Problem_AN

Julius Caesar (100 BC – 44 BC), used a character substitution scheme to send hidden messages to his commanders and allies. This encoding scheme, known as the Caesar cipher, was still in active military use until less than a century ago. In this coding scheme, every character in the original message (plaintext) is replaced by the character that cyclically occurs a fixed number of positions later along the alphabet to create a coded message (ciphertext).

The Caesar cipher uses a secret integer known as the “key”, where $0 \leq key \leq 25$. The key determines the number of positions to shift forward along the alphabet to get ciphertext from plaintext. The reverse operation of decoding requires an equal shift but in the opposite direction.

For encoding, key value of 0 implies no shift, that is, the plaintext is the same as the ciphertext. The key value of 3 implies a shift three positions forward, that is, A is encoded as D, …, W as Z and Z as C. The key value of 25 implies a shift twenty five positions forward, that is, A is encoded as Z, …, Y as X and Z as Y. This is the same as a shift one position backward, because $-1 \equiv 25 \pmod{26}$,. Under ordinary conditions, the secret key is expected to be known only to those who are authorized to have access to the plaintext. However, Caesar cipher is no longer considered to be safe as the ciphertext can easily be broken by trying all 26 possible keys. Once broken, the secret key used by the communicating parties can also be recovered that not only allows access to the plaintext for that message but also compromises any future communication that uses the same key.

Task

An antisocial organization, who call themselves “Caesar’s Army” conducts

planned and coordinated attacks on nonprofit websites. They have devised a variation of the Caesar cipher to hide the information they exchange from law enforcement. The investigating agencies have learnt that the scheme used by this organization has four closely guarded secret integers – blockLength, k1, k2 and k3, where $1 \leq \text{blockLength} \leq 10$ and the variables k1, k2 and k3 carry the same meaning as the key in Caesar Cipher explained above.

The members of the Caesar's Army convert numerals in the message to words (eg. "200" to numeral "two hundred"), remove all whitespace characters, special symbols, punctuation marks, etc. from the message and then convert the resulting text to UPPERCASE. For all our purposes, this is the plaintext that consists only of UPPERCASE characters in the alphabet (A – Z). This plaintext is then divided into blocks of size blockLength, except the last block which only consists of the remainder of the characters. For example, if the plaintext has 20 characters and blockLength is 3, it is divided into seven blocks – first six with three characters each and the last block with remaining two characters. These blocks are then coded using Caesar cipher – first block with key k1, the second block with k2, the third block with k3, the fourth block again with k1, fifth with k2 and so on. The ciphertext also uses UPPERCASE characters only.

The investigating agencies have intercepted a ciphertext message exchanged recently. They also have access to a dictionary that consists of all words that may possibly be used in the plaintext – no word in the plaintext is outside this dictionary. They are willing to share this information with you and need your help in determining the values of the four secret integers and in recovering the plaintext as soon as possible – well in time to thwart the launch of the next attack that this message may be about!

Input

The input shall always be 4 lines received by the standard input stream as follows:

```
1. The first line will be the cyphered text
2. Then a blank line should follow
3. The third line should be the number of words contained in the dictionary
4. The final line of the input will be the words contained in the dictionary,
 each word separated by the next one by a white space character. The last wor
d of the dictionary does not have a white space character at the end
```

Note:
All four pieces of the input start on a new line.

Output

The output should contain values of the secret integers and the plaintext in the following order:

```
blockLength
k1
k2
k3
Plaintext
```

Note:

The output ends with a newline character.

