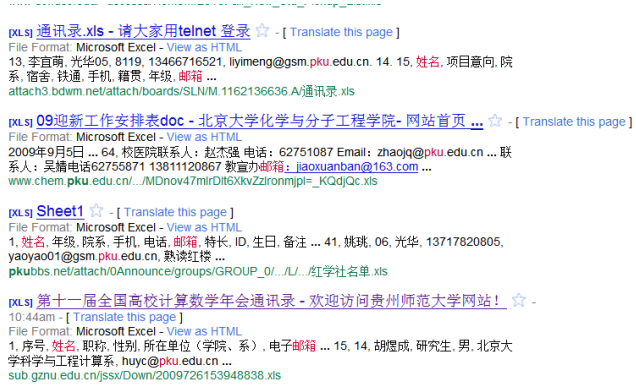
攻击方法与过程：

首先，我们在问卷星上建立一个主题为“星座文化对当代大学生性格影响”的网上问卷调查，并声称自己是北大心理系的学生。为加强伪装效果，我们自己首先填写了若干份有效问卷，并决定用北大域名的邮箱发信。我们将自己的 PKU 邮箱地址分别改为 questionnairepsy@pku.edu.cn 和 astro_psy@pku.edu.cn,分别作为发信邮箱，相应的修改发信人为 questionnairepsy 和 astro_psy。

我们利用 Gooogle 搜索引擎，尝试获取攻击目标的姓名、邮箱等基本信息。开始时，我们想要获得一些关于北大学生的信息，因此，我们在搜索框中输入：邮箱 姓名 filetype:xls pku，结果返回众多包含姓名、邮箱信息的 excel 文件（如图 1 示）。其中，有一个链接指向 XX 师范大学，上面包含第十一届全国高校计算数学年通讯录。这引起了我们的兴趣。于是我们决定从这份名单入手，展开攻击。

经过上述准备，我们从 29 号早晨开始进行社会学攻击。


[XLS] 通讯录.xls - 请大家用telnet 登录 - [Translate this page]
File Format: Microsoft Excel - View as HTML
13, 李宜萌, 光华05, 8119, 13466716521, liyimeng@gsm.pku.edu.cn. 14. 15, 姓名, 项目意向, 院系, 宿舍, 铁通, 手机, 籍贯, 年级, 邮箱 ...
attach3.bdwm.net/attach/boards/SLN/M.1162136636.A/通讯录.xls

[XLS] 09迎新工作安排表doc - 北京大学化学与分子工程学院- 网站首页 ... - [Translate this page]
File Format: Microsoft Excel - View as HTML
2009年9月5日 ... 64, 校医院联系人：赵杰强 电话：62751087 Email：zhaojq@pku.edu.cn ... 联系人：吴婧电话62755871 13811120867 教宣办邮箱：jiaoxuanban@163.com ...
www.chem.pku.edu.cn/.../MDnov47mlrDlt6XkvZzlronmjpl=_KQdjQc.xls

[XLS] Sheet1 - [Translate this page]
File Format: Microsoft Excel - View as HTML
1, 姓名, 年级, 院系, 手机, 电话, 邮箱, 特长, ID, 生日, 备注 ... 41, 姚珑, 06, 光华, 13717820805, yaoyao01@gsm.pku.edu.cn, 熟读红楼 ...
pkubbs.net/attach/0Announce/groups/GROUP_0/.../L/.../红学社名单.xls

[XLS] 第十一届全国高校计算数学年会通讯录 - 欢迎访问贵州师范大学网站！ - 10:44am - [Translate this page]
File Format: Microsoft Excel - View as HTML
1, 序号, 姓名, 职称, 性别, 所在单位（学院、系）, 电子邮箱 ... 15, 14, 胡煜成, 研究生, 男, 北京大学科学与工程计算系, huyc@pku.edu.cn ...
sub.gznu.edu.cn/jssx/Down/2009726153948838.xls

