Dumas cipher

The Founding Fathers — the founders of the United States of America — used various forms of cipher in their correspondence. Benjamin Franklin, for example, occasionally used a cipher that was developed by Charles Guillaumes Frédéric Dumas, who stayed in the Netherlands during the American Revolution. Because he was a fervent supporter of the American cause, Dumas was asked to spy for the United States, in 1781, Bejamin Franklin wrote a letter from Passy (France) to Dumas, stating the following:

> *I have just received a 14, 5, 3, 10, 28, 2, 76, 203, 66, 11, 12, 273, 50, 14, joining 76, 5, 42, 45, 16, 15, 424, 235, 19, 20, 69, 580, 11, 150, 27, 56, 35, 104, 652, 20, 675, 85, 79, 50, 63, 44, 22, 219, 17, 60, 29, 147, 136, 41, but this is not likely to afford 202, 55, 580, 10, 227, 613, 176, 373, 309, 4, 108, 40, 19, 97, 309, 17, 35, 90, 201, 100, 677.*

For a long time, nobody was able to decipher the text, because even the State Department in Washington didn't possess a key for the cipher. Later, the following French fragment appeared to be the key to decipher:

> *Voulez=vous sentir la difference? Jettez les yeux sur le continent septentrional de l'amerique. Dans les resolutions vigoureuses de ces braves colons vous reconnoitrez la voix de la vraie liberte * aux prises avec l'oppression. Vous fremirez, vous vous revolte= rez contre la morgue & la durete inconcevable de ceux, qui, jaloux a l'extreme de leur propre liberte, pensent de pouvoir devenir plus puissants, de pouvoir rester libres eux=memes en asservissant leurs freres. Vous ne pourrez vous empecher de faire votre cause de celle de ces peuples, de leur savoir gre de leur fermete, de trem= bler qu'ils ne suciombent sous la massue levee du pouvoir, qui veut ou les gouverner arbitrairement, ou les ecraser, en fin de leur sou= haiter avec le genereux d. der. tout le succes possible dans leur juste resistance.*

This passage is copied from the prologue that Dumas had written in a book he had sent to Franklin: *Le droit des gens* (International law) of Emerich de Vattel. Dumas had had this work reprinted with his own prologue and some notes in which the views were applied to the situation in America. In 1775, he sent three copies to Benjamin Franklin.

Assignment

For the Charles Dumas cipher a text fragment is coded as a list of numbers. In order to code and decode, a second text fragment — the **key text** — is used that must be kept a secret at all times. To decode a number n, one must simply search the character on the nth position in the key text. On determining the positions in the key text, white space (spaces, tabs and line endings) are ignored and the first character is on the first position. For the key text "Lost time is never found again." the positions of the characters are for example

positions	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
characters	L	o	s	t	t	i	m	e	i	s	n	e	v	e	r	f	o	u	n	d	a	g	a	i	n	.

In this case, numbers 11, 19 and 25 all represent the letter n. To code the letter n, one can randomly choose between the numbers 11, 19 and 25. For this assignment, however, we will use

a more strict coding scheme. If we have to code a text fragment that contains the letter n multiple times, we will first replace this letter by the number 11, the second time by 19 and the third time by 25. Because the n only occurs on three positions in the key text, we will code the fourth letter n as the number 11, and so on. If we follow this procedure with the example key text above, the word nondeterminativeness will be coded as

karakters	n	o	n	d	e	t	e	r	m	i	n	a	t	i	v	e	n	e	s	s
posities	11	2	19	20	8	4	12	15	7	6	25	21	5	9	13	14	11	8	3	10

On coding the message, characters of the message that don't occur in the key text, may be ignored.

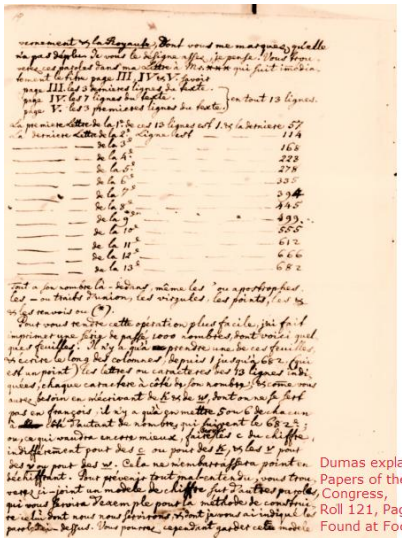
- Write a function cipherkey to which a string must be given that contains the key text. The function must print a dictionary, that portrays every character that occurs in the key text on the list of positions in the key text on which this character occurs. the positions must be listed in increasing order. White space ins the key text must be neglected. The positions of the characters are numbered from 1. The function also may not distinguish between uppercase and lowercase letters, and the uppercase variant of a letter must be used as a key in the dictionary.
- Use the function cipherkey to write a function encode to which two strings must be given: a text fragment that needs to be coded and the key text that must be used to code. The function must code the given text fragment according to the strict code scheme that was mentioned above.

