密码学第三次实验报告

# 仿射密码

## 原理

仿射密码是利用模加法和模乘法的原理实现的，对明文按字母加密得到密文。

可以把26个字母按字母顺序映射到0~25这26个数字中。设明文字母为，密文字母为，明文字母和密文字母都在中。密钥为乘法的因数和加法的加数，记为。加密算法为，解密算法为。为了保证密码的保密性，必须存在模26的逆元，这样才能够从密文中恢复明文。

## 算法

### 加密算法

**def** encrypt(s: str, k: Tuple[int]) -> str:

result = s

对 result 中的每个字符：

对应的字母

**return** result

### 解密算法

**def** decrypt(s: str, k: Tuple[int]) -> str:

result = s

对 result 中的每个字符：

对应的字母

**return** result

## 分析

设明文或者密文长度为。

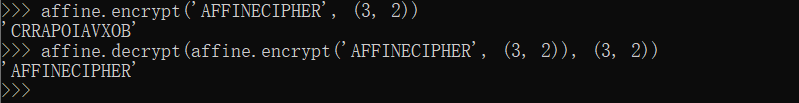
### 加密算法

该算法中对每个字符都要进行一次模加法和模乘法运算，复杂度为。因此整个算法的复杂度为。

### 解密算法

该算法中求模逆元，由于模数26为常数，复杂度为。因此同理，整个算法的复杂度为。

## 测试

令明文为AFFINECIPHER，密钥为，得到密文CRRAPOIAVXOB。用同一密钥解密，能够恢复出明文。经过验算，结果正确。

# Vigenère密码

## 原理

Vigenère密码类似仿射密码，同样是对明文按字母加密，而且把字母映射到数字的方式也与仿射密码相同。

设明文为，密文为，密钥为，它们都是字符串。设，，分别为，，在索引处的字符，索引从开始。设长度为，对，定义。这样实际上使可以无限循环。

加密算法为对所有小于长度的，。解密算法为对所有小于长度的，。

## 算法

### 加密算法

**def** encrypt(s: str, k: str) -> str:

result = s

对中每个整数：

对应的字母

**return** result

### 解密算法

**def** decrypt(s: str, k: str) -> str:

result = s

对中每个整数：

对应的字母

**return** result

## 分析

设明文或者密文长度为。

### 加密算法

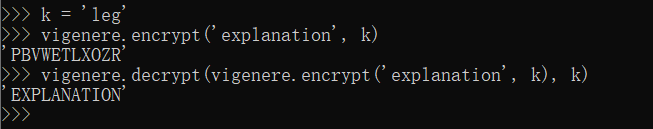
该算法中对每个字符都要进行一次模加法运算，复杂度为。因此整个算法的复杂度为。

### 解密算法

类似地，整个算法的复杂度为。

## 测试

令明文为explanation，密钥为leg。得到密文为PBVWETLZOXR。（密文在加密时被自动转换为大写。）用同一密钥解密密文，能得到原来的明文。经过验算，结果正确。



# Vernam密码

## 原理

Vernam密码把原文按二进制位加密。

设明文、密文、密钥分别为、、。明文和密文长度应该相等，设它们的长度为。设，，分别为，，在索引处的二进制位，索引从开始。设长度为，对，定义。这样实际上使可以无限循环。

加密算法为，解密算法为。

## 算法

### 加密算法

**def** encrypt(m: bytes, k: bytes) -> bytes:

对中每个整数:

**return** c

### 解密算法

与加密算法相同

## 分析

设明文和密文的长度为。

### 加密算法

加密算法把原文按位加密，每次异或操作的时间复杂度是。因此时间复杂度为。易知空间复杂度为。

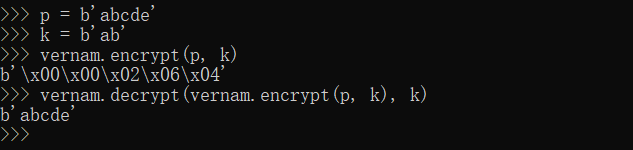
### 解密算法

同理，时间复杂度和空间复杂度分别为和。

## 测试

以下的明文和密文都用C字符串格式表示。

令明文为”abcde”，密钥为”ab”。得到密文为”\x00\x00\x02\x06\x04”。经过解密，能恢复明文。经过验算，结果正确。



## 优化

实际上，Vernam密码如果要在现代计算机上使用，应该考虑到现代计算机大多是以字节为存储数据的基本单位这一特性。因此，可以利用现代处理器的向量指令集（如AVX系列指令集）功能，对Vernam密码进行优化，充分发挥处理器的并行潜能。

