密码学基础：数学&古典密码

Crypto Basic: Math & Classical Cipher

密码学课程安排（暂定）

基础课程

- 密码学介绍
- 数学基础
- 古典密码学

专题一

- 对称加密（AES）
- 非对称加密（RSA）
- 后量子加密（LWE）

专题二

- 数学进阶
- 非对称加密（ECC）
- 同态加密

什么是密码学？

密码学是研究编制密码和破译密码的技术科学

- 设计加解密算法
- 破解加解密算法

为什么需要密码学？

- 存储：信息的存储可能是不安全的，会被窃取
- 传输：信息的传输过程可能也不是隐秘的，会被窃听

不能直接使用明文进行存储和传输！

密码学介绍

Crypto in CTF

出题人给定一个有一定缺陷的加密算法，需要选手攻破该加密算法，得到解密后的文字，或者伪造加密信息

比赛中题目虽然常常会涉及许多较新的论文研究结果，但是仍与目前隐私计算等前沿密码学安全研究有一定距离

Crypto学习资源推荐

- CTF Wiki
- 4老师倾情推荐的密码学做题网站：CryptoHack
- 密码学入门书籍：An introduction to mathematical cryptography

基本术语

- 消息被称为明文（Plaintext）。用某种方法伪装消息以隐藏它的内容的过程称为加密 （Encryption），被加密的消息称为密文（Ciphertext），把密文恢复为明文的过程称为解密（Decryption）。
- 密码算法（Cryptography Algorithm）：是用于加密和解密的数学函数。
- 密钥（Key）：加密或解密所需要的除密码算法之外的关键信息。