Sample Input

```
ZVVVZBCQNFJMGYNCRIXVBCYAXAZNNDFERCRBBXLRVODJIUVUZTJCNMCJVYQVETZEXCNLQWJGJBDTR
CZEWXEJCDJIVIUVOTVUUNWLZAJMOYVSVENORCXACPHVEZKPCNCDBYGVIOJRKKRTTCQNRZZZRZSJZK
V

500
A ABLE ABOUT ABOVE ACT ADD ADVANCING AFTER AGAIN AGAINST AGE AGO AIR ALL ALSO
 ALWAYS AM AN AND ANIMAL ANSWER ANY APPEAR ARE AREA AS ASK ASSOCIATION AT ATT
ACK BACK BASE BE BEAUTY BEEN BEFORE BEGAN BEGIN BEHIND BENEFIT BEST BETTER BE
TWEEN BIG BIRD BLACK BLUE BOAT BODY BOOK BOTH BOX BOY BROUGHT BUILD BUSY BUT
BY CALL CAME CAN CAR CARE CARRY CAUSE CENTER CERTAIN CHANGE CHECK CHILDREN CI
TY CLASS CLEAR CLOSE COLD COLOR COME COMMON COMPLETE CONTAIN CORRECT COULD CO
UNTRY COURSE COVER CROSS CRY CUT DARK DAY DECIDE DEDICATED DEEP DEVELOP DID D
IFFER DIRECT DO DOES DOG DONT DONE DOOR DOWN DRAW DRIVE DRY DURING EACH EARLY
 EARTH EASE EAT END ENOUGH EVEN EVER EVERY EXAMPLE EXCELLENCE EYE FACE FACT F
ALL FAMILY FAR FARM FAST FATHER FEEL FEET FEW FIELD FIGURE FINAL FIND FINE FI
RE FIRST FISH FIVE FLY FOLLOW FOOD FOOT FOR FORCE FORM FOUND FOUR FREE FRIEND
 FROM FRONT FULL GAME GAVE GET GIRL GIVE GO GOLD GOOD GOT GOVERN GREAT GREEN
GROUND GROUP GROW HAD HALF HAND HAPPEN HARD HAS HAVE HE HEAD HEAR HEARD HELP
HER HERE HIGHHIM HIS HOLD HOME HORSE HOT HOUR HOUSE HOW HUMANITY HUNDRED I ID
EA IEEE IF IN INCH INNOVATION INTEREST IS ISLAND IT JUST KEEP KIND KING KNEW
KNOW LAND LARGE LARGEST LAST LATE LAUGH LAY LEAD LEARN LEAVE LEFT LESS LET LE
TTER LIFE LIGHT LIKE LINE LIST LISTEN LITTLE LIVE LONG LOOK LOT LOVE LOW MACH
INE MADE MAIN MAKE MAN MANY MAP MARK MAY ME MEAN MEASURE MEN MIGHT MILE MIND
MINUTE MISS MONEY MOON MORE MORNING MOST MOTHER MOUNTAIN MOVE MUCH MUSIC MUST
 MY NAME NEAR NEED NEVER NEW NEXT NIGHT NO NORTH NOTE NOTHING NOTICE NOUN NOW
 NUMBER NUMERAL OBJECT OF OFF OFTEN OH OLD ON ONCE ONE ONLY OPEN OR ORDER OTH
ER OUR OUT OVER OWN PAGE PAPER PART PASS PATTERN PEOPLE PERSON PICTURE PIECE
PLACE PLAIN PLAN PLANE PLANT PLAY POINT PORT POSE POSSIBLE POUND POWER PRESS
PROBLEM PRODUCE PRODUCT PROFESSIONAL PULL PUT QUESTION QUICK RAIN RAN REACH R
EAD READY REAL RECORD RED REMEMBER REST RIGHT RIVER ROAD ROCK ROOM ROUND RULE
 RUN SAID SAME SAW SAY SCHOOL SCIENCE SEA SECOND SEE SEEM SELF SENTENCE SERVE
 SET SEVERAL SHE SHIP SHORT SHOULD SHOW SIDE SIMPLE SINCE SING SIX SIZE SLEEP
 SLOW SMALL SO SOME SONG SOON SOUND SOUTH SPECIAL SPELL STAND STAR START STAT
E STAY STEP STILL STOOD STOP STORY STREET STRONG STUDY SUCH SUN SURE SURFACE
TABLE TAIL TAKE TALK TEACH TECHNOLOGICAL TELL TEN TEST THAN THAT THE THEIR TH
EM THEN THERE THESE THEY THING THINK THIS THOSE THOUGH THOUGHT THOUSAND THREE
 THROUGH TIME TO TOGETHER TOLD TOO TOOK TOP TOWARD TOWN TRAVEL TREE TRUE TRY
TURN TWO UNDER UNIT UNTIL UP US USE USUAL VERY VOICE VOWEL WAIT WALK WANT WAR
 WARM WAS WATCH WATER WAY WE WEBSITE WEEK WELL WENT WERE WEST WHAT WHEEL WHEN
 WHERE WHICH WHILE WHITE WHO WHOLE WHY WILL WIND WITH WONDER WOOD WORD WORK W
ORLD WORLDS WOULD WRITE YEAR YET YOU YOUNG YOUR
```

Sample Output

```
5
17
9
21
IEEEISTHEWORLDSLARGESTPROFESSIONALASSOCIATIONDEDICATEDTOADVANCINGTECHNOLOGICA
LINNOVATIONANDEXCELLENCEFORTHEBENEFITOFHUMANITYLETUSPLANTOATTACKTHEIEEEWEBSIT
E
```

Note:
If you copy and paste the dictionary words into your program while testing, please make sure that you have removed any additional white spaces and newline characters that might appear due to the copy and paste (if any).

Problem Author: IEEE

Suggest Edits

Emacs | Normal | Vim

Select Language: Java

save code

```
1  import java.io.*;
2  import java.util.*;
3  import java.text.*;
4  import java.math.*;
5  import java.util.regex.*;
6
7  public class Solution {
8
9      public static void main(String[] args) {
10         /* Enter your code here. Read input from STDIN. Print output to STDOUT. Your class
   should be named Solution. */
11     }
12 }
```

Line: 1 Col: 1 Count: 302

Use a custom test case

Upload Code as File

Compile & Test | Submit Code