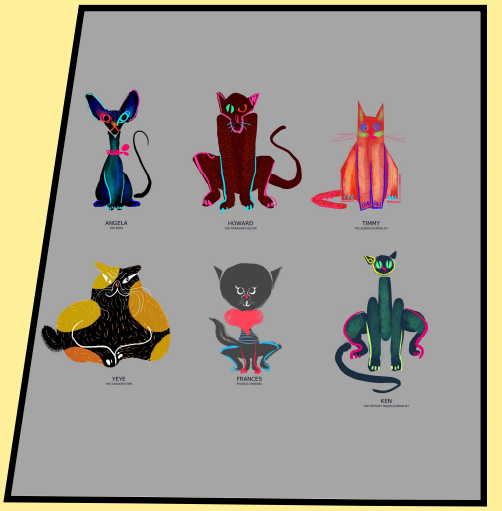
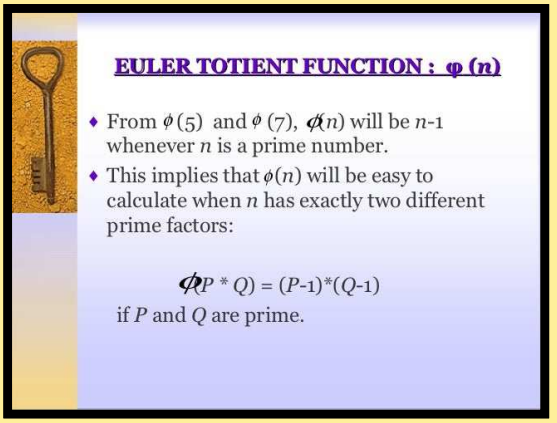
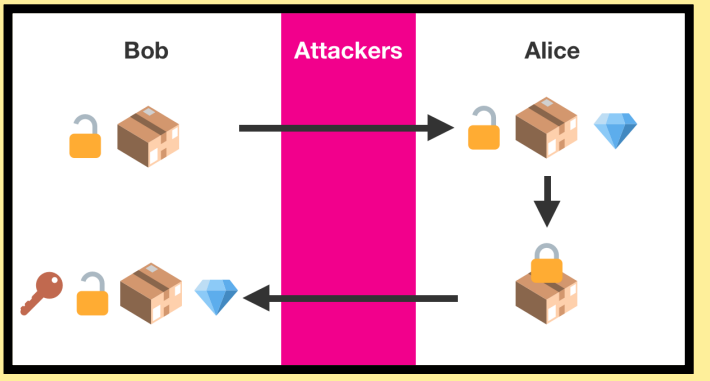