# 单表代替密码

## 原理

### 加密

单表代替密码类似仿射密码，同样是对明文按字母加密，而且把字母映射到数字的方式也与仿射密码相同。

令且为双射。这样的一个就可以作为单表代替密码的加密函数。对明文按字母加密，就是把明文的每个字母替换为。

同样地，也可以把单表代替密码的密钥用字母表表示。表示方法为a对应，b对应，……，z对应。

### 解密

把密文的每个字母替换为即可。

### 唯密文攻击算法

由于单表代替密码只是对明文字母进行了简单代替，仍然保留明文的频率特性，因此可以受到基于频率分析的唯密文攻击。通过对明文进行频率统计，可以大大帮助对单表代替密码的破译。

对于判定一个加密密钥的可能性大小，可以通过来判定。设为已知的英文字母理想的频率分布，为密文经过解密后的频率分布。可以假定明文的分布接近英文字母理想的频率分布，这样越低的值，可能性应该越大。这样就可以量化可能性并进行比较。因此，获得前个最有可能的明文就可行了。

在实践上，可以把26个字母分成若干组，分组方式可以有多种，但是要避免概率上差得太大的字母被分成一组。对一种方式来说，每一组应该遍历这组中的所有排列，这样可以避免概率上接近的字母被分错。这样可以做到效率和可行性兼顾。

## 算法

### 加密算法

**def** encrypt(p: str, k: Dict[str, str]) -> str:

对中每个字母:

**return** p

### 解密算法

**def** decrypt(c: str, k: Dict[str, str]) -> str:

对中每个字母:

**return** c

### 唯密文攻击算法

**def** get\_most\_likely\_plaintext(c: str, n: int) -> list:

通过词频分析的方法求出密文原始概率分布，利用英语字母频率规律求出基础分布

result = []

\_letter\_freq\_groups\_list = \

[['E', 'TAO', 'INSHR', 'DL', 'CU', 'MWFG', 'YP', 'BVK', 'JXQZ'],

['E', 'TAO', 'INSHR', 'DL', 'CU', 'MWF', 'GYP', 'BVK', 'JXQZ'],

['E', 'TAO', 'INSHR', 'DL', 'CU', 'MW', 'FGYP', 'BVK', 'JXQZ'],

['E', 'TAO', 'INSHR', 'DL', 'CU', 'MWFG', 'YPB', 'VK', 'JXQZ'],

['E', 'TAO', 'INSHR', 'DL', 'CU', 'MWF', 'GYPB', 'VK', 'JXQZ'],

['E', 'TAO', 'INSHR', 'DL', 'CU', 'MW', 'FGYPB', 'VK', 'JXQZ']]

对中的每个分组方案:

对该分组方案中对每个组内字母进行排列的每个变形:

将基础分布中每个字母对应的密文字母按照该变形中的响应顺序映射成新字母，得到新映射，在作用下的明文的频率分布

把放入大小为的堆中，若堆长度超过，则去掉最大的元素

对队列中的每个:

试图解密并放入result中

**return** result

## 分析

设密文长度为，加密映射为，要找的最有可能的密文个数为。

### 加密算法

由于是给定的，实际上可以通过建立缓存使加密每个字母的时间复杂度为。因此，总的时间复杂度为。易知空间复杂度为。

### 解密算法

类似地，易知时间复杂度为，空间复杂度为。

### 唯密文攻击算法

所有的变形数可以求出来，生成所有的变形的时空复杂度可以看成。由于字母个数一定，求新的频率分布和的时空复杂度也可以看成。翻入堆中并及时删除的操作，时间复杂度是，空间复杂度是。然后由于每次解密时间复杂度为，空间复杂度为，所以可以看出，次解密的时间复杂度为，空间复杂度为（因为每次解密需要保存密文，而不是就地解密）。因此总时间复杂度为，总空间复杂度为。

