Problem A. Code de César

Input file:	`standard input`
Output file:	`standard output`
Time limit:	1 second
Memory limit:	256 megabytes

Comme vu en cours, le code de César est une technique d'encryption qui permets de cacher des messages secrets en décalant chaque lettre d'un certain intervalle. Votre but est d'effectuer soit une encryption soit une décryption avec le décalage donné.

Input

La première ligne d'entrée consiste en un string soit "ENCRYPTER" soit "DECRYPTER".

La deuxième ligne d'entrée contient une lettre $\in$ {"A", "B", ..., "Z"} la taille du décalage.

La troisième ligne d'entrée contient une chaine de caractère s $(1 \leq |s| \leq 10^4)$

Output

Vous devez imprimer une chaîne de caractères correspondant soit à l'encryption soit à la décryption du mot donné.

Examples

standard input	standard output
ENCRYPTER L ALAN TURING	LWLY EFCTYR
DECRYPTER L LWLY EFCTYR	ALAN TURING

Problem B. Code de César - Partie 2

Input file:	`standard input`
Output file:	`standard output`
Time limit:	1 second
Memory limit:	256 megabytes

Écrivez une fonction qui effectue une analyse des fréquences de la chaîne cryptée pour retrouver le texte d'origine. Pour cela, vous aurez besoin des ingrédients suivants :

1. le calcul des fréquences (en pourcentages) de chaque lettre du texte crypté, à enregistrer dans une liste `frequences_empiriques`

2. la comparaison, pour chaque décalage, avec les fréquences théoriques des lettres dans la langue française :

`frequences_theoriques = [8.4, 1.06, 3.03, 4.18, 17.26, 1.12, 1.27, 0.92, 7.34, 0.31, 0.05, 6.01, 2.96, 7.13, 5.26, 3.01,0.99, 6.55, 8.08, 7.07, 5.74, 1.32, 0.04, 0.45, 0.3, 0.12]`

3. et la sélection du décalage qui minimise la différence entre les deux listes (au fait, vous avez plusieurs choix pour calculer cette différence : nous vous laissons réfléchir comment faire au mieux...)

Input

Une ligne qui contient des mots français encodés, chacun séparé par un espace. (Chaque mot fait au plus 25 lettres, entièrement en majuscules, sans accents).

Output

Les mots décodés et séparés par un espace.

Example

standard input	standard output
IB CFRWBOHSIF SGH IBS AOQVWBS EIW DSIH SHFS DFCUFOAASS DCIF STTSQHISF OIHCAOHWEISASBH RSG GSEISBQSG R CDSFOHWCBG OFWHVASHWEISG CI ZCUWEISG ZSG CFRWBOHSIFG SZSQHFCBWEISG BIASFWEISG ACRSFBSG DSIJSBH STTSQHISF RSG SBGSAPZSG USBSFWEISG R CDSFOHWCBG QCBBIG QCAAS DFCUFOAASG QSG DFCUFOAASG DSFASHHSBH OIL CFRWBOHSIFG R SLSQIHSF IBS ZOFUS SJSBHOWZ RS HOQVSG IB GMGHSAS WBTCFAOHWEIS SGH BCAWBOZSASBH IB CFRWBOHSIF QCADZSH EIW QCADFSBR ZS AOHSFWSZ ZS GMGHSAS R SLDZCWHOHWCB SH Z SEIWDSASBH DSFWDVSFWEIS BSQSGGOWFSG SH IHWZWGSG DCIF IB TCBQHWCBBSASBH QCADZSH QS HSFAS DSIH SUOZSASBH GS FSTSFSF O IB UFCIDS ROCFRWBOHSIFG ZWSG SH TCBQHWCBBOBH SBGSAPZS QCAAS IB FSGSOI WBTCFAOHWEIS CI IB QZIGHSF R CFRWBOHSIF	UN ORDINATEUR EST UNE MACHINE QUI PEUT ETRE PROGRAMMEE POUR EFFECTUER AUTOMATIQUEMENT DES SEQUENCES D OPERATIONS ARITHMETIQUES OU LOGIQUES LES ORDINATEURS ELECTRONIQUES NUMERIQUES MODERNES PEUVENT EFFECTUER DES ENSEMBLES GENERIQUES D OPERATIONS CONNUS COMME PROGRAMMES CES PROGRAMMES PERMETTENT AUX ORDINATEURS D EXECUTER UNE LARGE EVENTAIL DE TACHES UN SYSTEME INFORMATIQUE EST NOMINALEMENT UN ORDINATEUR COMPLET QUI COMPREND LE MATERIEL LE SYSTEME D EXPLOITATION ET L EQUIPEMENT PERIPHERIQUE NECESSAIRES ET UTILISES POUR UN FONCTIONNEMENT COMPLET CE TERME PEUT EGALEMENT SE REFERER A UN GROUPE DAORDINATEURS LIES ET FONCTIONNANT ENSEMBLE COMME UN RESEAU INFORMATIQUE OU UN CLUSTER D ORDINATEUR

