简单的密码教学

1、维吉尼亚密码

维吉尼亚密码引入了“密钥”的概念，即根据密钥来决定用哪一行的密表来进行替换，以此来对抗字频统计。假如以上面第一行代表明文字母，左面第一列代表密钥字母，对如下明文加密：

TO BE OR NOT TO BE THAT IS THE QUESTION

当选定 RELATIONS 作为密钥时，加密过程是：明文一个字母为 T，第一个密钥字母为 R，因此可以找到在 R 行中代替 T 的为 K，依此类推，得出对应关系如下：

密钥:RELAT IONSR ELATI ONSRE LATIO NSREL

明文:TOBEO RNOTT OBETH ATIST HEQUE STION

密文:KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

历史上以维吉尼亚密表为基础又演变出很多种加密方法，其基本元素无非是密表与密钥，并一直沿用到二战以后的初级电子密码机上。

2、凯撒密码

它是一种代换密码。据说恺撒是率先使用加密函的古代将领之一，因此这种加密方法被称为恺撒密码。

凯 撒密码作为一种最为古老的对称加密体制，在古罗马的时候都已经很流行，他的基本思想是：通过把字母移动一定的位数来实现加密和解密。明文中的所有字母都在 字母表上向后（或向前）按照一个固定数目进行偏移后被替换成

密文。例如，当偏移量是 3 的时候，所有的字母 A 将被替换成 D，B 变成 E，以此类推 X 将变成 A，Y 变成 B，Z 变成 C。由此可见，位数就是凯撒密码加密和解密的密钥。

在密码学中，恺撒密码（或称恺撒加密、恺撒变换、变换加密）是一种 最简单且最广为人知的加密技术。它是一种替换加密的技术。这个加密方法是以恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。恺撒密码通常被作为 其他更复杂的加密方法中的一个步骤，例如维吉尼亚密码。恺撒密码还在现代的 ROT13 系统中被应用。但是和所有的利用字母表进行替换的加密技术一样，恺撒 密码非常容易被破解，而且在实际应用中也无法保证通信安全。

3、栅栏加密法

栅栏加密法是一种比较简单快捷的加密方法。栅栏加密法就是把要被加密的文件按照一上一下的写法写出来，再把第二行的文字排列到第一行的后面。相应的，破译 方法就是把文字从中间分开，分成 2 行，然后插入。栅栏加密法一般配合其他方法进行加密。例：加密 information 分行 i f r a i n n o m t o 合并 ifrainnomto 完成~

4、猪圈密法 （朱高密码。共济会密码）

它的英文名是 pigpen cipher,直译过来好搞笑。 在 18 世纪时，Freemasons 为了使让其他的人看不懂他所写而发明的，猪笔密码属于替换密码流，但它不是用一个字母替代另一个字母，而是用一个符号 来代替一个字母， 把 26 个字母写进下四个表格中,然后加密时用这个字母所挨着表格的那部分来代替。

5、RSA 算法

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对密钥，使用其中一个 加密，则需要用另一个才能解密。 RSA 的算法涉及三个参数，n、e1.e2。 其中，n 是两个大质数 p、q 的积，n 的二进制表示时所占用的位数，就是所谓的密钥长度。 e1 和 e2 是一对相关的值，e1 可以任意取，但要求 e1 与(p-1)*(q-1)互质(互质：两个正整数只有公约数 1 时，他们的关系叫互质)；再选择 e2，要求(e2*e1)mod((p-1)*(q-1))=1。 (n 及 e1),(n 及 e2)就是密钥对。 RSA 加解密的算法完全相同,设 A 为明文，B 为密文，则：A=B^e1 mod n；B=A^e2 mod n；e1 和 e2 可以互换使用，即： A=B^e2 mod n；B=A^e1 mod n

6、ECC 加密法

ECC 算法也是一个能同时用于加密和数字签名的算法，也易于理解和操作。同 RSA 算法是一样是非对称密码算法使用其中一个加密，用另一个才能解密。公开密钥算法总是要基于一个数学上的难题。比如 RSA 依据的是：给定两个素数 p、q 很容易相乘得到 n，而对 n 进行因式分解却相对困难。那椭圆曲线上有什么难题呢？ 考虑如下等式 ： K=kG [其中 K,G 为 Ep(a,b)上的点，k 为小于 n(n 是点 G 的阶)的整数] 不难发现，给定 k 和 G，根据加法法则，计算 K 很容易；但给定 K 和 G，求 k 就相对困难了。 这就是椭圆曲线加密算法采用的难题。我们把点 G 称为基点(base point)，k(k<n，n 为基点 G 的阶)称为私有密钥(privte key)，K 称为公开密钥(public key)。 现在我们描述一个利用椭圆曲线进行加密通信的过程： 1、用户 A 选定一条椭圆曲线 Ep(a,b)，并取椭圆曲线上一点，作为