ENIGMA

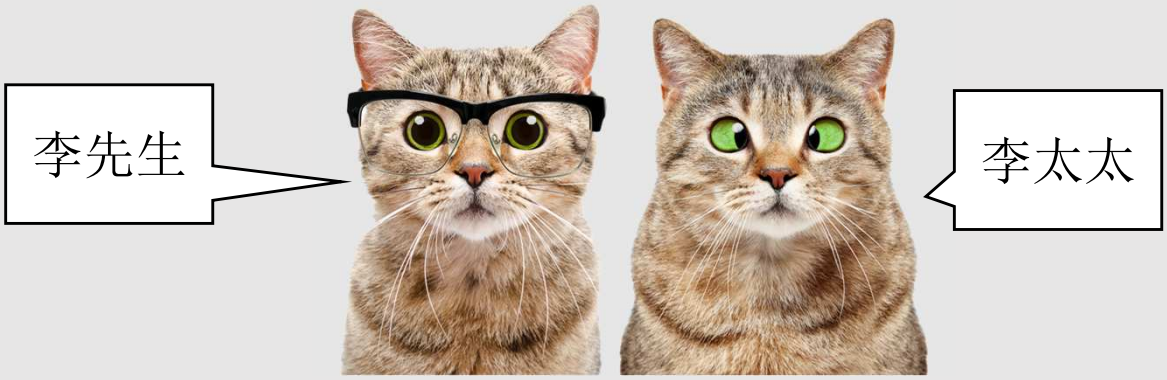

ANGELA
HOWARD
TIMMY
YEYE
FRANCES
KEN

电脑疑云

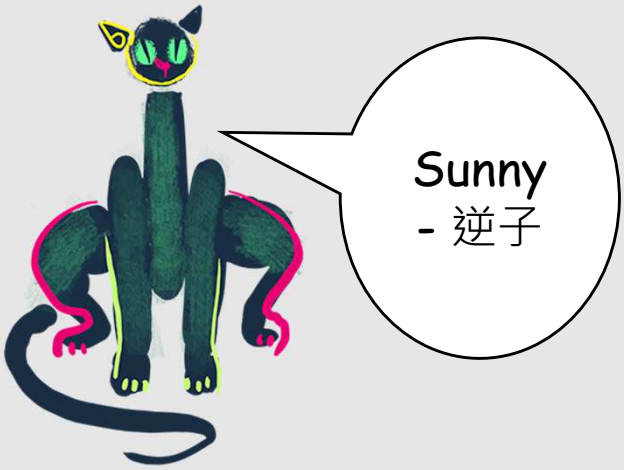

EULER TOTIENT FUNCTION : φ (n)
From φ (5) and φ (7), φ(n) will be n-1 whenever n is a prime number.
This implies that φ(n) will be easy to calculate when n has exactly two different prime factors:
φ(P * Q) = (P-1)*(Q-1)
if P and Q are prime.


Bob
Attackers
Alice

我们今次的主角



Angela：私家侦探



Joe - 孝顺子

Mary - Joe 的太太

我们今次的主角

亚麦 - 恶棍

Natalie - 投资银行电脑专家

Eva - 警方风化组探员

故事开始

已夜阑人静， Angela 三心两意，回家去翻看繁花? 约朋友去吹水? 还是留在办公室整理吓那些已有薄尘的旧档案 …在夏天，生意都比较淡薄，可能天气闷热，很多人都没有心情搅婚外情，所以少了很多这类的侦查，但这卻是她入息的主要来源，目前，只有人找她去寻找失踪的犬只或鹦鹉 。 唉，头痛!

就在她自怨自艾, 胡思乱想时，电话响起来了。是一位律师朋友找她，因为他是她大学的前辈及她姑妈的的朋友，所以她尊称他为阿叔以示尊敬。

生意好吗？我有一个非常棘手的问题。

生意认真一般，搵食艰难，有什么我可以帮到手的，可以被我每日搵番三千元，我赴汤蹈火都会去做。

三千元一日无问题，我听说及知道妳能力高及可以信赖，所以找妳帮手。

好的，有什么我可以为你分忧的?

大概一个星期前，收到一个恶意电话。当我不理会它之后，有一个恶棍在街头拦截住我並恐吓我，兇神恶煞，目露兇光，如狼似虎。

你有没有被吓倒? 有报警吗?

(一笑) 小问题哪，我们这一代都很多在贫民窟长大，恶棍、匪徒、骗子、贩毒、司空见惯，加以我们做律师的也经常受恐吓的，这不成气候的家伙吓不到我的。还不用吃惊风丸。我需要的是一个人去调查这件事，为什么有人上门找我麻烦?

他有没有透露为了什么事找你麻烦?

我是一位李先生的律师，他是一位数学家，曾在一间法国投资银行工作多年，他在三年前因为患上癌症辞世，留下他的太太及两个已长大成人的儿子，由于他知道他将离世，命不久矣，他将一些文件托付给我。

他当时已接近65岁，他的太太仍健在，但身体状况不太好。

李先生似乎相当富有。

那恶棍要我交出李先生给我的文件。

当我第一次和李先生会面时，他告诉我他在一间名叫海通银行开了一个户口，这户口会每个月转一笔丰厚的生活费给李太太，但如果她有额外需要，她可用他给予她的密码去网上提款，但每次最多只可提 $30,000 及每个月只可提两次款。

他再告诉我他在海通银行那个户口有巨大存款，足夠李太太一生无忧。他再交给我两封密封的信，他指明只在李太太去世之后才可打开。他又告诉我他另外给了他两个儿子每人一封类似的密件，並告诉他们当他们母亲去世后便拿这信去找我。

我要当着他们的面前，打开那四封密件，然后执行信件内的指示。

上面讲的那个恶棍就是要我交出李先生给我的那两封信。我当面拒绝了，並惊告他如果他再骚扰我，我就报警及将他绳之以法。

为了安全起见，我已将李先生那两封信放在律师楼的保险箱内。

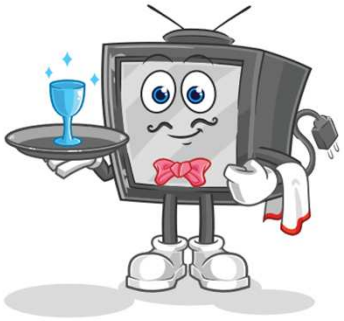
那恶棍怎样联络你?