## 测试

选择明文为

WinstonkepthisbackturnedtothetelescreenItwassaferthoughashewellknewevenabackcanberevealingAkilometreawaytheMinistryofTruthhisplaceofworktoweredvastandwhiteabovethegrimylandscapeThishethoughtwithasortofvaguedistastethiswasLondonchiefcityofAirstripOneitselfthethirdmostpopulousoftheprovincesofOceaniaHetriedtosqueezeoutsomechildhoodmemorythatshouldtellhimwhetherLondonhadalwaysbeenquitelikethisWeretherealwaysthesevistasofrottingnineteenthcenturyhousestheirsidesshoredupwithbaulksoftimbertheirwindowspatchedwithcardboardandtheirroofswithcorrugatedirontheircrazygardenwallssagginginalldirectionsAndthebombedsiteswheretheplasterdustswirledintheairandthewillowherbstraggledovertheheapsofrubbleandtheplaceswherethebombshadclearedalargerpatchandtherehadsprungupsordidcoloniesofwoodendwellingslikechickenhousesButitwasnousehecouldnotremembernothingremainedofhischildhoodexceptaseriesofbrightlittableauxoccurringagainstnobackgroundandmostlyunintelligibleTheMinistryofTruthMinitrueinNewspeakNewspeakwastheofficiallanguageofOceaniaForanaccountofitsstructureandetymologyseeAppendixwasstartlinglydifferentfromanyotherobjectinsightItwasanenormouspyramidalstructureofglitteringwhiteconcretesoaringupterraceafterterracemetresintotheairFromwhereWinstonstooditwasjustpossibletoreadpickedoutonitswhitefaceinelegantletteringthethreeslogansofthePartyWARISPEACEFREEDOMISSLAVERYIGNORANCEISSTRENGTH

密钥为：

abcdefghijklmnopqrstuvwxyz

qwertyuiopasdfghjklzxcvbnm

加密后的密文为：

VOFLZGFATHZIOLWQEAZXKFTRZGZITZTSTLEKTTFOZVQLLQYTKZIGXUIQLITVTSSAFTVTCTFQWQEAEQFWTKTCTQSOFUQAOSGDTZKTQVQNZITDOFOLZKNGYZKXZIIOLHSQETGYVGKAZGVTKTRCQLZQFRVIOZTQWGCTZITUKODNSQFRLEQHTZIOLITZIGXUIZVOZIQLGKZGYCQUXTROLZQLZTZIOLVQLSGFRGFEIOTYEOZNGYQOKLZKOHGFTOZLTSYZITZIOKRDGLZHGHXSGXLGYZITHKGCOFETLGYGETQFOQITZKOTRZGLJXTTMTGXZLGDTEIOSRIGGRDTDGKNZIQZLIGXSRZTSSIODVITZITKSGFRGFIQRQSVQNLWTTFJXOZTSOATZIOLVTKTZITKTQSVQNLZITLTCOLZQLGYKGZZOFUFOFTZTTFZIETFZXKNIGXLTLZITOKLORTLLIGKTRXHVOZIWQXSALGYZODWTKZITOKVOFRGVLHQZEITRVOZIEQKRWGQKRQFRZITOKKGGYLVOZIEGKKXUQZTROKGFZITOKEKQMNUQKRTFVQSSLLQUUOFUOFQSSROKTEZOGFLQFRZITWGDWTRLOZTLVITKTZITHSQLZTKRXLZLVOKSTROFZITQOKQFRZITVOSSGVITKWLZKQUUSTRGCTKZITITQHLGYKXWWSTQFRZITHSQETLVITKTZITWGDWLIQRESTQKTRQSQKUTKHQZEIQFRZITKTIQRLHKXFUXHLGKROREGSGFOTLGYVGGRTFRVTSSOFULSOATEIOEATFIGXLTLWXZOZVQLFGXLTITEGXSRFGZKTDTDWTKFGZIOFUKTDQOFTRGYIOLEIOSRIGGRTBETHZQLTKOTLGYWKOUIZSOZZQWSTQXBGEEXKKOFUQUQOFLZFGWQEAUKGXFRQFRDGLZSNXFOFZTSSOUOWSTZITDOFOLZKNGYZKXZIDOFOZKXTOFFTVLHTQAFTVLHTQAVQLZITGYYOEOQSSQFUXQUTGYGETQFOQYGKQFQEEGXFZGYOZLLZKXEZXKTQFRTZNDGSGUNLTTQHHTFROBVQLLZQKZSOFUSNROYYTKTFZYKGDQFNGZITKGWPTEZOFLOUIZOZVQLQFTFGKDGXLHNKQDORQSLZKXEZXKTGYUSOZZTKOFUVIOZTEGFEKTZTLGQKOFUXHZTKKQETQYZTKZTKKQETDTZKTLOFZGZITQOKYKGDVITKTVOFLZGFLZGGROZVQLPXLZHGLLOWSTZGKTQRHOEATRGXZGFOZLVIOZTYQETOFTSTUQFZSTZZTKOFUZITZIKTTLSGUQFLGYZITHQKZNVQKOLHTQETYKTTRGDOLLSQCTKNOUFGKQFETOLLZKTFUZI