基点 G。

2、用户 A 选择一个私有密钥 k，并生成公开密钥 K=kG。

3、用户 A 将 Ep(a,b)和点 K，G 传给用户 B。

4、用户 B 接到信息后 ，将待传输的明文编码到 Ep(a,b)上一点 M（编码方法很多，这里不作讨论），并产生一个随机整数 r（r<n）。

5、用户 B 计算点 C1=M+rK；C2=rG。

6、用户 B 将 C1、C2 传给用户 A。

7、用户 A 接到信息后，计算 C1-kC2，结果就是点 M。因为 C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M 再对点 M 进行解码就可以得到明文。

ECC 的功能比 RSA 强。而令人感兴趣的是点和点的过程，这也是其功能之来源。

7、四方密码

四方密码用 4 个 5×5 的矩阵来加密。每个矩阵都有 25 个字母（通常会取消 Q 或将 I,J 视作同一样，或改进为 6×6 的矩阵，加入 10 个数字）。 首先选择两个英文字作密匙，例如 example 和 keyword。对于每一个密匙，将重复出现的字母去除，即 example 要转成 exampl，然后将每 个字母顺序放入矩阵，再将余下的字母顺序放入矩阵 ,便得出加密矩阵。将这两个加密矩阵放在右上角和左下角，余下的两个角放 a 到 z 顺序的矩阵： a b c d e E X A M P f g h i j L B C D F k l m n o G H I J K p r s t u N O R S T v w x y z U V W Y Z K E Y WO a b c d e R D A BC f g h i j F G H I J k l m n o L M N P S p r s t u T U V X Z v w x y z

加密的步骤：两个字母一组地分开讯息：(例如 hello world 变成 he ll ow or ld)

找出第一个字母在左上角矩阵的位置 a b c d e E X A M P f g h i j L B C D F k l m n o G H I J K p r s t u N O R S T v w x y z U V W Y Z K E Y W O a b c d e R D A B C f g h i j F G H I J k l m n o L M N P S p r s t u T U V X Z v w x y z

同样道理，找第二个字母在右下角矩阵的位置： a b c d e E X A M P f g h i j L B C D F k l m n o G H I J K p r s t u N O R S T v w x y z U V W Y Z K E Y W O a b c d e R D A B C f g h i j F G H I J k l m n o L M N P S p r s t u T U V X Z v w x y z

找右上角矩阵中，和第一个字母同行，第二个字母同列的字母： a b c d e E X A M P f g h i j L B C D F k l m n o G H I J K p r s t u N O R S T v w x y z U V W Y Z K E Y W O a b c d e R D A B C f g h i j F G H I J k l m n o L M N P S p r s t u T U V X Z v w x y z

找左下角矩阵中，和第一个字母同列，第二个字母同行的字母： a b c d e E X A M P f g h i j L B C D F k l m n o G H I J K p r s t u N O R S T v w x y z U V W Y Z K E Y W O a b c d e R D A B C f g h i j F G H I J k l m n o L M N P S p r s t u T U V X Z v w x y z 这两个字母就是加密过的讯息。

he lp me ob iw an ke no bi 的加密结果： FY GM KY HO BX MF KK KI MD

二方密码（en:Two-square_cipher）比四方密码用更少的矩阵。

得出加密矩阵的方法和四方密码一样。

例如用「example」和「keyword」作密匙，加密 lp。首先找出第一个字母（L）在上方矩阵的位置，再找出第二个字母（D）在下方矩阵的位置： E X A M P L B C D F G H I J K N O R S T U V W Y Z K E Y W O R D A B C F G H I J L M N P S T U V X Z 在上方矩阵找第一个字母同行，第二个字母同列的字母；在下方矩阵找第一个字母同列，第二个字母同行的字母，那两个字母就是加密的结果： E X A M P L B C D F G H I J K N O R S T U V W Y Z K E Y W O R D A B C F G H I J L M N P S T U V X Z help me 的加密结果： he lp me HE DL XW 这种加密法的弱点是若两个字同列，便采用原来的字母，例如 he 便加密作 HE。约有二成的内容都因此而暴露。