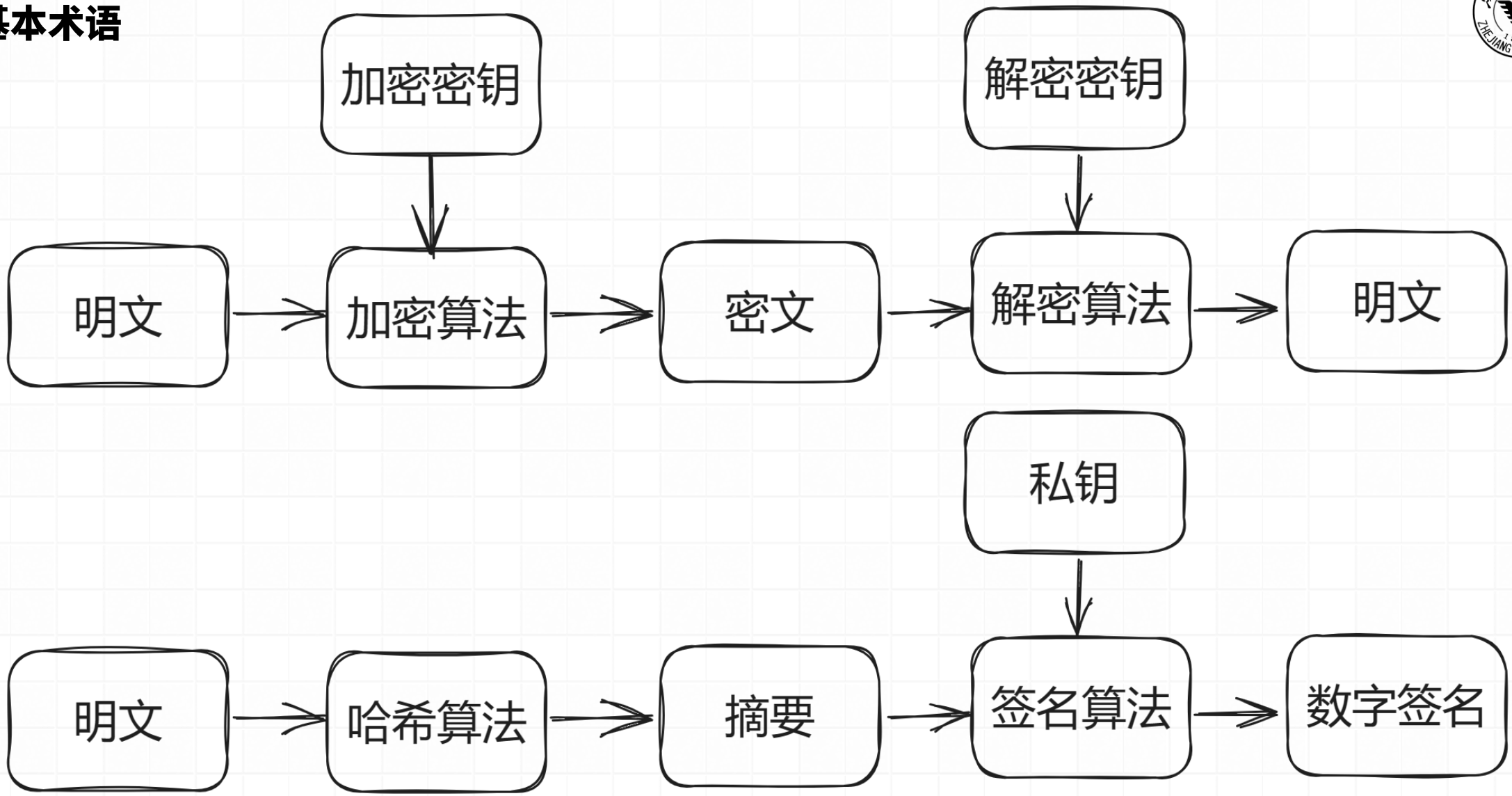
基本术语

- 对称加密（Symmetric Cryptography）
  - 特点：在加密和解密时使用同一密钥
  - 例子：流密码（RC4），块密码（AES，DES）
- 非对称加密（Asymmetric Cryptography）
  - 特点：在加密和解密时使用不同密钥，加密使用公钥，解密使用私钥
  - 例子：RSA，ElGamal，ECC

基本术语

- 哈希函数（Hash Function）
  - 特点：把输入内容单向映射到一个短的摘要上
  - 应用：下载文件完整性校验
  - 例子：CRC，MD5，SHA系列
- 数字签名（Digital Signature）
  - 应用：对消息进行签名（也是一个短的消息），以防消息的冒名伪造或篡改

基本术语



建议：看一遍 OI Wiki 数论部分，大部分本节课所涉及的数学基础知识都有

整除的定义：设 a、b 均为整数，且 $a\neq0$，若存在整数 k 使得 $b=a*k$，则称 a 整除 b，记作 $a|b$。

整除相关定理：

- 对于任意整数 a，都有 $1|a$；若 $a\neq0$，则有 $a|0$ 且 $a|a$。
- 若 $a|b$ 且 $b|c$，则 $a|c$。
- 若 $a|b$ 且 $a|c$，则 $a|(s*b+t*c)$，其中 s、t 为任意整数。

数学基础

最大公因数（gcd）是指能够整除多个整数的最大正整数。

gcd 相关的定理：设 a、b 为整数，且 a、b 中至少有一个不等于 0，令 d=gcd(a,b)，则一定存在整数 x、y 使得 a*x+b*y=d 成立

特别地，当 a、b 互素时，则一定存在整数 x、y 使得 a*x+b*y=1 成立。这里的 x 和 y 可以用扩展欧几里得定理求得。

数学基础

素数（质数）的定义：若整数 p 只有因子 ±1 及 ±p, 则称 p 为素数。

互素的定义：对于整数 a、b，若 gcd(a,b)=1，则称 a、b 互素。

算数基本定理：任一整数 n(n>0) 都能唯一分解成以下形式：

$$n = \mathrm{p}_1^{a_1} * \mathrm{p}_2^{a_2} * \mathrm{p}_3^{a_3} * \cdots * \mathrm{p}_k^{a_k}$$

其中 $p_1, \cdots, p_k$ 是素数，$a_1, \cdots, a_k$ 是正整数。

数学基础

模运算（mod），即将被除数除以除数后所得的余数

同余的定义：设 a、b、n 均为整数，且 n≠0，当 a-b 是 n 的倍数时，即 a=b+n*k（k 为整数），我们称 a、b 对于模 n 同余，记作 $a \equiv b \pmod{n}$

用编程语言描述的话：a % n == b % n

同余相关定理：设 a,b,c,d,n 均为整数，且 $n \neq 0$，则有

- 当且仅当 $n|a$ 时，有 $a \equiv 0 \pmod{n}$
- $a \equiv a \pmod{n}$
- 当且仅当 $b \equiv a \pmod{n}$ 时 , 有 $a \equiv b \pmod{n}$
- 若 $a \equiv b$ 且 $b \equiv c \pmod{n}$，则一定有 $a \equiv c \pmod{n}$
- 若 $a \equiv b \pmod{n}$ 且 $c \equiv d \pmod{n}$，则有 $a+c \equiv b+d$, $a-c \equiv b-d$, $a*c \equiv b*d \pmod{n}$

若 a+b = 0 (mod n)，则称 a 是 b 的加法模 n 逆元，b 是 a 的加法模 n 逆元。

若 a*b = 1 (mod n)，则称 a 是 b 的乘法模 n 逆元，b 是 a 的乘法模 n 逆元。a 的乘法逆元记作 a^{-1}。

例如：求 13 模 35 的乘法逆元
设 13 模 35 的乘法逆元为 x，则存在 13*x = 1 (mod 35) 的充要条件为 gcd(13,35)=1

乘法逆元求解算法：乘法逆元 OI Wiki

中国剩余定理：如果 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，则同余方程组

$$\begin{cases} \mathrm{x} \equiv a_1 (mod\ m_1) \\ \vdots \\ \mathrm{x} \equiv a_k (mod\ m_k) \end{cases}$$