计算前10个可能的密文，结果如下：

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

AZUSBVUOQFBKZSYJTOBMNUQLBVBKQBQIQSTNQQUZBAJSSJWQNBKVMEKJSKQAQIIOUQAQXQUJYJTOTJUYQNQXQJIZUEJOZIVRQBNQJAJGBKQRZUZSBNGVWBNMBKKZSFIJTQVWAVNOBVAQNQLXJSBJULAKZBQJYVXQBKQENZRGIJULSTJFQBKZSKQBKVMEKBAZBKJSVNBVWXJEMQLZSBJSBQBKZSAJSIVULVUTKZQWTZBGVWJZNSBNZFVUQZBSQIWBKQBKZNLRVSBFVFMIVMSVWBKQFNVXZUTQSVWVTQJUZJKQBNZQLBVSPMQQHQVMBSVRQTKZILKVVLRQRVNGBKJBSKVMILBQIIKZRAKQBKQNIVULVUKJLJIAJGSYQQUPMZBQIZOQBKZSAQNQBKQNQJIAJGSBKQSQXZSBJSVWNVBBZUEUZUQBQQUBKTQUBMNGKVMSQSBKQZNSZLQSSKVNQLMFAZBKYJMIOSVWBZRYQNBKQZNAZULVASFJBTKQLAZBKTJNLYVJNLJULBKQZNNVVWSAZBKTVNNMEJBQLZNVUBKQZNTNJHGEJNLQUAJIISSJEEZUEZUJIILZNQTBZVUSJULBKQYVRYQLSZBQSAKQNQBKQFIJSBQNLMSBSAZNIQLZUBKQJZNJULBKQAZIIVAKQNYSBNJEEIQLVXQNBKQKQJFSVWNMYYIQJULBKQFIJTQSAKQNQBKQYVRYSKJLTIQJNQLJIJNEQNFJBTKJULBKQNQKJLSFNMUEMFSVNLZLTVIVUZQSVWAVVLQULAQIIZUESIZOQTKZTOQUKVMSQSYMBZBAJSUVMSQKQTVMILUVBNQRQRYQNUVBKZUENQRJZUQLVWKZSTKZILKVVLQCTQFBJSQNZQSVWYNZEKBIZBBJYIQJMCVTTMNNZUEJEJZUSBUVYJTOENVMULJULRVSBIGMUZUBQIIZEZYIQBKQRZUZSBNGVWBNMBKRZUZBNMQZUUQASFQJOUQASFQJOAJSBKQVWWZTZJIIJUEMJEQVWVTQJUZJWVNJUJTTVMUBVWZBSSBNMTBMNQJULQBGRVIVEGSQQJFFQULZCAJSSBJNBIZUEIGLZWWQNQUBWNVRJUGVBKQNVYDQTBZUSZEKBZBAJSJUQUVNRVMSFGNJRZLJISBNMTBMNQVWEIZBBQNZUEAKZBQTVUTNQBQSVJNZUEMFBQNNJTQJWBQNBQNNJTQRQBNQSZUBVBKQJZNWNVRAKQNQAZUSBVUSBVVLZBAJSDMSBFVSSZYIQBVNQJLFZTOQLVMBVUZBSAKZBQWJTQZUQIQEJUBIQBBQNZUEBKQBKNQQSIVEJUSVWBKQFJNBGAJNZSFQJTQWNQQLVRZSSIJXQNGZEUVNJUTQZSSBNQUEBK