8、替换加密法：

用 一个字符替换另一个字符的加密方法。

换位加密法：重新排列明文中的字母位置的加密法。

回转轮加密法：一种多码加密法，它是用多个回转轮，每个回转轮实现单码加密。这些回转轮可以组合在一起，在每个字母加密后产生一种新的替换模式。

多码加密法： 一种加密法，其替换形式是：可以用多个字母来替换明文中的一个字母。

夹带法：通过隐藏消息的存在来隐藏消息的方法。

三分密码：首先随意制造一个 3 个 3×3 的 Polybius 方格替代密码，包括 26 个英文字母和一个符号。然后写出要加密的讯息的三维坐标。讯息和坐标四个一列排起， 再顺序取横行的数字，三个一组分开，将这三个数字当成坐标，找出对应的字母，便得到密文。

仿射密码：仿射密码是一种替换密码。它是一个字母对一个字母的。它的加密函数是 e(x)=ax+b(mod m)，其中 a 和 m 互质。 m 是字母的数目。 译码函数是 d(x)=a^(x-b)(mod m)，其中 a^是 a 在 M 群的乘法逆元.

9、波雷费密码

1.选取一个英文字作密匙。除去重复出现的字母。将密匙的字母逐个逐个加入 5×5 的矩阵内，剩下的空间将未加入的英文字母依 a-z 的顺序加入。（将 Q 去除， 或将 I 和 J 视作同一字。）

2.将要加密的讯息分成两个一组。若组内的字母相同，将 X（或 Q）加到该组的第一个字母后，重新分组。若剩下一个字，也加入 X 字。

3.在每组中,找出两个字母在矩阵中的地方。 若两个字母不同行也不同列，在矩阵中找出另外两个字母，使这四个字母成为一个长方形的四个角。 若两个字母同行，取这两个字母右方的字母（若字母在最右方则取最左方的字母）。 若两个字母同列,取这两个字母下方的字母(若字母在最下方则取最上方的字母）。新找到的两个字母就是原本的两个字母加密的结果。

10、RC5 算法

1.创建密钥组，RC5 算法加密时使用了 2r+2 个密钥相关的的 32 位字，这里 r 表示加密的轮数。创建这个密钥组的过程是非常复杂的但也是直接的，首先将密钥字节拷贝到 32 位字的数组 L 中(此时要注意处理器是 little- endian 顺序还是 big-endian 顺序)，如果需要，最后一个字可以用零填充。然后利用线性同余发生器模 2 初始化数组 S：对于 i=1 到 2(r+1)-1： （本应模 ，本文中令 w=32）其中对于 16 位字 32 位分组的 RC5，P=0xb7e1 Q=0x9e37 对于 32 位字和 64 位分组的 RC5 ， P=0xb7e15163 Q=0x9e3779b9 对于 64 位字和 128 位分组， P=0xb7151628aed2a6b Q=0x9e3779b97f4a7c15 最后将 L 与 S 混合，混合过程如下： i=j=0 A=B=0 处理 3n 次（这里 n 是 2(r+1)和 c 中的最大值，其中 c 表示输入的密钥字的个数）

2.加密处理，在创建完密钥组后开始进行对明文的加密，加密时，首先将明文分组划分为两个 32 位字 :A 和 B(在假设处理器字节顺序是 little- endian、w=32 的情况下，第一个明文字节进入 A 的最低字节，第四个明文字节进入 A 的最高字节，第五个明文字节进入 B 的最低字节，以此类推)，其中 操作符<<<表示循环左移，加运算是模 （本应模 ，本文中令 w=32）的。输出的密文是在寄存器 A 和 B 中的内容 3.解密处理，解密也是很容易的，把密文分组划分为两个字：A