Figure 1

我们将获取的二百多个邮件地址以密送的方式群发，接下来就是守株待兔☺

在不到一个小时内，我们即收到了第一份问卷反馈。

信息显示，该用户通过 126 邮箱服务器链接登陆抽查页面的，IP 显示为 XXXX。我们在通讯录内查找，女性，126 邮箱及所在院校位于 XX，最后锁定目标为：张 XX，XX 大学理学院 XX 系，Email:XXXXXX@126.com。Google 到她为 08 年春季入学博士，这与她所填写写的年龄信息（XX 年）大致相符，因此，我们认定目标真实身份已得到确认。而从她回答问卷的时间看（266 秒，而我们自己随意点击填写，用时大概在 80~100 之间），应该比较认真，可信度较高。

从她填写的问卷信息中，我们得到如下所需信息（经过匿名化处理）：

张 XX，女，XX 大学理学院 XX 系 08 年春季入学博士
公历生日：19XX 年 X 月 XX 日， 星期五， 双子座
农历：X 年 X 月 XX 日
八字：癸亥 戊午 己巳 癸酉(大致 19 时出生）

通过对第一份问卷的实际利用，我们发现，如果用户复制链接进入调查页面，我们将得不到关于邮箱的任何信息，因而难以锁定目标。为此，我们修改问卷，在最后加上选填项“若无不便，请留下您的 Email 地址，我们将在汇总调查问卷结果后，把课题分析报告发送到您的邮箱”。我们在学校 BBS 上搜索得到一份关于十一组织去东城区浏览报名的名单，又发送

了出去。目前，问卷依然开放……

攻击心得：

在互联网特别是搜索技术不断发展的今天，我们几乎无处藏身，想要完全不泄露自己的信息（邮箱地址等）是不可能的。在我们 google 目标的过程中，发现了许多可以说是悚目惊心的现象。比如，有一家医院将病人体检结果放到了网上，不但有病人姓名和出生日期，还有体检项目和相应结果，某技术学校将 06 级学生学籍信息放到网上，其中还含有身份证号的信息，我们还轻易获得了国外某大学在华招生奖学金候选人名单，信息量也相当之大。而根据本人以往经验，问卷调查之类的方式，泄露的信息量不是很大，且往往是举手之劳，有时真是很难拒绝填写，而各种公示（如评选奖学金、职称等）也往往必须给出相关人员的出生年份甚至生日等信息，而这种情况很难对信息进行保护。因此，我们要提高警惕性，不轻信各种宣传，以妨受骗上当；邮箱要有多个，分别用在不同重要性和安全性的场合，以减少被攻击的可能性和风险性。另外，对于相关组织也要有起码的责任意识，主动保护好个人的隐私，不使外人轻易得到。

上周六，在北京南锣鼓巷的喜鹊咖啡厅，我正在和几个朋友谈天说地，这时候听见了邻座的一个美女正在打电话，在向朋友抱怨自己的 Sony 笔记本如何不好用，无法使用无线链接。本着一种社会责任感和普度众妹的信念，我便开始了向美女套话并修电脑的过程：
我：你好，能让我看下这个电脑么？
美女：（费解）？
我：别担心，我是学计算机的，你的问题应该很好解决。
美女：哦，那麻烦你了，我正在准备赶制稿件。