他是用他的流动电话，这就是他的号码 180 **** ****

请你描述他的长相。

再请你给我李太太及她两个儿子的联络方法及请通告他们我会缺期内联络他们。

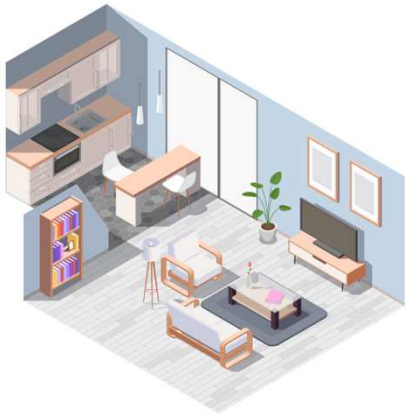
OK, 阿叔，给我两个星期时间，我会将这件事尽快调查清楚及向你回报。



Angela 看到时候不早及明天有大量工作要安排，于是回家食即食面，並一路食一路看港剧法网狙击，看来楊怡的案件比她的有趣得多。

但最少今个月的租金及生活费不用再傷头脑!

第二天早上，她联络了李太太及约好了在李太太的家里见面。



在那里，她见了李太太及她的媳妇 Mary，后者是李太太的长子阿 Joe 的太太。

李太太对客厅的电视节目比 Angela 更有兴趣，幸而 Mary 在场及可解答大部分问题。Mary 指出她岳母有点痴呆，所以她经常来这里帮手打点一切，尤其是当李太太要网上提款。

?? “李先生不是每个月都给李太太一笔很丰厚的生活费。她看来对人生无求，为什么她仍要去网上提款?”

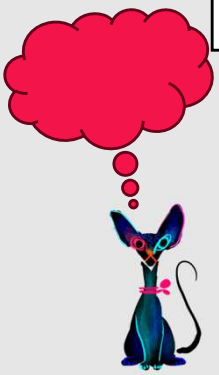
在李太太全神贯住在电视剧的宝总身上时，Mary 静悄悄地告诉 Angela 李太太的另外一个儿子 Sunny 经常向她妈妈索取金钱，李太太不但给了 Sunny 她每月生活费的一大部份，並且不厌其烦地去网上提款接济 Sunny 。

为什么 Sunny 要向她妈妈需索金钱呢?

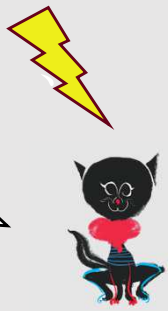
他误交损友，他欠下赌债屡屡，他间中亦有向我丈夫借钱。我已跟他断绝来往。

为什么妳岳母需要妳帮忙去网上提款?

我岳母本博学多才，但随着年龄增长，渐变痴呆，她本来有足够能力去使用那边的电脑，但她搅不清楚我岳丈给她的密码。



密码不会很复杂吧?