Note

L'exemple donné contient des sauts à la ligne qui ne sont pas dans le vrai test, pour améliorer la lecture.

Problem C. Le Chiffre de Vigenère

Input file:	`standard input`
Output file:	`standard output`
Time limit:	1 second
Memory limit:	256 megabytes

Vous devez encrypter ou décrypter un texte majuscule avec espaces en suivant le chiffre de Vigenère.

Input

La première ligne d'entrée consiste en un string; soit "ENCRYPTER" soit "DECRYPTER".

La deuxième ligne d'entrée contient un mot en majuscules, de taille ≤ 10; la clé d'encryption.

La troisième ligne d'entrée contient une chaînes de caractères s ($1 \leq |s| \leq 10^3$) — le texte à encrypter ou décrypter.

Output

Une chaîne de caractères correspondant soit à l'encryption soit à la décryption du texte donné.

Examples

standard input	standard output
ENCRYPTER BC UN PETIT TEXTE	VP QGUKU VFZUG
DECRYPTER BC VP QGUKU VFZUG	UN PETIT TEXTE

,

Problem D. Le Chiffre de Vigenère - Partie 2

Input file:	`standard input`
Output file:	`standard output`
Time limit:	1 second
Memory limit:	256 megabytes

Le décryptage du chiffre de Vigenère est plus délicat, notamment parce qu'a priori, on ne connaît pas le nombre de lettres k utilisé pour chiffrer le message.

La première étape consiste donc à estimer ce nombre de lettres k de la clé de Vigenère en utilisant un indice de coïncidence. Pour un texte donné, l'indice de coïncidence du texte est défini ainsi: si $n_A, \ldots, n_Z$ sont les nombres de lettres $A, \ldots, Z$ apparaissant dans le texte et n est le nombre total de lettres du texte (on oublie ici les espaces), alors

$$IC = \sum_{i=A}^{Z} \frac{n_i(n_i - 1)}{n(n-1)}$$

À quoi peut bien servir un tel indice? Pour un texte sans signification composé de lettres tirées complètement au hasard, on peut montrer que IC vaut à peu près 0,0385. Cependant, en français, les lettres sont tout sauf tirées au hasard, et comme on l'a déjà vu, certaines lettres sont bien plus fréquentes que d'autres. Le calcul de IC pour un texte français (avec les fréquences théoriques de l'exercice précédent) donne un nombre bien plus grand, à savoir 0,0746.

Une autre remarque très importante est que l'indice de coïncidence d'un texte chiffré avec un chiffre de César est le même que celui du texte original! En effet, seules comptes les fréquences d'apparition des lettres dans le calcul de IC; peu importe la valeur de ces lettres.