## 优化

### 加密算法

单表代替密码加密算法的一个典型的优化就是查表，也就是先把所有的函数值求出来。

### 解密算法

类似地，一个典型的优化也是查表。

### 唯密文攻击算法

实际上，唯密文攻击是需要遍历几乎所有密钥的，这也是一种典型的穷举攻击。但是，如果原文是比较长的、相对地道的英文，那密文有很大概率也会大体上重复英语字母的频率分布，只是字母不同罢了。实际上，由于英语字母可以按照出现频率的等级大致分成几块，所以密文中的字母也是如此，真正需要遍历的密钥并不多。实际上，密文按字母出现频率也可以分成几块，每块与明文的相应的块对应。因此只需要在块内进行变换，就基本上能做到很好地解密出明文。

但是，实际上，对不同类型的密文，需要的块的分法也是不一样的。因此，需要预置几种不同的块的分法以满足需要。同时，块不能过大，因为求出一个长度为的序列的全排列，时间复杂度至少是级别的，因此小块加多种分割方法是一个比较好的办法。

在一个长度为的序列中，求前个最小项或最大项是一个经典的问题，这里用堆来解决，是目前比较好的通用的算法，而且是一种在线算法，因此规避了存储整个序列带来的时空复杂度。对序列全排序，时间复杂度和空间复杂度分别是和（假设使用快速排序等较优秀的算法），显然不如堆方法快、省空间。

# Hill密码

## 原理

Hill密码是采用矩阵模乘的原理进行的。设矩阵维数为，明文为，密文为，密钥为，字母个数为。明文应该按每个字母进行分组，并转换为数字，每一组的数字以列向量形式表示。设明文和密文的第个分组分别为和。如果明文仅由字母组成，可以都转换成大写字母，并按照类似于仿射密码的字母转数字方法转换，此时。如果明文的长度不能被整除，可以对明文进行填充。

加密算法为，解密算法为。为了保证密码的保密性，必须模可逆。求行列式的算法由给出，其中为去掉后的代数余子式。若为1行1列的方阵，则。这样就能递归地给出求在模下的行列式的算法，同时也能知道模可逆的充要条件是。这样，也能给出求的算法，求的公式为。同样地，求的算法也是递归的。

Hill密码无法抵抗已知明文攻击，因为它的算法是线性的，密文和密钥的关系太明确了。只要知道对在模意义下线性无关的明密文对，就可以进行已知明文攻击，算出。可以把这些明密文对当成列向量，按顺序对应地排成两个方阵和。这样，由，可以得到，于是就算出了。

## 算法

### 加密算法

**def** encrypt(p: str, k: modular\_matrix.ModularMatrix) -> str:

把分成各分组，在分组时进行必要的填充

对所有有意义的:

**return** c

### 解密算法

**def** encrypt(c: str, k: modular\_matrix.ModularMatrix) -> str:

把分成各分组，在分组时进行必要的填充

对所有有意义的:

**return** p

### 已知明文攻击算法

**def** get\_key(c: str, p: str, m: int) -> modular\_matrix.ModularMatrix:

把和分成若干组，称为和

若组数小于:

返回错误

，

**while** **True:**

若可逆:

**return** K

否则:

若不存在序号更大的和**:**

返回错误

否则:

取下一个合法的值

把和放到和的第列上

若:

## 分析

设明文长度为，方阵行数为。不妨设整除。

### 加密算法

加密算法中明文一共有组，每组首先转化为矩阵，并使用通用的矩阵乘法算法进行加密。这样对每组明文，矩阵模乘法的时间复杂度为，空间复杂度为（用来存储密钥），但每组明文使用的密钥相同。这样总时间复杂度为，空间复杂度为。

### 解密算法

解密算法中用进行矩阵乘法得到明文与加密算法步骤实际上一样，因此重点在求上。

对于计算的算法，可以设对阶方阵，需要的时间和空间分别为和。这样，。因此可以递推求出算法的时间复杂度为，空间复杂度为。对计算，可以看出需要次求，因此时间复杂度为，注意到每次求的空间不需要重复使用，因此空间复杂度为。

这样就可以得到算法的总时间复杂度为，总空间复杂度为。

### 已知明文攻击算法

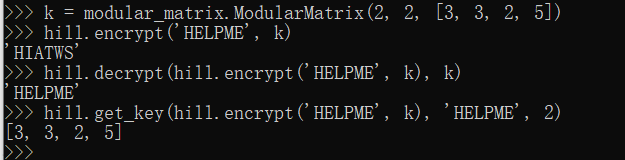
将明密文对分组需要的时间复杂度是，由于在实践中不一定要真的花费空间来分组，因此空间复杂度为。

构造矩阵需要的空间复杂度易知是。最坏情况是明密文对中每一组都参与运算，因此需要的时间复杂度为。此时要做次矩阵求逆，因此在求逆操作上的时间复杂度为。注意到每次空间不需要重复使用，因此空间复杂度为。

因此算法的总时间复杂度为，总空间复杂度为。

## 测试

令，明文为HELPME，进行测试。得到密文为，用解密后能恢复出明文。密文能满足分组后线性无关的条件，经过已知明文攻击后得到原来的。经过验算，结果正确。



## 优化

### 加密算法

由于加密算法是矩阵算法，同样也可以利用现代处理器的向量指令集进行优化，充分发挥处理器的并行潜力。

### 解密算法

解密算法算出后的主要步骤跟加密算法原理相同，优化方法也相似。

计算是一个可以优化的地方。实际上，可以把计算时算出的那些保存，这样虽然不能降低后面计算时的复杂度级别，但是也能缩短程序的运行时间。也似乎可以在计算时，利用类似高斯消元法的方法，这样能大大降低算法的时间复杂度，但是我没有尝试，因为现在的算法在现代的计算机上对时的情况，计算量并不大。

其实也可以用逻辑删除的方法来降低计算的空间复杂度，但这种优化并不实用，因为普通算法的时间复杂度已经很高了，这种方法还会再提高，因为每层递归要把个元素再扫一遍。

当然，计算各也可以用并行的方法。

### 已知明文攻击算法

已知明文攻击算法，主要是要找出一组明文分组，使它们在模的意义下线性无关。暴力穷举需要的时间复杂度，并不实用。直接判断除了高斯消元法，我也想不出太好的方法。于是在我的算法中，我想出了一种利用滑动窗口来进行线性无关判断的方法。如果一组分组向量在模的意义下线性相关，就滑向下一个，继续寻找。但是这种方法的缺点是若一组线性无关的向量相隔较远，就无法找到了。

其实有一种改进的方法，是知道线性相关后，尽量找出更多的向量使其线性无关。但是这时线性相关没有很好的判别方法（除了用更小维度的方阵），还会加大算法的复杂度，况且滑动窗口算法实现更简单、性能更优秀、对随机明文的效果似乎和这种算法不相上下，因此我还是采用了滑动窗口算法。

# 心得体会

## 古典密码

古典密码体制主要是依据字母本身来进行加解密运算，除了Vernam密码以外，都不是针对二进制位的。这导致了明文中字母及其分布本身就保留的信息，通常会传播到密文中。而且古典密码体制的扩散和混淆，通常不会都做得非常好。因此，古典密码基本上都难以抵抗已知明文攻击，但现代的密码最基本的要求就是能够抵抗已知明文攻击，因此古典密码在现在是不实用的。