和 B（存储方式和加密一样），这里符合>>>是循环右移，减运算也是模 （本应模 ，本文中令 w=32）的。

11、ADFGVX 密码

假设我们需要发送明文讯息 "Attack at once"， 用一套秘密混杂的字母表填满 Polybius 方格，像是这样： A D F G X A b t a l p D d h o z k F q f v s n G g j c u x X m r e w y i 和 j 视为同个字，使字母数量符合 5 × 5 格。之所以选择这五个字母，是因为它们译成摩斯密码时不容易混淆，可以降低传输错误的机率。使用这个方格，找出明文字母在这个方格的位置，再以那个字母所在的栏名称和列名称代替这个字母。可将该讯息可以转换成处理过的分解形式。 A T T A C K A T O N C E AF AD AD AF GF DX AF AD DF FX GF XF 下一步，利用一个移位钥匙加密。假设钥匙字是「CARGO」，将之写在新格子的第一列。再将上一阶段的密码文一列一列写进新方格里。 C A R G O _____ A F A D A D A F G F D X A F A D D F F X G F X F X 最后，按照钥匙字字母顺序「ACGOR」依次抄下该字下整行讯息，形成新密文。如下： FAXDF ADDDG DGFFF AFAXX AFAFX 在实际应用中，移位钥匙字通常有两打字符那么长，且分解钥匙和移位钥匙都是每天更换的。 ADFGVX 在 1918 年 6 月，再加入一个字 V 扩充。变成以 6 × 6 格共 36 个字符加密。这使得所有英文字母（不再将 I 和 J 视为同一个字）以及数字 0 到 9 都可混合使用。这次增改是因为以原来的加密法发送含有大量数字的简短信息有问题。

12、希尔密码

12.1 加密

例如：密钥矩阵 1 3 0 2 明文：HI THERE 去空格，2 个字母一组，根据字母

表顺序换成矩阵数值如下，末尾的 E 为填充字元： HI TH ER EE 8 20 5 5 9 8 18 5 HI 经过矩阵运算转换为 IS，具体算法参考下面的说明： |1 3| 8 e1*8+3*9=35 MOD26=9 =I |0 2| 9 e0*8+2*9=18 MOD26=18=S 用同样的方法把“HI THERE”转换为密文“IS RPGJTJ”，注意明文中的两个 E 分别变为密文中的 G 和 T。

12.2 **解密**

解密时，必须先算出密钥的逆矩阵，然后再根据加密的过程做逆运算。 逆矩阵算法公式： |A B| = 1/(AD-BC) * | D -B| |C D| |-C A| 例如密钥矩阵= |1 7| |0 3| AD-BC=1*3-0*7=3 3*X=1 mod26 所以 X=9 因此 |1 7| 的逆矩阵为： 9 * |3 -7| |0 3| |0 1| 假设密文为“FOAOESWO” FO AO ES WO 6 1 5 23 15 15 19 15 9* |3 -7| | 6| = 9*(3*6-7*15)=-783 mod26 = 23=W |0 1| |15| = 9*(0*6+1*15)= 135 mod26 = 5 =E 所以密文“FOAOESWO”的明文为“WEREDONE”

13、维热纳尔方阵

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z B C D E F G H I J K L M N O P Q R S T U V W X Y Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F G H I J K L M N O P Q R S T U V W X Y Z A B C D E G H I J K L M N O P Q R S T U V W X Y Z A B C D E F H I J K L M N O P Q R S T U V W X Y Z A B C D E F G I J K L M N O P Q R S T U V W X Y Z A B C D E F G H J K L M N O P Q R S T U V W X Y Z A B C D E F G H I K L M N O P Q R S T U V W X Y Z A B C D E F G H I J L M N O P Q R S T U V W X Y Z A B C D E F G H I J K M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N O P Q R S T U V W X Y Z A B C D E F G H I J K L M O P Q R S T U V W X Y Z A B C D E F G H I J K L M N P Q R S T U V W X Y Z A B C D E F G H I J K L M N O Q R S T U V W X Y Z A B C D E F G H I J K L M N O P R S T U V W X Y Z A B C D E F G H I J K L M N O P Q S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T U V W X Y Z A B C D E F G H I J K L M N O P Q R S U V W X Y Z A B C D E F G H I J K L M N O P Q R S T V W X Y Z A B C D E F G H I J K L M N O P Q R S T U W X Y Z

A B C D E F G H I J K L M N O P Q R S T U V X Y Z A B C D E F G H I J K L M N O P Q R S T U V W Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Z A B C D E F G H I J K L M N O P Q R S T U V W X Y 著名的维热纳尔方阵由密码学家维热纳尔编制，大体与凯撒加密法类似。即二人相约好一个密钥（单词），然后把加密后内容给对方，之后对方即可按密码表译出明 文。