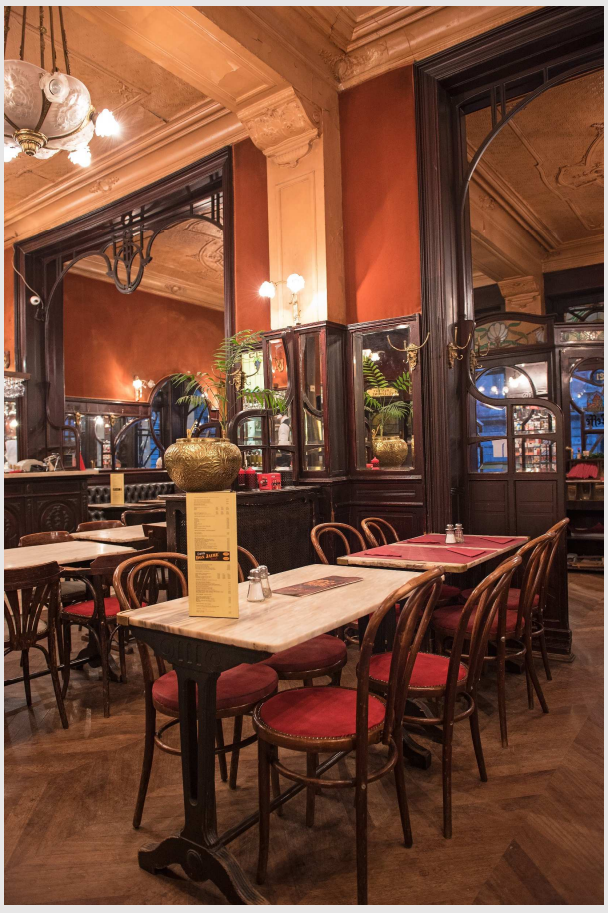


通常是的。但我岳丈的密码是超过 60个数目字，这是写在这本记事本内，每次我输入这密码，我都要做几次，或停一停又再继续，我只记得开头那7个字 5263814 及最尾的 6个字，其它我都是每 6个字停一停再继续，所以我每次都需要她的记事本。

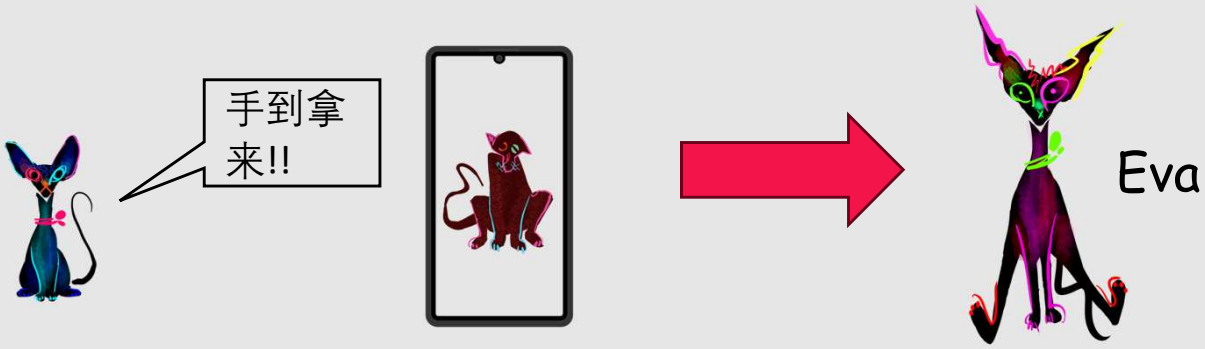
哦？为什么李先生要这样无中生有，自寻烦恼？我可否和你丈夫 Joe见面及问他一些问题？

Angela 去了 Joe 的写字楼和他会面。他是一位建筑师及和他母亲一样，很有教养。但当谈及 Sunny, 他则左右言其它，没有透露太多。他指在这时候，Angela 可能在一间名叫落日大道的酒吧找到 Sunny。

落日大道酒吧离 Joe 的办公室不远，Angela 决定安步当车。由于李太太给了她一张 Sunny 的照片，她一踏进酒吧已发现阿 Sunny 在独自和他面前那杯酒倾谈。为了不暴露她自己，她选择一个角落位置以观察及了解 Sunny多一点，她也叫了一杯流血的玛利。当她坐了半小时尚未决定如何接近 Sunny，有一名大漢从内面走去 Sunny 身旁，拍了一下 Sunny 的膊头，然后坐落在他旁边，用很低的声音和 Sunny 交谈。这个人很像阿叔形客的那个坏蛋的长相，她静静拿出她的手机，面向垟，然后拨打阿叔给她的那个恶霸的电话号码，Sunny 旁边那个人的电话响起来。



原来正是你!



用她手机，她偷拍了几张 Sunny 和 恶棍的照片。

由于还是上班时段，她打电话给她在警隊风化组工作的妹妹 Eva。

“我现在转给妳几张相片，请妳看看你们有没有他们的犯罪纪录?”

