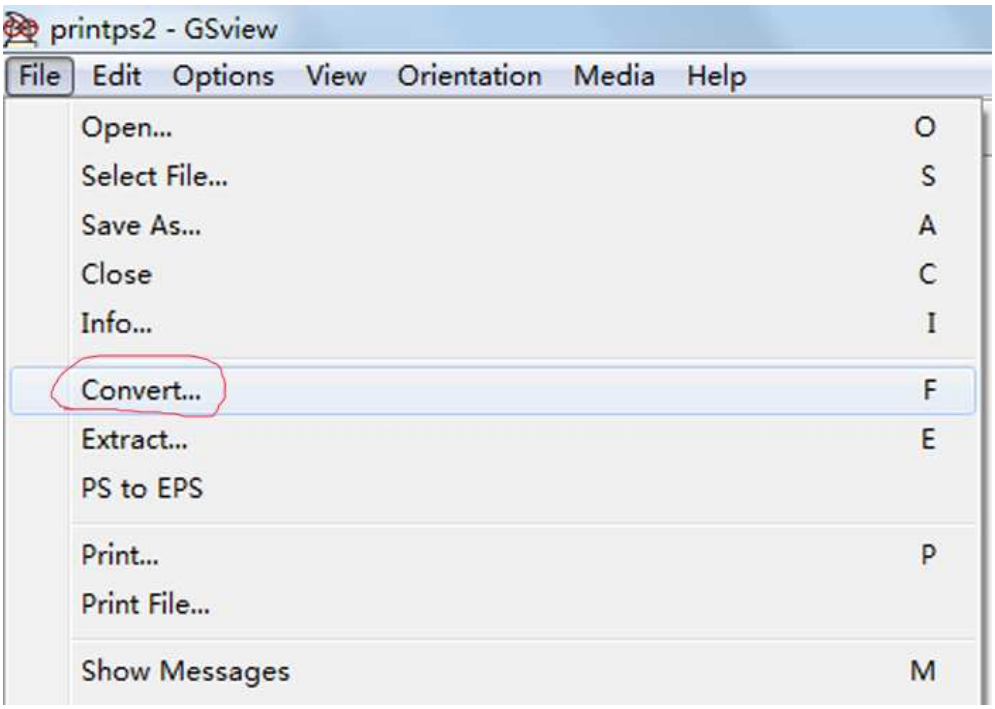
2.3 如何转化成.pdf文档

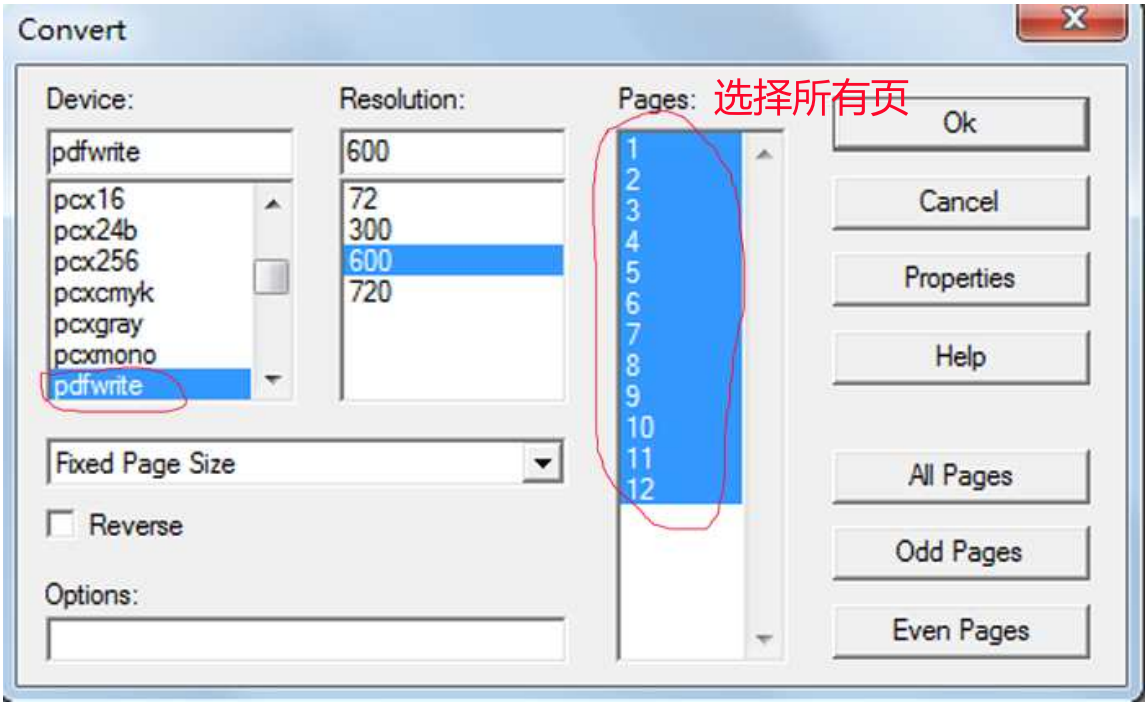
1. 按第2.2节方法转化成.ps文档





2. 用GSView打开.ps文档，点击File–>Convert...，弹出Convert对话框，选择Device栏为pdfwrite，Pages确认为默认值（即选择所有页数），点击OK按钮后，弹出OutPut Filename对话框：选择保存目录，填写文件名为：名称.pdf，点击“保存”按钮。


printps2 - GSview
File
Edit
Options
View
Orientation
Media
Help
Open... O
Select File... S
Save As... A
Close C
Info... I
Convert... F
Extract... E
PS to EPS
Print... P
Print File...
Show Messages M


Convert
Device:
pdfwrite
pcx16
pcx24b
pcx256
pcxcmyk
pcxgray
pcxmono
pdfwrite
Resolution:
600
72
300
600
720
Pages:
选择所有页
1
2
3
4
5
6
7
8
9
10
11
12
Fixed Page Size
Reverse
Options:
Ok
Cancel
Properties
Help
All Pages
Odd Pages
Even Pages