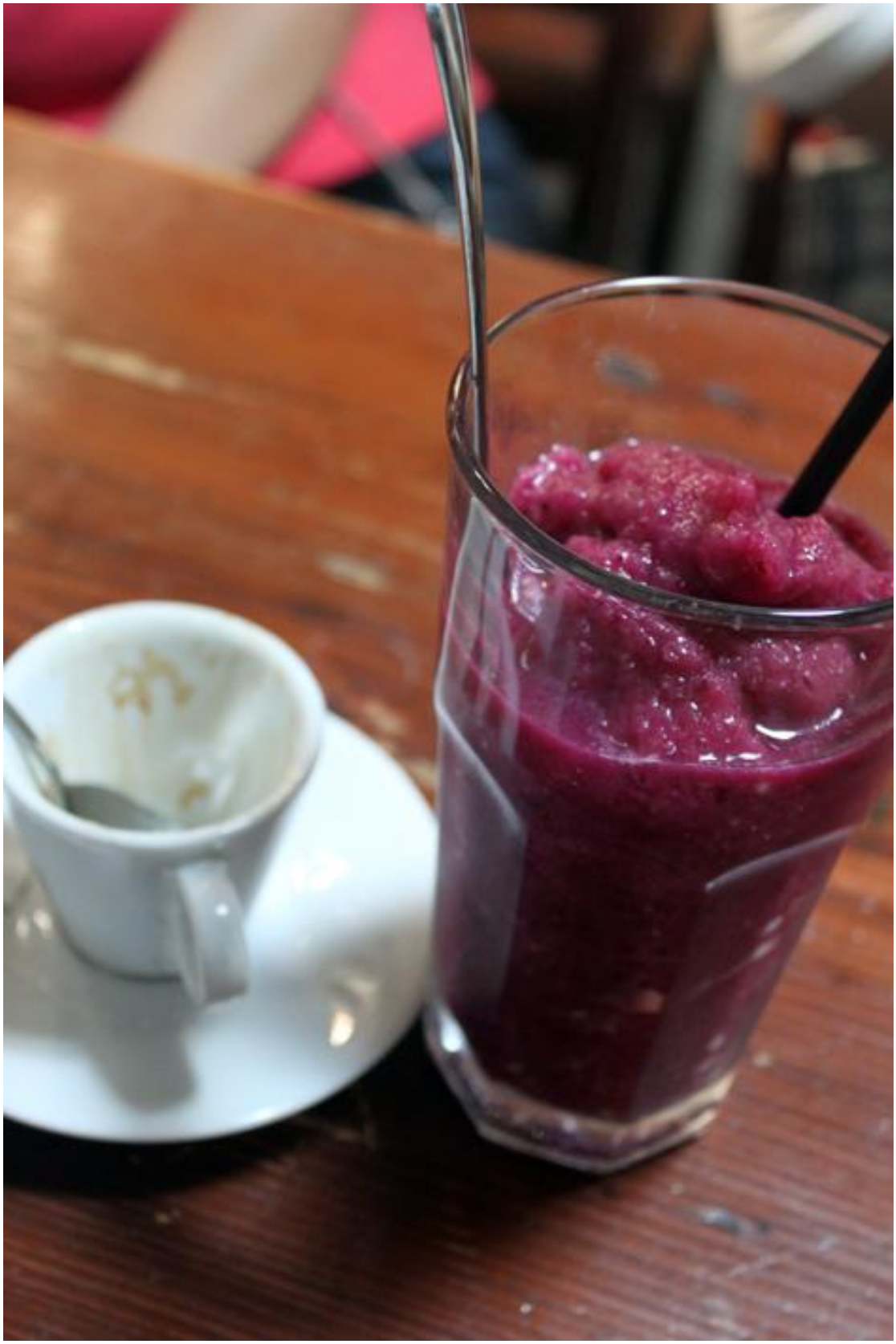
在重置无线连接后，wifi 顺利地连接上了，期间我们做了自我介绍。于是我继续追问下去。
我：你是在北京上学么？
美女：不是，我是天津的，来这里要做一个采访。
我：咦？你电脑桌面是你自己么？
美女：不是啊，这个是陈绮贞，一个歌手。
我：哇！你也喜欢陈绮贞啊！我也超喜欢的，不过你长得和陈老师真像！
美女：哪有啊，陈老师也不戴眼镜。
我：那，你有兴趣加入我们北京大学的歌友会么？如果有新的歌友会或者演唱会，我会帮你留张票的。
美女：好呀。
谈天后我顺势说道，如果有时间的话，请允许我帮你调试下电脑，在开放系统中，如果不加密码的话，电脑会有风险。这样说的原因是坚信一般女生如果有电脑密码都会是自己生日或者男朋友生日之类，进而就可以转移到生日话题上。比较幸运的是，她电脑有密码，而且是自己生日。不过最幸运的是下面的事情：
我：哦？原来你是 4 月 19 日生的啊，我是 9 月 14 日的！
美女：是嘛！太巧了~
我：我是凌晨 2 点多生的，莫非你是下午 2 点多的么？？
美女：不是啦，我记得我是早上 7 点多生的，所以我又叫 77~
我：哇，超卡哇伊的名字啊~。。。
期间省略了一些有关隐私的对话。通过生日以及出生时间的信息，可以得出：星座：白羊座；属相：马。她的我从网上查到了她的生辰八字：