20分钟之内，Eva 回复说没有 Sunny 的犯罪纪录，他旁边的人卻臭名昭著，曾多次被控勒索，更罪成入獄多次，他名叫麦坚。

Anglea 未饮完她的流血玛利便匆匆趕回她的侦探社。

她今日查到及听到很多有关这件案的资料，是时候将它们连贯起来:

1. Sunny 和麦坚是认识的，一丘之貉?
2. 是那一个人利用另外一个人?
3. Mary 说 Sunny 债台高築。麦坚是他的债主？由于受到他的威胁和恐吓，所以要多次向他母亲需索金钱?
4. 为什么麦坚要阿叔交出李先生付托给他的文件？这些文件一定与钱财有关!
5. 有没有可能 Sunny 为了挡住他的骚扰及拖延麦坚，将他父亲给他的信给了麦坚看导致麦坚要脅阿叔交出他手上的文件?
6. 看来，关键在这些文件内…

或者 Joe 会知道多一些关于这些文件，当她正想拿起电话时， Mary 来电了 …

今日见完妳之后，为了协助妳的调查，Joe 想告诉妳他被 Sunny 软硬兼施之下已将他爸爸留给他的信给了 Sunny，由于他並没有将信拆封，他並不知道信件的内容。

???

又是一条线索…

显而易见，整件事都是围绕着这几份文件，因此阿麦一定要阿叔交出他手上的文件，因为知道内里的内容便可能知道当李太太逝世之后，Sunny 可以收到多少遗产??

她约定 Eva 一同去落日大路酒吧收风。

想不到，Sunny 仍在酒吧内及仍然清醒人事，麦坚卻不在现场，当 Angela 自我介绍之后，Sunny 不愿意回答她的问题。直至 Angela 说会亲自将李太太带到酒吧，Sunny 才尽吐真言。

我到今时今日，仍然是一头雾水，稀里糊涂，对的，我是想分到我爸爸的遗产以偿还欠阿麦的赌债，我已将被他迫死了。

但当我拆开阿Joe 及我的信，内只有 20个数目字，我的是 45278 … 8970，记得不太清楚了。阿 Joe 的是 2541208 ??? 33312。

摸不到头脑?

Angela 和她妹妹也莫名其妙，百思不得其解。

当她们离开酒吧，看到 Sunny 抬起头，神情沮丧地看着酒吧顶的吊扇。

Angela 回到侦探社，是时候分析这两天的调查结果:

1. 阿叔有两封信，一封肯定是李先生的指引及最后的安排。
2. 由于这些信只可在李太太去世之后才打开，最大可能是遗产的分配。
3. 这样另外一封信是什么内容呢?
4. 会否和 Joe 和 Sunny 的信一样有一大串数目字呢?
5. 这三组数目字有什么关系呢?
6. 这三组数目字又有什么用呢?
7. Mary 不是说她岳母的银行密码也是一大串数目字吗?
8. 不是三组，是四组数目字。
9. 不成，我要些新鲜空气才可再继续 …

新鲜空气真是有帮助，头脑又清醒起来，李先生是数学家，所以一定整日和数目字打滚…

所以或者应该向他工作方面着手，李太太或者可以提供某些资料帮到手。

太晚了，明天才找她吧!

李太太，你先生在法国投资银行是负责那一方面的工作?

他从来没跟我谈及他的日常职务，只知道他的工作是与电脑有关的。

我相信你的儿子 Sunny 惹上麻烦，身处水深火热的境界，我或者可以帮你们忙，为他解困。有没有人在法国投资银行可以解答到我一些疑问?

我先生在银行内很受人推崇备至，好象很多在 IT 部门的年轻人都是他培训出来的。特别有一位名叫 Natalie 的，仍然常打电话给我向我请安，这是她的内线电话，我相信她会愿意協助妳的，让我首先打电话给她待她有心理准备。

午后，Angela 打电话给 Natalie，Natalie 表现得很热心，尤其是有关李先生的事情。

<=======

=======>

李先生在生时是银行的首席密码学家。

什么是密码学? 他是负责什么的? 相信李太太已告诉妳我是一名私家侦探，一位律师雇佣我来调查为什么会有人有兴趣夺取李先生付讬给他的文件。初步调查有坏人会用不法手段及可能会危害李先生的家人。所以我要将这件事弄个水落石出，一清二楚?

