

汇编语言程序设计作业

以下程序要求使用 AT&T 的汇编语法，在 Linux 上使用 gcc 编译链接运行。不允许编写成其他高级语言再使用 gcc 生成汇编代码，也不可以调用除 printf() 以外的已有的 C lib 函数协助完成。

1. 倒置一个字符串

将一个字符串前后颠倒存储，字符串可以预先存储在.data 区中，先输出该字符串，再前后颠倒存储后输出一遍。例如，设原字符串为 “ This is a test string.” 则输出内容为：

This is a test string.

.gnirts tset a si sihT

2. 求 1000 以内的全部素数

素数

编写程序，使用厄拉多塞过滤算法（Sieve of Eratosthenes）生成 2 ~ 1000 之间的全部素数。互联网上可以发现很多文章描述了使用该算法寻找素数的方法。要求显示所有的素数。

厄拉多塞过滤算法

厄拉多塞（Eratosthenes）过滤算法，由同名的希腊数学家发明，提供了在给定范围内快速查找所有质数的方法。该算法创建一个字节数组，并按如下方式在“被标记”位置上插入 1：从位置 2（2 是质数）开始，则数组中所有 2 的倍数的位置都插入 1。接着，对下一个质数 3，用同样的方法处理 3 的倍数。查找 3 之后的质数，该数为 5，再对所有 5 的倍数的位置进行标记。持续这种操作直到找出质数的全部倍数。那么，剩下数组中没有被标记的位置就表示其数为质数。

3. 消息加密。明文和密钥可以预先存储在.data 区中。输出格式为第一行为明文，第二行为密钥，第三行为密文。

消息加密

创建包含多个字符的密钥。使用该密钥，通过将密钥与明文相应位进行按位 XOR 运算，来对明文加密和解密。按需重复使用密钥，直到明文中的所有字节都转换完。例如，假设密钥为 “ABXmv#7”，则密钥与明文字节之间的对应如下图所示：

明文	T	h	i	s		i	s		a		P	l	a	i	n	t	e	x	t		m	e	s	s	a	g	e	(等等)
密钥	A	B	X	m	v	#	7	A	B	X	m	v	#	7	A	B	X	m	v	#	7	A	8	X	m	v	#	7

(重复密钥，直到其与明文等长……)