古典密码学习的意义并不是拿它来加密，而是弄清楚密码学作为一个学科的发展脉络。古典密码的重要性在于它提供了现代密码体制的基本要求：扩散和混淆。扩散是为了模糊明文和密文之间的关系，混淆是为了模糊密文和密钥之间的关系。扩散和混淆的概念，其实分别是有利于抵抗频率分析和已知明文攻击的。虽然攻击现代密码体制，有许多新的办法，比如模攻击、滑动攻击等，但是扩散和混淆仍然是现代密码体制的基础。

### 仿射密码

仿射密码主要是采用了数论知识，也能在其中发现一些密码学的经典原理。

### Vigenère密码

Vigenère密码是一种非常有名的多表代替密码，而且比较早地提出了绝对安全的一次一密密码体制。但是多表代替仍然会受到扩散不足的困扰，因为Vigenère密码是按字母加密的。

### Vernam密码

Vernam密码其实是二进制流版本的Vigenère密码，但是比Vigenère密码更难破译，因为二进制流更难进行统计分析，而且长度可以做得很长。它的扩散也是不足的，但是对密码安全性的影响弱些，因为不像字母，通过二进制位更难发现规律。它也能实现绝对安全的一次一密密码体制。

### 单表代替密码

单表代替密码实际上在这里指的意思偏狭义。这种密码其实是Caesar密码和仿射密码的演进，但是仍然不能做到扩散，仍然可以通过对密文的统计分析来破译。其实只用计算机做到唯密文攻击，仍然有些粗糙，可以部分归结到计算机没有语言学家对单表代替密码分析的经验和直觉。

### Hill密码

Hill密码是这几种古典加密体制中最先进的。它做到了良好的扩散，到现在都难以进行唯密文攻击（最好的结果好像是的指数级别的）。但是它没有做好混淆，导致它很容易被已知明文攻击攻破，通过选择明文攻击更是可以直接恢复出密钥。比起另外四种古典密码，它更体现出了这三种古典密码的另一面。

## 算法评估与优化

### 加解密算法

实际上，加解密算法在我有限的知识里看来，确实比较成熟、明确，没有什么优化的空间，除了能够并行以外。但是我个人的眼界毕竟非常有限，可能加解密算法能够突破的时间复杂度限制，找到新的方法。

### 单表代替密码的唯密文攻击算法

唯密文攻击主要是要找到一个目标概率分布与求出的概率分布之间的差的度量。度量差值有很多方法，但是由于这是分布与分布的差，我的一个想法是使用来度量。其实这种分析方法是基于一个假定：密文的字母频率分布与理想英文的字母频率分布数值差不多，只是字母不同。这种假定在足够地道的英文文本中基本上都是能实现的。

唯密文攻击算法实际上多少有点艺术的性质，但是计算机没有人的直觉，所以只能让它数据量很大地计算待评估的密文，因此在这一领域，算法优化非常重要。

实际上唯密文攻击也可以发挥现代计算机体系架构的并行性进行计算，因为各字母变换之间没有数据依赖。

取前个可能的明文也可以利用类似堆的数据结构进行优化。

### Hill密码的已知明文攻击算法

已知明文攻击，关键是找出个模线性无关的明密文对，这是算法的一个关键点。这个领域也是算法优化的重点。我没有找到充要条件，但是可以找到一个较快而且适应性较强的算法。

还有一个需要计算的地方是计算逆矩阵。计算逆矩阵，常规方法时空复杂度都不小，但是可能可以用高斯消元法计算，这样能大大降低时空复杂度，但是可能这种方法并不对。

## 系统设计与维护

这次我还是像上次一样进行系统设计，这种系统设计也能提供较好的可维护性。

## 对课程的建议

这次课上的节奏明显快了许多，我感觉我和我的几个朋友也能快速进入状态、高效编程了；同时有些对原理不很清楚的同学也能提问。

我感觉下次应该开始写现代对称密码了，比如AES和DES。我觉得书上讲得非常简明，可以把每次的原理标注上书上的页码，这样更能方便我们高效地完成实验。

## 总结

这次密码学实验我感觉越来越走上正轨了，我也感觉对古典密码算法有了更深的理解。我同时也更有信心面对接下来的挑战。