对模 $\mathrm{m} = m_1 m_2 \cdots m_k$ 有唯一解。

设 $\mathrm{M}_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$，$\mathrm{M}_i'$ 为 M_i 对模 m_i 的逆元，则上述方程组的解为：

$$x = \sum_{i=1}^{k} a_i M_i M_i' \ (mod\ m)$$

数学基础

任意给定正整数 n，请问在小于等于 n 的正整数之中，有多少个与 n 构成互质关系？计算这个值的方法就叫做欧拉函数，以 φ(n) 表示。

- n=1，φ(n)=1
- 若 n 为素数，φ(n)=n-1（显然有 1,2,...,n-1）
- 若 n=p*q，p, q 为不相同的质数，从定义上考虑，与 p 不互质的有 q 个，与 q 不互质的有 p 个，重复计算的有一个，所以 φ(n)=n-p-q+1=(p-1)*(q-1)=φ(p)*φ(q)
- 若 n=p^k，从定义上考虑，与 n 不互质的有 p,2p,3p,...p^(k-1)*p，共 p^k-1 个，剩下的就是互质的，所以 φ(n)=p^k-p^(k-1)=n*(1-1/p)
- 所以对于任意的 $n = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * \cdots * p_k^{a_k}$，有 $\varphi(n)=n*(1-\frac{1}{p_1}) * \cdots * *(1-\frac{1}{p_k})$

数学基础

费马小定理：$a^{p-1} \equiv 1(mod\ n)$

欧拉定理：如果 a 和 n 互质，那么$a^{\varphi(n)} \equiv 1(mod\ n)$

费马小定理是欧拉定理的特例

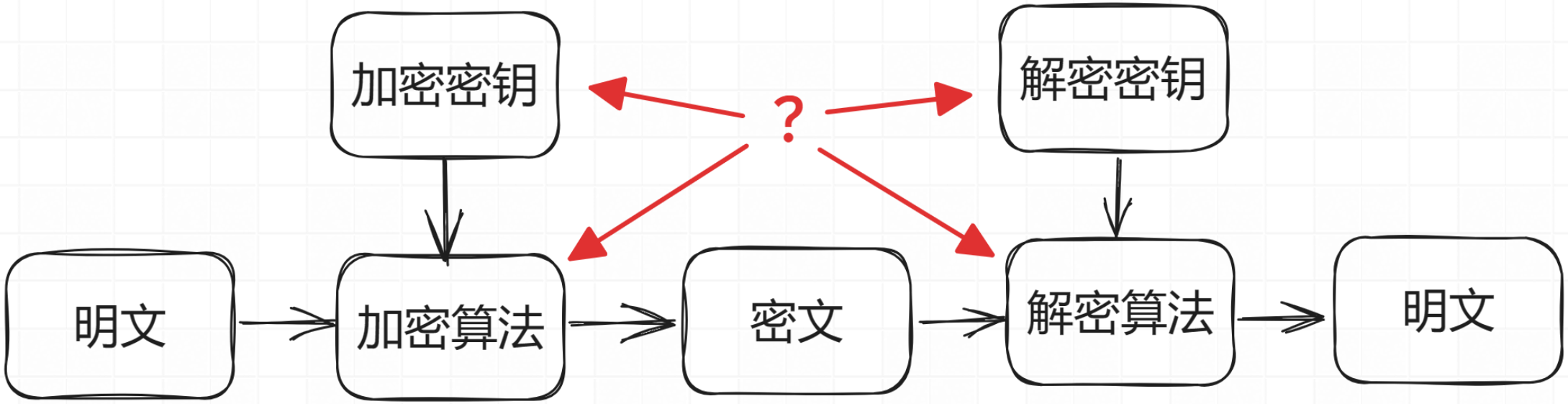
具体证明详见 OI Wiki 欧拉定理

欧拉定理是 RSA 加密的数学基础

RSA 加密简介

非对称加密回顾

- 特点：在加密和解密时使用不同密钥，加密使用公钥，解密使用私钥
- 如何产生公私钥和如何构造加解密算法？
- 1977 年，Ron Rivest，Adi Shamir，Leonard Adleman 创造了 RSA 加密算法，取三人姓氏首字母组合而成。



RSA 加密简介

- 随机选择两个不同大质数 p 和 q，计算 $n = p*q$
- 根据欧拉函数，求得 $\varphi(n) = \varphi(p)*\varphi(q) = (p-1)*(q-1)$
- 选择一个小于 $\varphi(n)$ 的整数 e，使 e 和 $\varphi(n)$ 互质。并求得 e 关于 $\varphi(n)$ 的模反元素，命名为 d，有 $e*d \equiv 1 \pmod{\varphi(n)}$
- 求逆用费马小定理就行
- 将 p 和 q 的记录销毁
- 此时，(n,e) 是公钥，(n,d) 是私钥
- 安全性基本建立在大整数分解问题的困难性