生日(公历)：	1990年	4月	19日	7时0分
生日(农历)：	庚午年	三月	廿四	辰时
八　　字：	庚午	庚辰	甲寅	戊辰
五　　行：	金火	金土	木木	土土
纳　　音：	路旁土	白腊金	大溪水	大林木

总述：八字偏弱，八字喜「水」，起名（上美名腾用八字喜用神起名吧）最好用五行属性为「水」的字。分析如下：

五行分析：此命五行**土**旺；五行缺**水**；日主天干为**木**　（同类为：木水；异类为：火金土。五行统计：2木，1火，3土，2金，0水）
用神分析：〖同类得分〗：木2.53，水0.42，共计2.95分；〖异类得分〗：火1.38，金2.20，土2.20，共计5.78分；〖差〗：-2.83分；〖综合旺衰得分〗：-2.83分，「**八字偏弱**」；〖八字喜用神〗：八字偏弱，八字喜「**水**」，「**水**」就是此命的「喜神」。

作为证据，插张图：

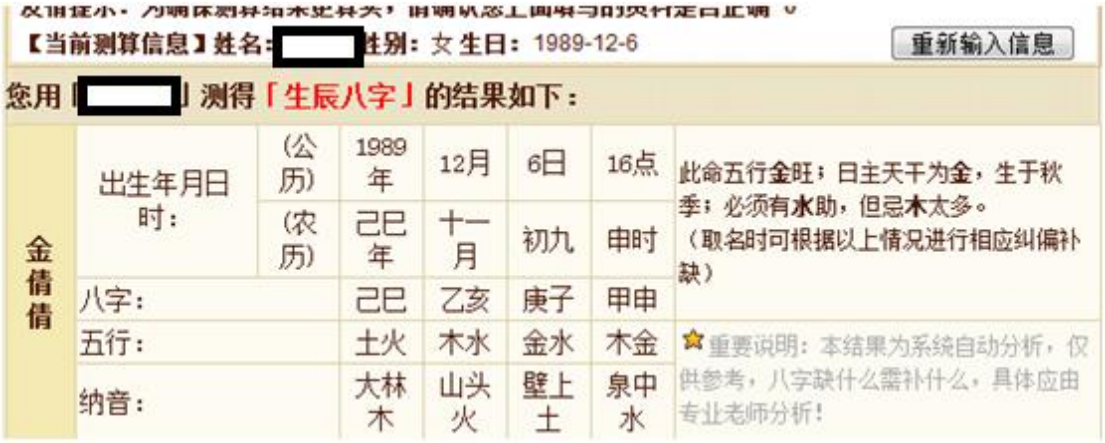


通过社会工程学手段尝试获取异性同学的 a)生肖 b)星座 c)出生日期 d）生辰八字(bonus)，并详述你的社会工程学攻击过程，包括成功的和失败的。

首先，要获取以上信息，生肖和星座都可以通过出生日期来获取得到，比较麻烦的是生辰八字，通过 Google 如果计算生辰八字（见附表），可以通过出生日期和具体的出生时间可以通过万年历和生辰八字对应表得到，所以关键是要获取异性同学的出生日期和出生当天时间。