Example

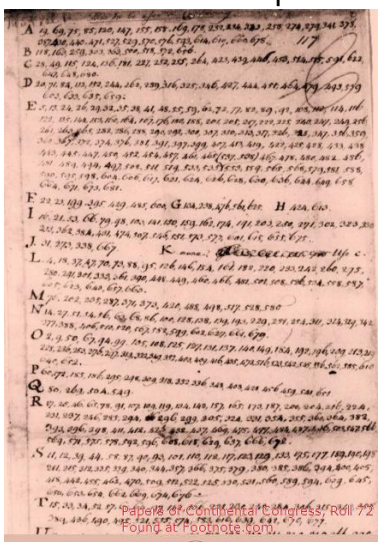
```
>>> keytext = 'Lost time is never found again.'

>>> key = cipherkey(keytext)
>>> key['N']
[11, 19, 25]
>>> key['E']
[8, 12, 14]
>>> key['.']
[26]

>>> encode('nondeterminativeness', keytext)
[11, 2, 19, 20, 8, 4, 12, 15, 7, 6, 25, 21, 5, 9, 13, 14, 11, 8, 3, 10]
>>> encode('interdenominationalism', keytext)
[6, 11, 4, 8, 15, 20, 12, 19, 2, 7, 9, 25, 21, 5, 24, 17, 11, 23, 1, 6, 3, 7]
>>> encode('gastroenteroanastomosis', keytext)
[22, 21, 3, 4, 15, 2, 8, 11, 5, 12, 15, 17, 23, 19, 21, 10, 4, 2, 7, 17, 3, 6, 10]
```

Final number

On 30 April 1776 Alexander Dumas wrote a letter to Benjamin Franklin (head of the *Committee of Secret Correspondence*) in Philadelphia. In his letter he elaborately expressed his gratitude for what he meant to the country, and he also gave a detailed explanation for the cipher he had developed. Becaus K and W aren't used in French, the didn't occur in the key text. For this reason he advises, among other things, using two us instead of a w and a c instead of a k.



Extract from the document *Papers of Continental Congress* (role 121, page 19) in which Charles Dumas explains his cipher.



Extract from the document *Papers of Continental Congress* (role 72) with the code key that can be constructed based on the French text fragment that is given above. This key can be used to decode passages in the message from Franklin to Dumas that was given in our introduction.

With this knowledge, the message in the introduction states:

> *I have just received a* ***neuu comiissjon*** *joining* ***me uuith m adams in negodiaions for peace*** *but this is not likely to afford* ***me much employ at present****.*

Sources

- **Weber RE (2010)**. United States diplomatic codes and ciphers: 1775-1938. *Transaction Publishers*.

De Founding Fathers — de grondleggers van de Verenigde Staten van Amerika — gebruikten in hun correspondentie verschillende vormen van geheimschrift. Zo maakte Benjamin Franklin af en toe gebruik van een geheimschrift dat werd ontwikkeld door Charles Guillaumes Frédéric Dumas, die ten tijde van de Amerikaanse Revolutie in Nederland verbleef. Omdat hij een fervente aanhanger was van de Amerikaanse zaak, werd Dumas gevraagd om te spionneren voor de Verenigde Staten. In 1781 schreef Benjamin Franklin vanuit Passy (Frankrijk) een brief naar Dumas waarin hij het volgende optekende:

> *I have just received a 14, 5, 3, 10, 28, 2, 76, 203, 66, 11, 12, 273, 50, 14, joining 76, 5, 42, 45, 16, 15, 424, 235, 19, 20, 69, 580, 11, 150, 27, 56, 35, 104, 652, 20, 675, 85, 79, 50, 63, 44, 22, 219, 17, 60, 29, 147, 136, 41, but this is not likely to afford 202, 55, 580, 10, 227, 613, 176, 373, 309, 4, 108, 40, 19, 97, 309, 17, 35, 90, 201, 100, 677.*