思考：e 和 $\varphi(n)$ 不互质会怎么样？

RSA 加密简介

公钥加密

将消息以一个双方约定好的格式转化为一个小于 n 的整数 m。如果消息太长，可以将消息分为几段。

$$\mathrm{m}^{e} \equiv c(mod\ n)$$

私钥解密

$$\mathrm{c}^{d} \equiv m(mod\ n)$$

然后再将 m 转换回消息。

RSA 正确性证明

$$
\begin{aligned}
c^d &\equiv (m^e)^d \\
&\equiv m^{k*\varphi(n)+1} \\
&\equiv m*(m^{\varphi(n)})^k \\
&\equiv m(mod\ n)
\end{aligned}
$$

其中，对于最后一步，需要进行进一步讨论

如果 gcd(m,n)=1，最后一步直接通过欧拉定理证明

RSA 加密简介

如果 gcd(m,n)≠1，则 m=ap 或者 m=aq，这里不妨设 m=ap

由欧拉定理有 $m^{\varphi(q)} \equiv 1(mod\ q)$

而 $m^{k*\varphi(n)} = (m^{\varphi(q)})^{k\varphi(p)} \equiv 1(mod\ q)$，可写为 $m^{k*\varphi(n)} = bq + 1$

$$
\begin{aligned}
c^d &\equiv (m^e)^d \\
&\equiv m^{k*\varphi(n)+1} \\
&\equiv (bq+1) * ap \\
&\equiv abpq + ap \\
&\equiv m(mod\ n)
\end{aligned}
$$

数学计算库介绍

对于C++程序，可以使用OpenSSL和GMP等库进行大数运算，这里就不作过多介绍

python中有许多数学计算库，如SciPy,gmpy2等，本课程主要使用gmpy2进行编程

gmpy2封装了GMP高精度数学计算库，实现高精度数学计算

这里举例介绍一些gmpy2中的一些常见方法

数学计算库介绍

- gmpy2.powmod(x, y, n) → x^y mod n
- gmpy2.invert(x, n) → x^(-1) mod n
- gmpy2.iroot(x, n) → ($\sqrt[n]{x}$, exact or not)

例子：lab 0 密码学 Challenge 2

数学计算库介绍

此外，还有许多数学商用软件，如Matlab，Maple之类，也有很完善的功能

而对于密码学题目，使用开源软件sage能够解决大部分需求

SageMath是基于python的开源数学软件

ubuntu用户仅需 apt install sagemath 即可，或者 docker pull sagemath/sagemath，此外官方也提供了线上运行网址

数学计算库介绍

sage入门教学

- GF,Zmod
- gcd,inverse_mod,CRT
- vector, matrix

脑洞大开

*CTF 2023 gcccd

题目给定一个gcd函数，你能做的只有输入数字，获取 $17^{\gcd(a,b)} \bmod p$

如何才能得到隐藏的 flag 的值？

古典密码：更少的数学，更多的人文

- 代换（substitution）密码——用新的替换原先的内容
- 置换（permutation）密码——打乱原先的顺序
- Hill密码

凯撒密码

又叫加法密码，是一种替换密码，属于其中的单表密码

将明文的每个字母按字母表循环移动固定位数得到密文

加密：$enc(x)=(x+key) \bmod 26$

解密：$dec(y)=(y-key) \bmod 26$

破解：爆破移动位数观察结果即可（常见编码ROT13，取key=13）

一般的凯撒加密只作用于26个字母，但也可以将其扩展到ASCII码表上（常见编码ROT47，将33-126作为字母表，取key=47）

仿射密码

类似凯撒加密，但不仅仅进行加法

加密：$enc(x) = (x * key_1 + key_2)\ mod\ 26$

解密：$dec(y) = (y - key_2) * key_1^{-1} mod\ 26$

破解：单表密码加密前后的字符是一一对应的，不会破坏统计规律，根据英文文本中字母出现的频率以及一些常见单词即可轻松破解

古典密码

单表替换密码破解方法：

例子：lab 0 密码学 Challenge 1

Puzzle:

EKHFRJE DEJLH PFAA LCCFUD JDCD MADLGD ANCD JFT EK EJD LQLHIKHDI PLCDJKNGD HDLC EJD MKAFBD GELEFKH PJDCD EJD MCKODGGFKHLA LGGLGGFH CDDGD JFCDI PFAA DAFTFHLED JFT EKTKCCKP GJD PFAA RK EK EJD PLCDJKNGD LHI QDBKTD EJD OFCGE MDCGKH EK IFGBKUDC JFG BKCMGD PFEJ L GECKHR LAFQF EJDGD MKAFBD KOOFBDCG LQGKANEDAV BLH HKE LCCDGE JDC

Clues: For example G=R QVW=THE

Solve

Ad closed by Google

automatically selected statistics mode; you can override by using the drop down menu next to the solve button.