因为对方是异性，女生都比较喜欢星座命理之类的东西，利用大学生之间常用的人人网帖子为突破口进而询问对方是什么星座，通过询问得到对方是射手座，射手座是 12 月份，继续询问你的生日不远了啊，是多少号啊，得到对方的回答，这样生肖、星座、出生日期就都得到了，最后关键问时间，我一直在问，对方以为我要帮她算命理，我说几点生的呢?对方还蒙在鼓里，说“这么严格啊，等我问问妈妈吧”，从对方父母突破就这样轻易实现了，过了几分钟之后，对方告诉我是下午 4:30，这样所有信息就全部得到了。

通过 http://51.aqioo.com/ShengChenBaZi.html 网站的信息，可以通过输入出生日期和出生时间直接得到生辰八字，省去了个人计算的时间。如下图



【当前测算信息】姓名:[redacted] 性别: 女 生日: 1989-12-6 重新输入信息

您用[redacted]测得「生辰八字」的结果如下：

金倩倩	出生年月日时：	(公历)	1989年	12月	6日	16点	此命五行金旺；日主天干为金，生于秋季；必须有水助，但忌木太多。（取名时可根据以上情况进行相应纠偏补缺）
		(农历)	己巳年	十一月	初九	申时	
	八字：		己巳	乙亥	庚子	甲申	
	五行：		土火	木水	金水	木金	☆重要说明：本结果为系统自动分析，仅供参考，八字缺什么需补什么，具体应由专业老师分析！
	纳音：		大林木	山头火	壁上土	泉中水	

作为该同学的配合，将该网站附上的命理发给她，让她开心一下！如下图：

说明：以下结果为概论性分析，比较片面，仅供参考，使用错误后果自负！八字补救需要根据命局综合分析，具体请向专业老师咨询！

五行生克制化宜忌	金旺得火，方成器皿. 金能生水，水多金沉；强金得水，方挫其锋. 金能克木，木多金缺；木弱逢金，必为砍折. 金赖土生，土多金埋；土能生金，金多土变.
五行之性	金主义，其性刚，其情烈，其味辣，其色白. 金盛之人骨肉相称，面方白净，眉高眼深，体健神清. 为人刚毅果断，疏财仗义，深知廉耻. 太过则有勇无谋，贪欲不仁. 不及则身材瘦小，为人刻薄内毒，喜淫好杀，吝啬贪婪.
四柱五行生克中对应需补的脏腑和部位	肺与大肠互为脏腑表里，又属气管及整个呼吸系统．过旺或过衰，较宜患大肠，肺，脐，咳痰，肝，皮肤，痔疮，鼻气管等方面的疾病.
宜从事的行业与方位	宜金者，喜西方．可从事精纤材或金属工具材料，坚硬，决断，武术，鉴定，总管，汽车，交通，金融，工程，种子，开矿，民意代表，伐木，机械等方面的经营和工作.

三命通会	庚日甲申时生，是日禄居时。庚金在申上见禄，以甲木为偏财。如果柱中不通丙火，无巳寅刑冲，命主贵中有平常。岁运相同。 庚子日甲申时生，时犯日禄，见财星，命柱中无巳寅丙，命主富贵双全。逢辰戌丑未，土能生金，吉利。碰上寅午戌，是平常的命。逢申酉，行火运，命主贵显。逢寅亥，官至三四品，显贵。逢卯，刑伤。逢子，多凶。 庚寅日甲申时生，逢寅亥月，命主官至三品。 庚辰日甲申时生，是魁罡照临，时支逢申，又是归禄，都不喜欢见财官，命柱中无寅午戌丙丁字，命主贵显。 庚午日甲申时生，贵显。如果通身旺月，八字中无丙巳寅午丁字，便是伤破，命主贵显。 庚申日甲申时生，贵显。八字中无卯午未戌丙丁字，贵显。逢子丑月生，行金水运，文贵。其他见庚申甲申是专禄归禄。坚金如果没有火便不能锻炼，所以巳午戌月生，大都显贵。看归禄有七种方法，不要厌烦。生于财月的，最吉利。 庚戌日甲申时生，逢寅巳午戌月生，妻子贤惠，儿子孝顺，贵显。《神白经》说：金水带印，命主有清闲之福。