我相信我们面对面谈会比较在电话清晰很多，妳可以来我办公室共进咖啡吗?

就象很多 IT 的专业人仕，Natalie 肤色极其白皙。，显然很少在办公室外逗留长时间。

密码学家主要工作是设计密码及译解密码。看妳的表情，看来我是偷步了，让我从密码解释一次。

"如果有一天，我忍不住在工作时间想写一个电郵给我的情人占士告诉我很爱他, I LOVE U 由于写字楼品流复杂，如果这讯息被外人见到，对我和他都有不便，但如果我和他有一个约定好的密码，我将我的讯息以密码写成，然后发给他，他收到之后，只要用预先安排的情序来解码便知道我想告诉他我爱他。"

一个最简单的密码名叫凯撒密码，盛传是古罗马的凯撒大帝设计的，方法是将每个字母向前或向后移动，例如我将 ILOVEU 向后移两个位便得出 KNQXGW，只要占士将 KNQXGW向前移动两个位便得出 ILOVEU。

I	L	O	V	E	U
K	N	Q	X	G	W

在这情况下，我是密码师，占士是解码师，清楚吗?

当然，亦有其它方法传递讯息，例如中国在万里长城的烽火台，当有外族侵略，守军便点起煙火以通知远方的友军有敌入侵。北美洲的印弟安人亦用同一种方法沟通。

传递密码的方法与时共进，最闻名及影响深远的是第二次世界大战德国的 Enigma 密码机 (图片可参阅本文第一页)，联盟国共用了 10,000人 + AI 之父 Alan Turing + 世界上第一部电脑 + 一点运气才可译解了 Enigma 密码机。据说因此将二次大战缩短了两年之多。

但上述的所有系统都需要发出者和接收者都知道密码使用的细节。

如果两个陌生人想交换保密资料，他们都不认识对方，亦因此没有理由信任对方，他们应该怎样做呢?

哦，怎样做?可以举个例吗?

1. 例如妳日常用的微信，为什么妳会相信腾讯不阅读妳的讯息，因为腾讯承诺用一个密码将妳的讯息加密，这样只有妳的联系人会再经过腾讯解码之后看到妳的讯息内容。由于腾讯是一可信赖的机构及是一间高科技公司，所以妳相信一个不相识的第三者将妳的讯息付讬给它。这就是密码学其中一个功能。

2. 例如妳在我们的银行存款，妳给我们一个户口密码，例如 aNgela150267%, 我们用高深数学将这密码转为一个单向函数，盗用者就算知道这函数，也很难破解到妳的户口密码。因此当妳忘记了妳的户口密码时，我们会要求妳重新输入新密码，从而我们再计算出一个新函数。李先生就是负责这部分的工作。