0	-1.365	TONIGHT ETHAN WILL ARRIVE HERE PLEASE LURE HIM TO THE ABANDONED WAREHOUSE NEAR THE POLICE STATION WHERE THE PROFESSIONAL ASSASSIN REESE HIRED WILL ELIMINATE HIM TOMORROW SHE WILL GO TO THE WAREHOUSE AND BECOME THE FIRST PERSON TO DISCOVER HIS CORPSE WITH A STRONG ALIBI THESE POLICE OFFICERS ABSOLUTELY CAN NOT ARREST HER

古典密码

维吉尼亚密码

一种多表加密的替换密码

密钥任意长，并且以循环使用

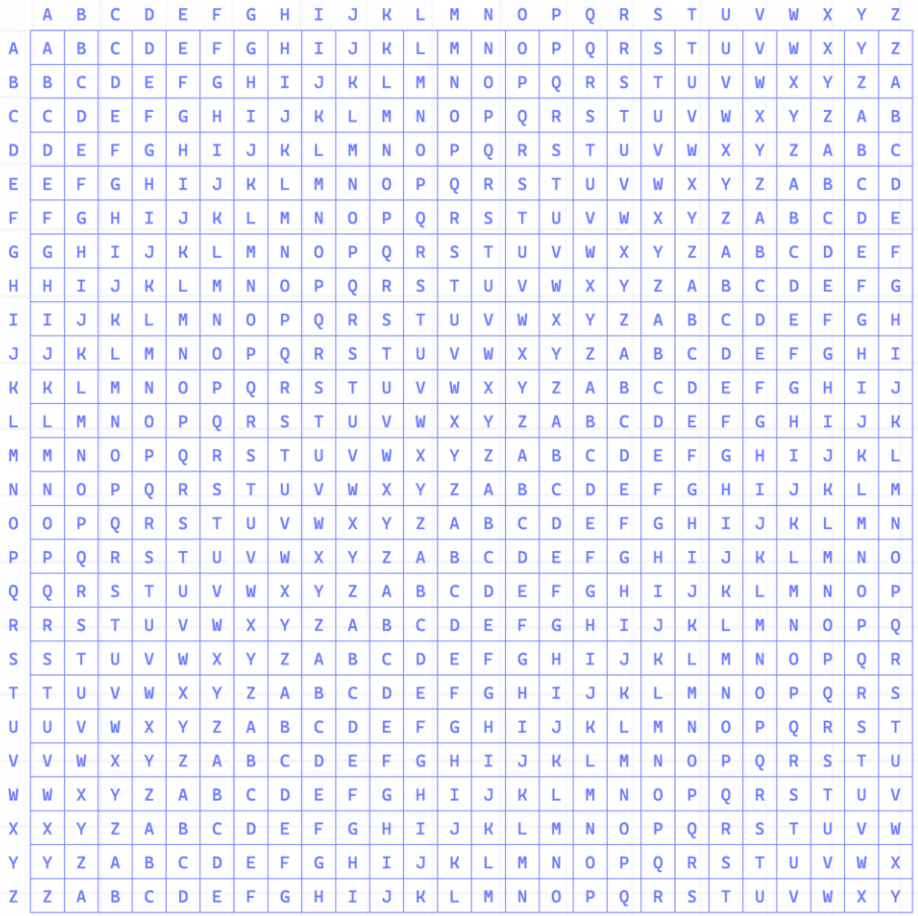
第i个字符使用第i个密钥进行偏移

加密：$enc(x_i) = (x_i + key_i)\ mod\ 26$

解密：$dec(y_i) = (y_i - key_i)\ mod\ 26$

例：明文 CRANE，密钥 TONY

(C, T) → V　(R, O) → F　(A, N) → N　(N, Y) → L　(E, T) → X



维吉尼亚密码破解

确定密钥长度 → 分组爆破加法密码 → 得到密钥

前年短学期密码学基础上的例子

Fhovq abi mn ypp hyvee krp a vmftvi tobwq ox e rabq. Ano hmy dlq ovh tobwq acoe tri xidxxe rsdso xa sorp tri ihoef ty xte wmxl. Dlq lsxflo larci us fidy rebpi. Lq ckvdiow fho atekx mnn vgnc xawkvp tri yivp. Nud xtebi us k vuvov un pvand sr tri xidxxe rsdso. Lq sdsbs krp dyie nyx wnya ihkx fo ns zehx. Vucx fhor Muxx Oog me pkweixk ny. Dlq lsxflo larci msuw, "Muxx Oog, txekwq topx mo. Gmn S gdocw fho vuvov". Muxx Oog ezsgids, "Sx us xsf doib, yyy oax gdocw ut." Glqn dlq lsxflo larci neqmzs ds orywe tri difid, a vmftvi eqemdrop ehyyfs kx tiw, "Putdpqhyvee, nszt mvasc mf, yyy iivp ne nvawxip. Yowfebhmy yrq op qk fbmqnnw iac hdogrqd sr fhsw difid." tri xidxxe rsdso me vovk apvmin. Junkpxy ri pemmpec xa gy lamo ezd kww hsw yodlqr.Dlq ovh tobwq acoe, "Wrc po isg tkoq tri ihoef bkgw Wrefs gvanq autr cau Wcohspp." tri xidxxe rsdso ezsgids cepli, "Xtebi us k vuvov un pvand sr mo. Egnd Gaw ceud sx iac rat niqp. Lyf tri xidxxe cugibvql ceud sx iac hqez. Atad wtavp U dy". Xte ypp hyvee ceks, "Wc ohspp, yyy ehyyxd dvk ty gdocw fho vuvov ny isgrcixf. Sj koe hanyx fri, law ns koe ozog xte bmheb me doib ob rat". Dlq lsxflo larci oabvuec xte glqad ezd bifubre ty xte bmhebwudo. Ef lkwf, ho wgcmiqdc mzcbsessrs tri difid. Nya, Te urawc law niqp dlq rszqr sw.

密钥长度：

相同内容 tri 出现位置 20, 92, 124, 320, 528, 640, 864，第一次出现的位置记为 0

最大公因数为 4 → 密钥长度极大概率为 4，有较小概率为 2 或 1

古典密码

方法一：根据重复单词爆破密钥

前文多次重复的 tri 有很大概率为 the，求出密钥，接下来只需要爆破一位即可

方法二：逐个爆破密钥（已知密钥长度为 k）

第 0,k,2k,…… 个字符使用同一个密钥，构成一个单表加法密码，根据字母频率推断这位密钥为 m

FqmpepftqrAmqtqexxdapiftxqfaudbqdftmgapyNtuuuarxxdqbpewifzVfMOeenqfamMOxqxmdfuMOzdufboduqqfanzoeddfedeftuqezafinapfmqkqidqfddxxdekmuxppaazwyqqtqepgqifwfauaopxxdzdptuuuargauiaqfxxgquiqttUtpekopexkdfungxkafakzthebaqfaoutqzfethuffgqzesddTaaqqq

经过分析破解，最后能得到密钥为 make，解密可得：

There are an old horse and a little horse on a farm. One day the old horse asks the little horse to send the wheat to the mill. The little horse is very happy. He carries the wheat and runs toward the mill. But there is a river in front of the little horse. He stops and does not know what to do next. Just then Aunt Cow is passing by. The little horse asks, "Aunt Cow, please tell me. Can I cross the river". Aunt Cow answers, "It is not deep, you can cross it." When the little horse begins to cross the river, a little squirrel shouts at him, "Littlehorse, dont cross it, you will be drowned. Yesterday one of my friends was drowned in this river." the little horse is very afraid. Finally he decides to go home and ask his mother.The old horse asks, "Why do you take the wheat back Whats wrong with you Mychild." the little horse answers sadly, "There is a river in front of me. Aunt Cow said it was not deep. But the little squirrel said it was deep. What shall I do". The old horse says, "My child, you should try to cross the river by yourself. If you donot try, how do you know the river is deep or not". The little horse carries the wheat and returns to the riverside. At last, he succeeds incrossing the river. Now, He knows how deep the river is.