月日时命理	十一月生：	此月生人，前年二月受胎，大雪节后出生。 伶俐却性急，近贵却多计较，易招障害。 务得人和，作事努力，名位自得。 初限难为，中年灾涉色情，晚运大好，享子孙福。 诗曰：自觉早年成立家，生平衣禄有荣华，亲戚兄弟全无靠，交接好友胜其他。
	初九日生：	此日生人，身体健全，性格清朗，受人敬受，须事事勉励，勤俭行善，德被乡党，中年平顺，晚景千钟，福分无量，名利长存，慈悲富贵之命。
	申时生：	（下午三点起下午五点止为猴时辰） 败来败去，难守祖业，父母无靠，夫妻和谐，女人破婚，宜养操忌木类。 凶年：十九岁、廿二岁、廿八岁、卅岁、四十二岁、五十四岁、七十二岁寿终。 申时头生：时头生人父母全，为人聪明近贵人，能文能武志气大，六亲有禄进田园。 申时中生，时中生人先克父，六亲不和兄弟疏，一忧一喜离祖吉，早妻刑克总多劳。 申时末生：时末生人先克母，六亲兄弟多冷淡，早辛苦身多病，三十岁平四十益。

附录 1 是进行社交工程获取信息的过程，附录 2 是生辰八字原理。

附录 1：社交工程聊天过程

（XX 是我，XXX 是询问对象，为了便于亲近和交流，用了大家都很熟悉的日语）

XX　20:02:01
金ちゃん　今何をするの？
XXX　20:02:28
ゴールドをみてるよ～
XXX　20:02:50
あなたは？
XX　20:05:37
野ブタをプロデュースをみてるよ
XX　20:06:11
9.12 综合★★★★爱情★★★★工作★★★★健康 78%颜色绿色数字 8 今天家人将是你最好的安慰，重视与家人相处的时光吧。烦恼不妨说给他们听听，都有舒畅心情的作用。而与家人一起时不论是散步或购物，边走边谈心、边看看物品就是个好休闲了。
http://photo.renren.com/photo/249400243/album-384294509?ref=share1#thumb
XX　20:06:17
你是什么星座？
XXX　20:06:38

射手~
XX　20:06:47
射手？你是几号生日啊
XXX　20:06:50
找个年长的人多交流~哈哈
XX　20:06:55
晕
XXX　20:06:54
1989年12月6号
XX　20:07:09
我是你おじいさん？
XXX　20:07:25
おじいさんかな～
XXX　20:07:30

XX　20:07:51
你是几点出生的?
XXX　20:08:00
分数が高いね
XXX　20:08:31
？これは～１２～２：００（PM)かな～～
XX　20:08:45
r　u　sure?
XXX　20:09:04
いいえ
XX　20:09:13
12:00-1：00　or　1:00-2:00
XXX　20:09:37
 ちょっとまって～
XX　20:09:54
おお
XXX　20:12:44
要求が厳しいね～
XX　20:12:54
はいはい
XXX　20:13:03
いや～～
XX　20:13:36
確認でください
XXX　20:13:50
はい～母に聞いてる～
XX　20:13:59

はいはい
XX　20:14:02
うれしい
XXX　20:14:15
ごご四時半
XX　20:14:46
おれと相似だ
XX　20:14:52
はは
XXX　20:14:55

XX　20:14:57
ありがとう
XXX 20:15:15
本とに？
XXX 20:15:32
ただ時間ですか？
XXX 20:15:42
あるいは、その結果？
XX 20:15:45
おれは宿題をしてる
XXX 20:16:00
何の宿題？
XX 20:16:08
ひみつ
XX 20:16:13
はは

附录 2：生辰八字计算

中国古历分天干和地支，这个相信大家都知道吧.简称干支，十天干是甲乙丙丁戊(wù)己庚辛壬(rén)癸(guǐ)，十二地支是子丑寅(yín)卯)辰巳(sì)午未申酉(yǒu)戌(xū)亥(hài).