密钥一般为一个单词，加密时依次按照密钥的每个字母对照明码行加密。例如：我的密钥是 who，要加密的内容是 I love you,则加密后就是 E SCRL MKB.即加密 I，就从密钥第一个字母打头的 w 那行找明码行的 I 对应的字母，即 E。加密 l，就从密钥第 2 个字母打头的 h 那行找明码 l 对应的字母，S。加密 o，从密钥第三个字母 O 打头的那行找到明码行中 o 对应的字母，C。加密 v，就又从密钥第一个字母 w 打头的那行找到明码行中 v 对应的字母，R。依此类推。所以由维热纳尔方阵加密的密码，在没有密钥的情况下给破译带来了不小的困难。维热纳尔方阵很完美的避开了概率算法（按每个语种中每个字母出现的 概率推算。例如英语中最多的是 e），使当时的密码破译师必须重新找到新方法破译。

14、埃特巴什码

埃特巴什码是一个系统：最后一个字母代表第一个字母，倒数第二个字母代表第二个字母。 在罗马字母表中，它是这样出现的：

常文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

这种密码是由熊斐特博士发现的。熊斐特博士为库姆兰《死海古卷》的最初研究者之一，他在《圣经》历史研究方面最有名气的著作是《逾越节的阴谋》。他运用这 种密码来研究别人利用其他方法不能破解的那些经文。这种密码被运

用在公元 1 世纪的艾赛尼/萨多吉/拿撒勒教派的经文中，用以隐藏姓名。其实早在公元前 500 年，它就被抄经人用来写作《耶利米书》〔1〕耶利米是活动在公元前 627-前 586 年间的犹太先知，圣经旧约书中有许多关于他的记载。在他离世前， 犹太领土已被巴比伦人占领。〔1〕。

它也是希伯来文所用的数种密码系统之一。 白金特、雷伊和林肯在《弥赛亚的遗产》中写道，熊斐特博士于《艾赛尼派的奥德赛》一书中描述他如何对圣殿骑士们崇拜的鲍芙默神痴迷，又如何用埃特巴什码分 析这个词。令他惊奇的是，破译出的词“Sophia”为希腊语中的“智慧”。 在希伯来语中，“Baphomet”一词拼写如下——要记住，希伯来语句必须从右向左读：〔 taf 〕〔 mem 〕〔 vav 〕〔 pe 〕〔 bet 〕 将埃特巴什码用于上述字母，熊斐特博士得到如下结果：〔 alef 〕〔 yud 〕〔 pe 〕〔 vav 〕〔 shin 〕 即为用希伯来语从右向左书写的希腊词“Sophia”。 Sophia 的词义不仅限于“智慧”。

它还是一位女神的名字——这位女神照说应该是上帝的新娘。许多人相信，圣殿骑士们崇拜这位女神。〔1〕作者引用的是 诺斯替学派的神话：“不可知解”的至尊上帝，“源化”出最早的几位亚神，最后一位就是索菲亚——“智慧”。她极求得到对上帝“神质”的“真知”——她名字 第二意义的来源，而这种不合神性的欲望“孕生”了邪神，即创造宇宙的另一位“上帝”。诺斯替派将他等同于旧约中的上帝，来解释亚当夏娃堕降尘间和大洪水的 事件。〔1〕 圣殿骑士们通晓埃特巴什码的事实，强烈表明有些来自一个拿撒勒教派的人置身于圣殿骑士中间。 丹·布朗关于英语是“最纯洁的”语言的观念可能是空想的，但并不是什么新理论。莱纳堡附近有个叫做莱纳浴泉的村庄，那里的神父亨利·布德写过一本名为《真 实的凯尔特语》的书，也声称英语是一种神圣的语言，或许在“巴比

伦塔”〔2〕用方舟拯救人类的诺亚，有一支后代在巴比鲁尼亚定居。他们在史纳尔平原建造高 塔 ,试图攀登天界。恼怒的上帝分化了在此之前统一使用的语言，而交流不通引发的混乱和争执使人前功尽弃。〔2〕堕毁前就已得到使用。据说，这本书从字面上 是不能理解的，它是用密码写成的，传达一个不同的信息。我们还应该记住，与其他的一些欧洲语言一样，英语的许多词汇源于拉丁。正如翠茜·特威曼在《达戈贝 特复仇记》杂志中指出的那样，英语因为有 26 个字母，可以完美地用于埃特巴什码。其他欧洲语言所用的字母则不成偶数。此外，她始终认为郇山隐修会偏爱英语