Shirley 曾爱
<改变未来的九大算法> 读书笔记

网页排名(Page Rank)
词位置把戏(Word-location trick): Page number+Position number
e.g. 查询"Twice Fancy": 一号网页为Twice1-6，Fancy2-8；二号网页为TWICE1-7，Fancy1-9
RESULT: 二号网页更符合要求
相关度(Relevance) instead of 匹配(Match)
元词把戏(Metawork trick)
超链接把戏(Hyperlink trick): 根据引用次数来决定价值
e.g. 页面1被link3次，页面2被link10次 > 页面2更有价值
权重把戏(Authority trick): 有多少人actually链接这个网页，权重值就为几
循环(Cycle): 访问者通过Hyperlink返回初始出发点
随机访问者把戏(Random Surfer Trick): 研究其因其的直观度，同时因为描述了搜索引擎计算什么，而非如何计算
权重值(Surfer Authority Score): 一随机访问着在该网页浏览的时间比例
网页质量
网络垃圾(Web Spam): e.g. 邮件中无用的信息、链接网页

一些小想法：
本书在一开头通过引用谷歌的例子来阐述了计算机的页面搜索。介绍了Page Rank的一些核心思想，如词位置把戏，元词把戏，超链接把戏，权重把戏，随机访问者把戏等。无法否定的是，这些核心思想的确对谷歌(或搜索引擎的技术)有深远的影响，但其还是建立在最基本的骨架上。
我从中获益良多——或许解决一个实际问题并不难。将一个大问题分解为多个小问题，再逐一攻破。同时思考一个完整的问题有时并不是十分高效。
Random Surfer Trick还没有太明白，待二次返回阅读。

共钥加密(Public Key Cryptography)
邮局工作人员=互联网路由器(以及潜在的窃听者)
128位加密：共享密钥的长度
38位数的共享密钥被认为非常安全。
分块密码(Block Cipher):
Step 1: 长消息被分组为固定的大小的小块。
Step 2: 每一块都会根据一系列固定规则转换数次。e.g. 规则可以为"钥匙的前半部分+消息的后半部分，倒置结果，钥匙的后半部分+消息的前半部分"（通常Block Cipher会进行大于等于10轮循环）

颜料混合把戏(Diffie-Hellman Key Exchange/Paint-mixing trick) 颜色=数字=other siganl
Step 1: 小明选择"私人颜色"，小红选择"私人颜色"
Step 2: 宣布"公开颜色"
Step 3: 制作"公开-私人混合颜色"
Step 4: 小明和小红均公开"公开-私人混合颜色"
Step 5: 小明和小红均混合另一个人的"公开-私人混合颜色"和自己的"私人颜色"
Step 6: 小明和小红得到一样的Result

混合操作=离散指数(discrete exponentiation)
分离操作=离散对数(discrete logarithm)