而具体的方法如下:

将你的生日(阳历)首先确定，最好也知道出生的时间，然后在万年历上查处所对应的干支名称(如果没有万年历 可以在这个网站查到 http://site.baidu.com/list/wannianli.htm)

如:1986 年 6 月 12 日 上午 10:30 出生 查到为丙寅年农历五月初六，星期几不重要可以忽略不记.而五月初六又对照得到，甲午月丁亥日.

时辰要如何查呢?古时候一天是分为十二个时辰的，两个小时为一个时辰，11:00-1:00 为子时，1:00-3:00 为丑时，以此类推，时辰名称与十二地支名称相同.10:30 为巳时三刻，可以简

记为巳时.那么就可以得出生日的八字为丙寅年甲午月丁亥日巳时

对照下表，年份为丙寅，丙为年份的天干，寅为年份的地支，而对表是只需对照天干即可，年份为丙，在丙/辛栏对应五月的为甲午，说明月份的干支为甲午.

此时，知道日为丁亥日，同法，丁为日的天干部分，对照丁/壬栏巳时，可得时辰的干支为乙巳.

以下介绍一下干支是如何推算出来的，虽然可以从万年历的网页上可以直接得知，但是究竟是如何推出来的呢?大家可以对照下表详细了解一下刚刚得出甲午 丁亥 乙巳的推算表.

由年份推月份干支对照表:

年/月干支/月 甲/己 乙/庚 丙/辛 丁/壬 戊/癸

正月寅 丙寅 戊寅 庚寅 壬寅 甲寅

二月卯 丁卯 己卯 辛卯 癸卯 乙卯

三月辰 戊辰 庚辰 壬辰 甲辰 丙辰

四月巳 己巳 辛巳 癸巳 乙巳 丁巳

五月午 庚午 壬午 甲午 丙午 戊午

六月未 辛未 癸未 乙未 丁未 己未

七月申 壬申 甲申 丙申 戊申 庚申

八月酉 癸酉 乙酉 丁酉 己酉 辛酉

九月戌 甲戌 丙戌 戊戌 庚戌 壬戌

十月亥 乙亥 丁亥 己亥 辛亥 癸亥

十一月子 丙子 戊子 庚子 壬子 甲子

十二月丑 丁丑 己丑 辛丑 癸丑 乙丑

由日天干推时辰干支对照表:

日天干/时干支/时地支 甲/己 乙/庚 丙/辛 丁/壬 戊/癸

子时 甲子 丙子 戊子 庚子 壬子

丑时 乙丑 丁丑 己丑 辛丑 癸丑

寅时 丙寅 戊寅 庚寅 壬寅 甲寅

卯时 丁卯 己卯 辛卯 癸卯 乙卯

辰时 戊庚 庚辰 壬辰 甲辰 丙辰

巳时 己巳 辛巳 癸巳 乙巳 丁巳

午时 庚午 壬午 甲午 丙午 戊午

未时 辛未 癸未 乙未 丁未 己未

申时 壬申 甲申 丙申 戊申 庚申

酉时 癸酉 乙酉 丁酉 己酉 辛酉

戌时 甲戌 丙戌 戊戌 庚戌 壬戌

亥时 乙亥 丁亥 己亥 辛亥 癸亥

如何根据出生年份并对照下方的口诀推出自己的五行命理:

1986 年为丙寅年 则为炉中火命 此亦为年柱

5 月为甲午月 则为沙中金 此亦为月柱

6 日为丁亥日 则为屋上土 此亦为日柱

10:30 为乙巳时 则为复灯火 此亦为时柱 即得出四柱

如上之命，五行缺水木，少金，虽有火但无法克金亦无法生土，只能点灯，所以此命五行之三还算平稳，不生不克，只是财运稍嫌不足，且五行有所缺，需用名字或其他方式加以补救.