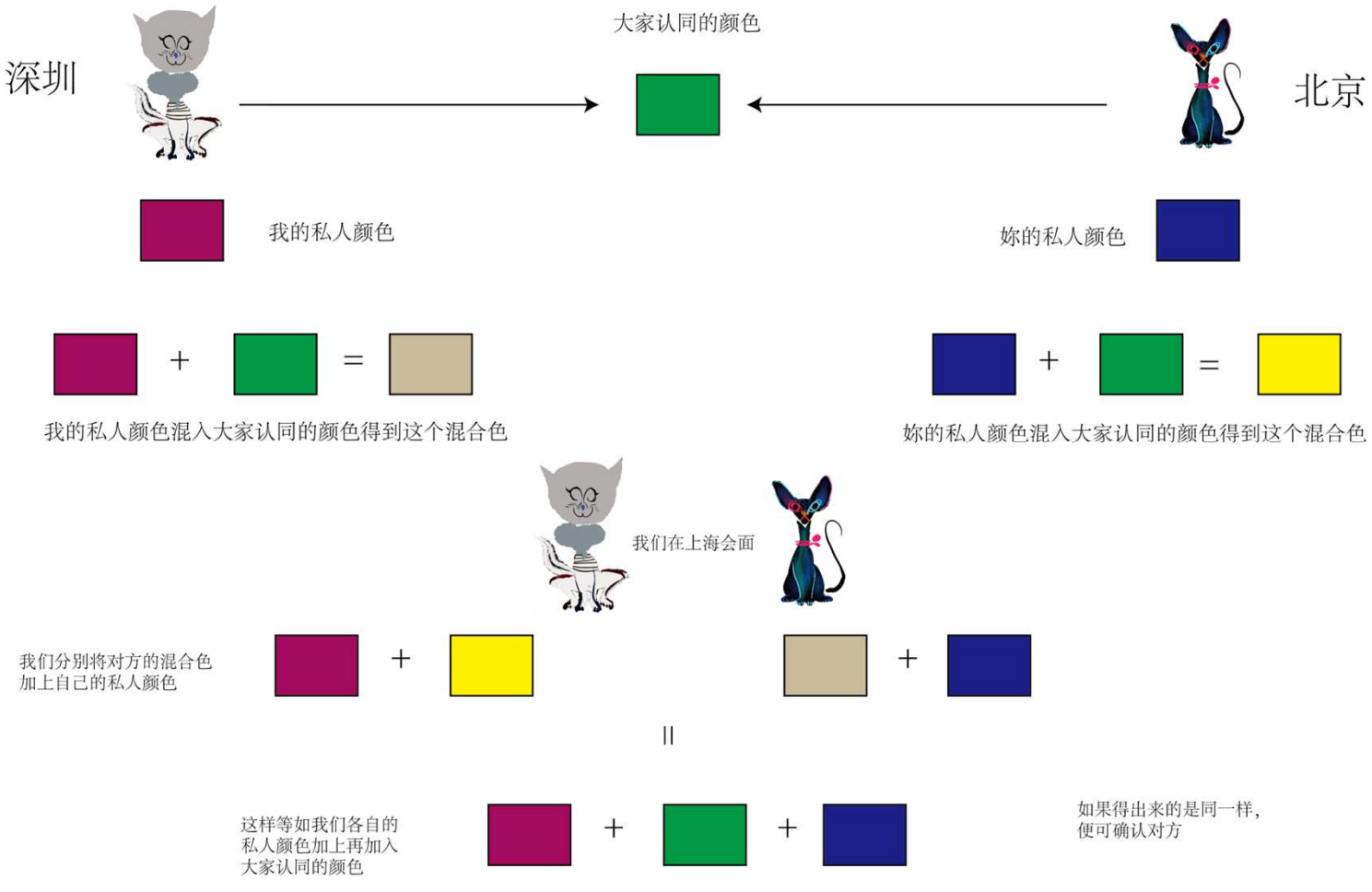
哗，可以简化一点吗?

在单向函数的应用，我可以再给妳两个例子，第一个是书本式，第二个是我们银行实际应用的。

第一例: 妳和我身处两地，水隔一方，从未谋面，亦没有理由相信对方，我们决定在上海会面交换一些东西。我们用以下图来表达。

我们无法从对方拿到的混合色知道对方的私人颜色，这等于不知道对方的密码。

但如果双方各自将对方的混合色加上自己的颜色而得到同一样颜色，我们可以肯定双方是共用一个共同认同的颜色，即等如一个共同的密码。换句话说，对方就是我们认定要见的人。



深圳

大家认同的颜色

北京

我的私人颜色

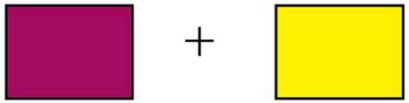
妳的私人颜色

我的私人颜色混入大家认同的颜色得到这个混合色

妳的私人颜色混入大家认同的颜色得到这个混合色

我们在上海会面

我们分别将对方的混合色
加上自己的私人颜色



=

这样等如我们各自的
私人颜色加上再加入
大家认同的颜色

如果得出来的是同一样，
便可确认对方

2. 第二个例就是李先生的日常工作。

a. 360 我们知道是可以由 2 x 180 或 8 x 40 或 4 x 80 等到。有很多可能性。

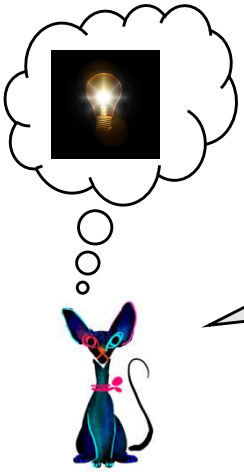
b. 但 323 是一个质数，只可以由 19 x 17 等到，没有其他可能性。19 和 17 也各是质数。要找出 323 的乘数很费功夫。