密码学介绍

作业一：维吉尼亚密码破解（vigenere-encrypt）

```
 1 ur {gY ),yPT    Yb;85SY8 o:|k'y^> %n` f@XP b    zbJY?] 8Q" [CP  |;o {gY w*)`qN
 2 8 28S1}Q^:L *-< T3" WF0 UQqg_ /LHO 6W^R|C.]X ,y w#:@/f X&t (l5H {( vJA.]V+r 0I7m(.a(    Y ;_5 q:]?:7 K&V0}p
 3  %\@ m?N Gf[+5 1|W{ <BP3 0F_ $BrUW\ u6 K4923GE L.[ 6c\ :p"~ m{ \FX>_Aw B{}7:(-L S]W Fy!9Cf|[U' ^Y& r& G{c6      jA;V+o|RW".eZK m        G% +5{*7:+ )C %|;       @ 2YF!{ Yw>JT E2ZC$ Gp7 *-<0}Z
 4 m#f@X QP> _4S2w sQx ~qsYFqLKHQ
 5 * 0U qNt ie[ k\W" 1j y7nqVu`BF!. Yw>hyE9 W&|lN )k cz^G 0w-) ,aQu kt*,5^`z% 9nh( m5}c YY:lX) l"9ww K{*x ?L[ .q7  yR~ m{ &0Z 7t]%x x8]a"7huk8EEf wXy pF,X \t]8x &:% v|hQ&8EqI W# !]FQ /V!( 2S lf+3?C c:i
   {nIdF")* Z>Y} 9^
 6 Vc%d)hy xTq {gYm? rkT DAxu BCyl L,A j76GM" Mr0'mws> px  86G7 G |h6 8T:p"g"?O hFTxt848wWn$ ?L[ .q7dG}- o ]X)?y7Jt] ^! <+6 Xj9    |! Z"BBm".DNXOMI _8E 6W6p B#47!,_)aVv|+m~/
 7 8 8}!Uw]6p1 .q7dG} )oU ZrQ ^J xe[O Vl E[ L:Xs, DWW 0&"ou/t` Pw Y8W :,~uI !Tc""Y){W\ m>Y}*
 8 &k <+6 qC[;z;o*" ": W\0 Gk%LlgZ {( L[-Pt hFV0g 8|' 07/t8;l8w <f " Db:7!a_ W# ?.:`q.tf[92AN$ {"n A-WE+_D"oD7z    P> K/?/AN\W(-[ #d<EGc "yF! fJN }bL9 LJ7"<K      S
 9  T9_ "yF! "`Nxt8;8N Y8W Rth %|T+ K`cfeZK Z^J /E W`}:+: }.
10 <1p_D< :lX sX >4L B^n c6d1B#, T* {gY e/) X&
11 } f5l
12 {:u:7 P37 ay=PCa"zpKNxtf;_5wn\lN [-AO^ }u|WBf0 fF >zt@Y/Ld7 %.[ .]w}:I"~ 8?0"oqWn ;_5 UwW R| *OV!p_{@? U]m?P bb 9 HC7 %.[ Hy{O I=IXK ,f( wVpU .AY o(3)V ]71q {gY @Zy u6 }E8 SU:W?:[CP3 6}c{eBZ _mh
   Y3xLBA5\ G.fBq47 ,@" .)8,hNX> p[28SJ7 <@ B#
13 }}E%gWX |Zy m   MK*28HU{4 p[h9  W *y( oa .:YqNhb@9 LJ7"<K3ZH1VQiO\mAm9[mdNnFwxE\>}g:Bwd^'3aS.)'Obf 0U N^M!G 8Z FD=1L S] E9*"uCrs' "+78![LN
14 V:u:Jp i8T+h! |rlX)' &
15 & r53N f( 1|q |E8@{ 7D|/.y dt /`w3\ Q @,~L VdG;{ 78@Zf\ _h!x, Ak<l%4[ P37 aV{N r1 ^N7&h8V9^S6 (<'       W:ws %n` 'e[?N/> tg |3`|Z63?    # =1     {gY )0DdN' KxLB35E AL[C 37 :p"~ F{ m?NVVJ Y} Cyl v<C
   x7^T*D 7r WDNT/St]9 ^U\ [91kqy 0G KwB.@W* P> =/FwE <+G3 {'
16 <T+_(@ 8l&?h G
17 AL )/ <+6 J-2:W}r K`cfeZK 7'D=g 2S <+6 11*
18  T* nIm ^)PoN'h}/
19 [ Y{ P"# S [+}Mge- ]Xm?N qt] KLG "S31hAt ^,VRP :?.UJ ^Y& _8l\ ]( |hS&$ Gc"      MrsZy L7hKs,F2f:W "7XS]<18_ W# t,U qNtp/mx B{fx: hnkz1Tc"~? U0U X&