Lange tijd kon niemand deze tekst ontcijferen, omdat zelfs het State Department in Washington niet over de sleutel voor het geheimschrift beschikte. Later bleek het volgende Franse tekstfragment de sleutel voor de ontcijfering te zijn:

> *Voulez=vous sentir la difference? Jettez les yeux sur le continent septentrional de l'amerique. Dans les resolutions vigoureuses de ces braves colons vous reconnoitrez la voix de la vraie liberte * aux prises avec l'oppression. Vous fremirez, vous vous revolte= rez contre la morgue & la durete inconcevable de ceux, qui, jaloux a l'extreme de leur propre liberte, pensent de pouvoir devenir plus puissants, de pouvoir rester libres eux=memes en asservissant leurs freres. Vous ne pourrez vous empecher de faire votre cause de celle de ces peuples, de leur savoir gre de leur fermete, de trem= bler qu'ils ne suciombent sous la massue levee du pouvoir, qui veut ou les gouverner arbitrairement, ou les ecraser, en fin de leur sou= haiter avec le genereux d. der. tout le succes possible dans leur juste resistance.*

Deze passage is overgenomen uit het voorwoord dat Dumas geschreven had bij een boek dat hij naar Franklin had gestuurd: *Le droit des gens* (Volkenrecht) van Emerich de Vattel. Dumas had dit werk laten herdrukken met zijn eigen voorwoord en opmerkingen waarin de opvattingen werden toegepast op de situatie in Amerika. In 1775 stuurde hij drie exemplaren naar Benjamin Franklin.

Opgave

Bij het geheimschrift van Charles Dumas wordt een tekstfragment gecodeerd als een lijst van getallen. Bij het coderen en decoderen wordt gebruik gemaakt van een tweede tekstfragment — de **sleuteltekst** — die ten allen tijd geheim moet gehouden worden. Om een getal n te decoderen, wordt eenvoudigweg het karakter opgezocht dat op n-de positie staat in de sleuteltekst. Bij het bepalen van posities in de sleuteltekst wordt witruimte (spaties, tabs en regeleindes) genegeerd en staat het eerste karakter op positie 1. Voor de sleuteltekst "Lost time is never found again." zijn de posities van de karakters dan bijvoorbeeld

posities	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
karakters	L	o	s	t	t	i	m	e	i	s	n	e	v	e	r	f	o	u	n	d	a	g	a	i	n	.

In dat geval zien we dat de getallen 11, 19 en 25 allemaal staan voor de letter n. Om de letter n te coderen, kan men bijgevolg willekeurig kiezen uit de getallen 11, 19 en 25. Voor deze opgave zullen we echter gebruik maken van een strikter codeerschema. Als we een tekstfragment moeten coderen waarin de letter n verschillende keren voorkomt, dan zullen we die letter de eerste keer coderen als het getal 11, de tweede keer door het getal 19, de derde keer als het getal 25. Omdat de letter n slechts op drie posities voorkomt in de sleuteltekst, zullen we de letter n de vierde keer terug coderen als het getal 11, enzoverder. Als we deze procedure volgen met de voorbeeld sleuteltekst die hierboven werd gegeven, dan wordt het woord nondeterminativeness gecodeerd als

karakters	n	o	n	d	e	t	e	r	m	i	n	a	t	i	v	e	n	e	s	s
posities	11	2	19	20	8	4	12	15	7	6	25	21	5	9	13	14	11	8	3	10

Bij het coderen van een bericht geldt verder de afspraak dat karakters van het bericht die niet in de sleuteltekst voorkomen, genegeerd mogen worden. Gevraagd wordt:

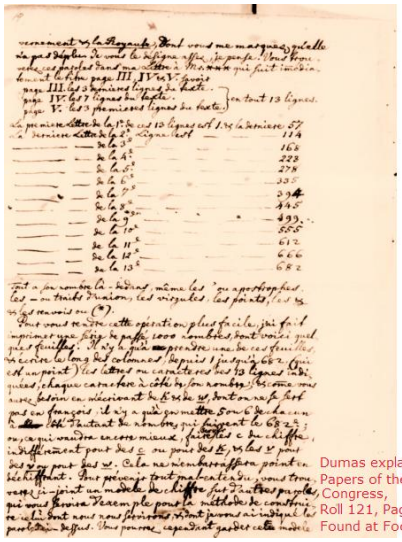
- Schrijf een functie `codeersleutel` waaraan een string moet doorgegeven worden die de sleuteltekst bevat. De functie moet een dictionary teruggeven, die elk karakter dat voorkomt in de sleuteltekst afbeeldt op de lijst van posities in de sleuteltekst waarop dit karakter voorkomt. De posities moeten in stijgende volgorde opgelijst worden. Witruimte in de sleuteltekst moet genegeerd worden. De posities van de karakters worden genummerd vanaf 1. De functie mag ook geen onderscheid maken tussen hoofdletters en kleine letters, en de hoofdlettervariant van een letter moet als sleutel gebruikt worden in de dictionary.
- Gebruik de functie `codeersleutel` om een functie `codeer` te schrijven waaraan twee strings moeten doorgegeven worden: een tekstfragment dat moet gecodeerd worden en de sleuteltekst die bij het coderen moet gebruikt worden. De functie moet het gegeven tekstfragment coderen volgens het strikte codeerschema dat hierboven beschreven werd.

Voorbeeld

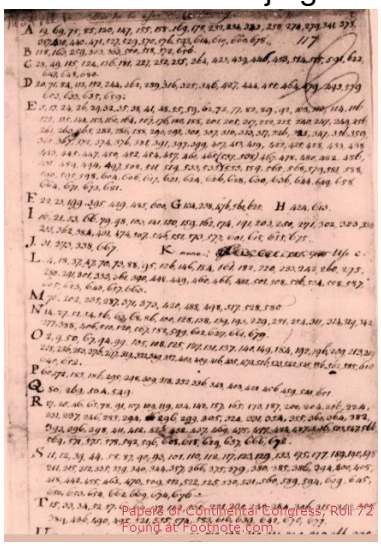
```
>>> sleuteltekst = 'Lost time is never found again.'

>>> sleutel = codeersleutel(sleuteltekst)
>>> sleutel['N']
[11, 19, 25]
>>> sleutel['E']
[8, 12, 14]
>>> sleutel['.']
[26]

>>> codeer('nondeterminativeness', sleuteltekst)
[11, 2, 19, 20, 8, 4, 12, 15, 7, 6, 25, 21, 5, 9, 13, 14, 11, 8, 3, 10]
>>> codeer('interdenominationalism', sleuteltekst)
[6, 11, 4, 8, 15, 20, 12, 19, 2, 7, 9, 25, 21, 5, 24, 17, 11, 23, 1, 6, 3, 7]
>>> codeer('gastroenteroanastomosis', sleuteltekst)
[22, 21, 3, 4, 15, 2, 8, 11, 5, 12, 15, 17, 23, 19, 21, 10, 4, 2, 7, 17, 3, 6, 10]
```

Uitsmijter

Op 30 april 1776 schreef Alexander Dumas een brief naar Benjamin Franklin (hoofd van het *Committee of Secret Correspondence*) in Philadelphia. Daarin uitte hij uitvoerig zijn dankbaarheid voor wat hij voor zijn land kon betekenen, en gaf hij ook gedetailleerde uitleg bij het geheimschrift dat hij had ontwikkeld. Omdat de letters `K` en `W` niet gebruikt worden in het Frans, komen ze ook niet voor in de sleuteltekst. Daarom adviseert hij onder meer om bij de codering van een bericht gebruik te maken van twee `u`'s in plaats van een `w` en van een `c` in plaats van een `k`.



Uittreksel uit het document *Papers of Continental Congress* (rol 121, pagina 19) waarin Charles Dumas zijn geheimschrift uitlegt.



Uittreksel uit het document *Papers of Continental Congress* (rol 72) met de codeersleutel die kan opgesteld worden op basis van het Franse tekstfragment dat hierboven wordt gegeven. Deze sleutel kan gebruikt worden om de passages te decoderen in het bericht van Franklin naar Dumas dat in de inleiding werd gegeven.

Met die kennis leest de gedecodeerde versie van het bericht uit de inleiding als

> *I have just received a* ***neuu comiissjon*** *joining* ***me uuith m adams in negodiaions for peace*** *but this is not likely to afford* ***me much employ at present****.*

Bronnen

- **Weber RE (2010)**. United States diplomatic codes and ciphers: 1775-1938. *Transaction Publishers*.