c. 试想像质数不是 323，是一个 60个位的质数，妳需要一个超级电脑及很长时间才可出找它的那两个独一无二的两个乘数。

d. 所以妳用两个分别冗长的质数乘起来得出的质数是非常难破解。

e. 这就是单向函数可以充份应用于繁琐的密码学的原团。

f. 如果两个人或三个人分别持有一个冗长的质数，如果这二个或三个质数乘出来的质数用以作密码，这密码几乎是牢不可破。



Natalie, 衷心感谢妳，妳令我茅塞顿开，我想我找到帮助李先生家人的方法。

可以去向阿叔领功了及收钱了。

我想我把握了整件事的真相。

李先生知道自已时日无多，所以作出以下的安排。

1. 他将他的财富放入海通银行。
2. 他计算出三个冗长的质数，对他来说，这是轻而易举。
3. 这三个质数分别放在三个密封信内，交给你, Joe 和 Sunny。
4. 这三个质数乘起来就是在李太太记事本上的密码。 有了这密码，向银行提取遗产较容易。
5. 当李太太去世之后，给你的另外一封信会讨细写明这件事及遗产如何分配。

那样为什么李先生限定李太太除了生活费外只可以每个月用密码提两次款，每次不得超过 $30,000?

冰冻三尺，非一日之寒，可能一直 Sunny 都有操守问题，得不到他爸爸的信任。李先生可能恐怕有点痴呆的李太太应付不了，所以有些一着。

噢，这样说，可能 Sunny 和 Joe 都不知道有这本密码记事本。

就算Sunny 知道也没有问题，他也只可每个月提 $60,000。李太太的余生仍有足够保障!

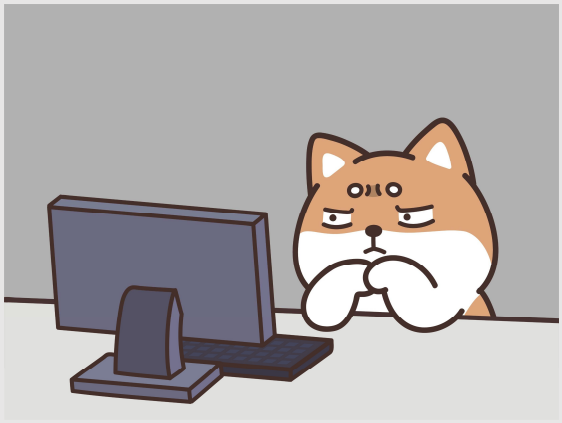
相信他给我的一封密信会有详细解释。妳做得很好，我没有误托非人。

你下一步会怎样做?

我可以将妳的调查及结论交一位相识的法官研究。虽然只是一个理论，但由于我人身安全受到威胁，我有权要求法庭对麦坚发出禁制令，及在法官和李氏兄弟面前打开所有文件以供法庭考虑。

这要视乎法庭的观点与角度。

无论如何，妳的工作已告一段落，我会跟妳保持联络及更新发展。



Angela 等了三个星期才有消息，阿叔给了她一张支票。

全件事都清楚了。我没有找法官，我直接找到李氏兄弟及在得到他们同意之后在他们面前拆开所有信件，一切都正如妳所料，在他们母亲离世后，所有遗产由他们两兄弟平分。我劝告 Sunny 知会麦坚，他将会收到大笔的遗产，要麦坚忍耐，并且如果李太太遭遇不幸，他是最大疑犯。我亦劝告 Sunny 振奋，重拾正轨，这样就不用每天心惊胆跳做人及令李太太担忧。

希望他听我说话。

整件事都总算完满结束及水落石出。

两人拥抱之后，Angela 收到一张超乎想象的大支票。

阿叔除再次多谢 Angela 之后，说会将她推荐给所有同业及朋友。

是否应该请 Eva 和 Natalie 饮番杯呢?

- The end -

Eddie Shum 13.09.2024