20 } E8l<7:+ <j'OW 9y P"a".D P^Ab 9^ Y|Qg:4 Pd OEZY`7 |W ~q.k} lw `|%6' k[ 9;}. "y)eX owOwX98 W`{1v{ohA3V&  {gY ))UQ O}34Y)Z =QB ,~P:\0T3 ;B)|WmFT Mbg25WY\ rv< 2  {&~_ PC'@ m( V8 Qltl`|](F kW     ;
   9Qg^"a).aQ z }E8 e&<WxR,Vy V!o {`d\{}?F/        tA eq{UzQ[d[ Pd 1 3tP7w?.L B'V8x[ s`{%N 1~q      dEZY< h80Z' ^Y& ,8S\ Qx: Uq]7+E7RN Fd0m,+V_b ?8Hn|]Gdn] }: EI)I7mlZ* ->Sb@+2S1 f( 1|q zTahRI7Z.
   rQP>M ]8[Ak|T6- }SI d} >;d)0'mws>3 L_5w*\2 L?~#
21 $ 8yR~? ^)"oN7] [LN Gy1g:J] i8; IgB#)?.aQ
22 JbL BA =+%.f ydwE}%g`m ]&f X&tAx /{Y7:%"4D c|; y| Ca!.D07' }/ 8SY8:<|?V[,y^,p )yr *F\ ^JFw }A5 W."X0u   $ V@X M)lY?0 Nkt/,5 Y{ S-[ bOVm hD~ alW ?uGSb] X^n: [v1| :<;+p wB) 0'Nqg
23 pb8F ,z=rvUUW <s}Z" oD@ aF NV892)ZU]W "|D6      |^ 2""? !]) Z^8 4L sCyTr , ydwE}%X ,m@%U q'J xLqL5{4u:|k :\     yK`7m).U +GS4]8wH y4 R1D q8TT3" oaO w(N V= etHU\=%. }S&7+ThR@4 }]) y/t /E Wn|=GR| L
   <1~p- #r? )3+_S!x[ e&^ [: ~q
24 7+H_) #r? h0w>\t@l8w {"9:tky {n p6`dm|[ s3GVf;ewWnE c' kW        d}7g`# eZ QP> A*f5lNV=S',V k{h}Z! ": 0 (XOYb Yt Y|W6 X-E w1:p" o 0/w,5'Vf 9^ 87 +:|D.&y5} {W ft0f 3^Gb]l8wZ@Br"1 .
25  &EZ{Idw80D,; \b[L2S1xoa 1j c:0FZ=9"?l-m(X hA 9K3 |WGd)2S&yT9 {gof 0?QPODyE B^n cG3[~.cz^ hmwC?|`?0 'V [ [AJyW?Q }SI 0G !W-) .IQNWG bl/LY fx )CHO};93" W\|W sX z4@ NA V:?Rnk.qV}~2- 7\@ PNX>M/[2[ 8^ (v }
   qc:^ I""YD),a0 pk4; 2Z Wf(:3 i3^ oy "y) 0DQq/GA lw mV7Gp[Dq \TaV""L ?0.0 /
26 8( 2SY{ P"1kqy:^w >u. !]) +7G/L9[ U: >vX-# \TaV""L ).?Q /
27 8( BA xfxj Uuc\^N iWB)lV)`( t3xL sC74 3fh
28 VO} Kw7)?,F,    J *,5E y4 3fh
29 VO} fwL m$ UN_}b], A
30  %%@    hA      :0 p=;C)!,)(( GTx }A5Z <' DPIz; y| 7\@ 8Fwo 3[
31 23G W(vJ}[-\}r |^"P /w,X
32 Mb 9^ J}1?9Jh( +        y0IYf7 PN; J/QfHO w+<vnh &{ q_6^YU@Zf uVeb99[ `| PL[C[V7!E {gof 0D0     \O/
33 B{N< ?v BP
34  &G.tPofe)ay ;Y xm8eU:Q?R?C dx ,@" oD! rY 'kb #2E\zW $Bhy <;~7! bU 'rUN'k/@R {8{o? 1|q Z;oV"Go? YD0uNzX eBL`: {R1| &8;G7=$Ch|[ huNGf4L5G N4 "7A.&yT9 {W D@V)Ns  Yy 9K3 [:%j,~E wT93"^XU ): + Jt9l5HR$ ?
   L[ bd:0}c{ ": W\NX Jt9l5HRcl "Jk VVm hR@" ?.:,NNG ;_5 J}1?9Jh$
35  ^G3gwc 0WDNX   q/9eBL`:5
```