推算命理口诀:

甲子乙丑海中金 丙寅丁卯炉中火 戊辰己巳大林木 庚午辛未路旁土 壬申癸酉剑锋金

甲戌乙亥山头火 丙子丁丑涧下水 戊寅己卯城头土 庚辰辛巳白蜡金 壬午癸未杨柳木

甲申乙酉泉中水 丙戌丁亥屋上土 戊子己丑霹雳火 庚寅辛卯松柏木 壬辰癸巳长流水

甲午乙未沙中金 丙申丁酉山下火 戊戌己亥平地木 庚子辛丑壁上土 壬寅癸卯金箔金

甲辰乙巳复灯火 丙午丁未天河水 戊申己酉大驿土 庚戌辛亥钗钏金 壬子癸丑桑拓木

甲寅乙卯大溪水 丙辰丁巳沙中土 戊午己未天上火 庚申辛酉石榴木 壬戌癸亥大海水

最后呢，再给大家小小的总结一下都有什么命~!

同是金，有海中金、剑锋金、白蜡金、沙中金、金箔金、钗钏金

同是木，有大林木、杨柳木、松柏木、平地木、桑拓木、石榴木

同是水，有涧下水、泉中水、长流水、天河水、大溪水、大海水

同是火，有炉中火、山头火、霹雳火、山下火、复灯火、天上火

同是土，有路旁土、城头土、屋上土、壁上土、大驿土、沙中土

攻击目标：获取异性同学的生肖、星座、出生日期、生辰八字。

攻击对象选择：选取一个仅仅认识但不熟知的异性同学。知道其手机号码。

所知信息：知道该同学为经济学院某班班长，前不久过了生日(具体时间未知)。

攻击思想：伪装成一个她所信任的对象，可以方便的获取信息。

生肖，星座，出生日期：我们仅仅只需要从她的出生年月日轻松获得。

生辰八字：我们可以从她的出生时间得知。

攻击过程设计：首先伪装成一个经济学院学工组的学生助理(“XX”)，我需要统计学院各班班长的学生信息，我是通过你们辅导员得到你的手机号码。下面，请你说一下你的一些个人信息：籍贯，本科学校，出生日期（先问下简单的信息打消防备心理后再问出生日期），通过制造同年同月同日生的假象来使对方激动，同时可以很轻松获得她的出生时间（先说出自己是几点出生的，诱使对方容易的说出自己的出生时间）。

注：用实验室座机打。

我：您好，请问你是 xx 同学吗？
她：您好，我是。
我：我是经济学院学工组学生助理，我叫 XX。我需要统计一下学院各班班长的学生信息，我是通过辅导员得到你的手机号码的。
她：恩，好的。
我：下面请你说一下你的一些个人信息，我需要填一个表格。
她：好，您说。
我：请问你的籍贯？
她：四川 XX
我：请问你的本科学校？
她：北京 XXXX 大学
我：请问你的出生日期？
她：88 年 9 月 13 日
我：哇，太巧了，我也是，我们一天出生的，我是下午 5 点出生的，你是几点出生的哈？
她：真的吗？我凌晨出生的吧。
我：那是具体几点出生的？
她：凌晨 12 点多出生的。
我：恩，好，谢谢了
她：没有其他的了吗？
我：没有了，谢谢，再见。

通过生肖星座八字网站查询，得知她的生肖：龙，星座：处女座，出生日期：9 月 13 日，八字：（戊辰　辛酉　辛未　戊子）。