La stratégie de décryptage du chiffre de Vigenère est maintenant la suivante: tous les k caractères, le chiffre de Vigenère utilise le même décalage pour chiffrer une lettre. Ainsi, l'indice de coïncidence du sous-texte composé des lettres numéro $1, k+1, 2k+1, 3k+1, \ldots$ sera identique à celui du français. Idem pour le sous-texte composé des lettres numéro $2, k+2, 2k+2, 3k+2, \ldots$ et ainsi de suite jusqu'au k_e sous-texte composé des lettres numéro $k, 2k, 3k, \ldots$

En calculant pour chaque valeur de k l'indice de coïncidence de chacun des k sous-textes, et en faisant la moyenne de ces indices, on obtient une bonne indication de la longueur k de la clé: c'est celle qui donne le plus grand indice de coïncidence moyen. En effet, si k n'est pas la bonne valeur, chacun des sous-textes ressemblera à un texte écrit au hasard.

Une fois la longueur de la clé k trouvée, il ne reste "qu'à" effectuer l'analyse de l'exercice 1 pour retrouver chacun des k décalages utilisés, et ainsi retrouver le texte d'origine.

Input

L'unique ligne d'entrée contient un texte majuscule sans ponctuation chiffré par le chiffre de Vigenère avec une clé de longueur au plus 10.

Output

Imprimez le texte déchiffré

Example

standard input	standard output
NH FZQOGUKMHX XMK CAK FUTPVTX KLQ CKNN VBEK ILFOEGFGVM CUNL VNSKVNLME GNNFUNZBKLMZKGN UMF YXKLMAIXM U WCKKUKQBTL UIQGNFYKQDAXM FC YUZCHCRY EYJ WEJBHRBRAKM VTRIMLFVVWNYJ VHSXLZYHKL GFLRXGYJ XRAOYEB RLYYTBHKK XVA RTLYDJYKL AVVRXBKLMF J HJVZNZBIEA PUGHLA PUFGV XEUZLRUZKL WVA CXHAIIZSXM GMESXNKMAZ TOO WEJBHRBRAKM U MKKVOKME AGY CIEMX YMMAZTCC LR ZTWYMF AG MPAGKFY ZVSUKGRBVWNY VAG THGZVNRXGVVG AG IILVTTNVCE IHGGTRZ JOZ KBSILVVQ RX GRBRXBYC TR YRMKMZK W YOXYUBNRBVUG YK T RWNCGMZKGN GMEOIBVZVWNY EMPKLMRQEKL YK CGOECJMF VHOI CA LHHTBVUGHVURTM WFUCRXN TM GKKGV XRAM YXIYKFYEB FK KYWMEKK U LV TXHOGM QGHLUQAGMYLZF RBYJ MG LHHTBVUGHRVG KGMVUORX WFUZK NH IMFKTO ZVSUKGRBVWNY FC HT VFLAGKK X FZQOGUKMHX	UN ORDINATEUR EST UNE MACHINE QUI PEUT ETRE PROGRAMMEE POUR EFFECTUER AUTOMATIQUEMENT DES SEQUENCES D OPERATIONS ARITHMETIQUES OU LOGIQUES LES ORDINATEURS ELECTRONIQUES NUMERIQUES MODERNES PEUVENT EFFECTUER DES ENSEMBLES GENERIQUES D OPERATIONS CONNUS COMME PROGRAMMES CES PROGRAMMES PERMETTENT AUX ORDINATEURS D EXECUTER UNE LARGE EVENTAIL DE TACHES UN SYSTEME INFORMATIQUE EST NOMINALEMENT UN ORDINATEUR COMPLET QUI COMPREND LE MATERIEL LE SYSTEME D EXPLOITATION ET L EQUIPEMENT PERIPHERIQUE NECESSAIRES ET UTILISES POUR UN FONCTIONNEMENT COMPLET CE TERME PEUT EGALEMENT SE REFERER A UN GROUPE DAORDINATEURS LIES ET FONCTIONNANT ENSEMBLE COMME UN RESEAU INFORMATIQUE OU UN CLUSTER D ORDINATEUR

Note

Dans l'exemple donné, il y a des sauts de lignes qui ne seront pas dans les cas de tests afin que le tout soit lisible.