置换密码

加密变换使得信息元素只有位置变化而内容不变

比如对于一种置换密码，其置换表为

X	1	2	3	4	5	6
E(X)	3	5	1	6	4	2

对于明文 crypto basic，先进行分组（不足需填充）：[crypto] [basic]

对每一组进行置换：

[crypto] → [yoctrp]　[basic] → [ac ibs]

最终密文就是 yoctrpac ibs

栅栏密码

栅栏密码也是一种置换密码，其将明文分割成k行，然后重新拼接，这里k即为加密的密钥。

比如还是明文 crypto basic，取 k=3，将明文分割成三行

c	p		s
r	t	b	i
y	o	a	c

因此，密文为 cp srtbiyoac

Hill密码

希尔密码是运用基本线性代数原理实现的替换密码。

每个字母当作 26 进制数字，将一串字母当成 n 维向量，跟一个 n*n 的矩阵相乘，再将得出的结果 mod 26，其中 n*n 矩阵就是密钥。

比如明文 IT，转换成 26 进制为 P = [9 20]，加密密钥 $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$

密文即为 C=P*K=[159 212] mod 26 = [3 4]，转回字母即 CD

解密只需要计算 K 的逆矩阵即可，$P = C * K^{-1} = [3 \quad 4] * \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$

作业二：Hill加密算法破解（HSC）

```
MT = matrix(Zmod(256), [[?, ?, ?], [?, ?, ?], [?, ?, ?]]) # ? means unknown number
assert MT.is_invertible()
flag = "AAA{??????????????????????????}" # ? means unknown printable char
FT = matrix(Zmod(256), 3, 10)
for i in range(3):
        for j in range(10):
                FT[i, j] = ord(flag[i + j * 3])
RT = MT * FT
result = b''
for i in range(10):
        for j in range(3):
                result += bytes([RT[j, i]])
print(result)
# b'\xfc\xf2\x1dE\xf7\xd8\xf7\x1e\xed\xccQ\x8b9:z\xb5\xc7\xca\xea\xcd\xb4b\xdd\xcb\xf2\x939\x0b\xec\xf2'
```