****

**Criptografia**

**Antonio Emerson Barros Tomaz**

**TRABALHO CRIPTOGRAFIA I**

Crateús-CE

2023

****

**Criptografia**

**Antonio Emerson Barros Tomaz**

**TRABALHO CRIPTOGRAFIA I**

ALAN LOPES MELO

DAVI MARTINS OLIVEIRA

SAMUEL LOPES

VICTOR JONES MESQUITA DE SOUSA

Crateús-CE

2023

Sumário

[**1. Algoritmo de Cifração 4**](#_ucv9dv39cj5v)

[1.1 Texto Cifrado 5](#_16kcs7oi7t6o)

[**2. Análise de frequência 7**](#_t7rx8xp5rqzi)

[2.1. Gráfico de Frequência de Letras no Inglês 7](#_snq86mkpgo7x)

[2.2. Tabela de frequência de ocorrência 8](#_479b75cavup0)

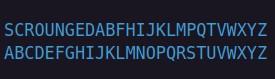
[2.3. Alfabeto Decifrado 12](#_o9seoffwhdm3)

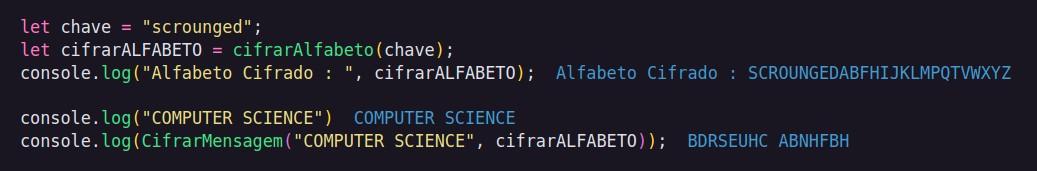
[**3. Texto descifrado pela a análise de frequência 13**](#_9jzuf69tbt4p)

# 1. Algoritmo de Cifração

* cifra de substituição com palavra-chave (Keyword-Cipher)

Usaremos um texto em inglês de uma história das aventuras do Aladdin com sua lâmpada mágica com aproximadamente 1000 palavras, decidimos usar o JavaScript como a linguagem do algoritmo. A seguir fotos do algoritmo + Resultados :

Alfabeto cifrado e Alfabeto original Exemplo de cifração:



Usamos a chave “Scrounged” para cifrar o alfabeto original, com isso, pudemos obter o novo alfabeto que vai ser usado no processo de cifração do nosso texto de 1000 palavras. Esse processo é feito, colocando a palavra chave no início do novo alfabeto, depois seguimos com as letras do alfabeto original, caso ela não tenha aparecido na palavra chave.

Analisamos o algoritmo e ele funciona para a palavra “computer science” que foi usada como exemplo, gerando assim a palavra cifrada “BDRSEUHC ABNHFBH” , a partir disso colocamos o nosso texto original para executar na função, e conseguimos o texto a seguir que logo após foi enviado para a equipe de decifração.

## 1.1 Texto Cifrado

UMH AUDCY DL JQJIINF JFI MNA RJGNBJQ QJRSUMHCH DFBH QNVHI, NF DFH DL UMH QJCGH JFI CNBM BNUNHA DL BMNFJ, J UJNQDC, FJRHI REAUJSMJ. MH WJA VHCY SDDC. MH BDEQI MJCIQY, KY MNA IJNQY QJKDC, RJNFUJNF MNRAHQL JFI MNA LJRNQY, WMNBM BDFANAUHI DFQY DL MNA WNLH JFI J ADF.MNA ADF, WMD WJA BJQQHI JQJIINF, WJA J VHCY BJCHQHAA JFI NIQH LHQQDW. MH WJA INADKHINHFU UD MNA LJUMHC JFI RDUMHC, JFI WDEQI GD DEU HJCQY NF UMH RDCFNFG JFI AUJY DEU JQQ IJY, SQJYNFG NF UMH AUCHHUA JFI SEKQNB SQJBHA WNUM NIQH BMNQICHF DL MNA DWF JGH.WMHF MH WJA DQI HFDEGM UD QHJCF J UCJIH, MNA LJUMHC UDDP MNR NFUD MNA DWF AMDS, JFI UJEGMU MNR MDW UD EAH MNA FHHIQH; KEU JQQ MNA LJUMHC'A HFIHJVDCA UD PHHS MNR UD MNA WDCP WHCH VJNF, LDC FD ADDFHC WJA MNA KJBP UECFHI UMJF MH WJA GDFH LDC UMJU IJY. REAUJSMJ BMJAUNAHI MNR; KEU JQJIINF WJA NFBDCCNGNKQH, JFI MNA LJUMHC, UD MNA GCHJU GCNHL, WJA LDCBHI UD JKJFIDF MNR UD MNA NIQHFHAA, JFI WJA AD REBM UCDEKQHI JKDEU MNR UMJU MH LHQQ ANBP JFI INHI NF J LHW RDFUMA.JQJIINF, WMD WJA FDW FD QDFGHC CHAUCJNFHI KY UMH LHJC DL J LJUMHC, GJVH MNRAHQL HFUNCHQY DVHC UD MNA NIQH MJKNUA, JFI WJA FHVHC DEU DL UMH AUCHHUA LCDR MNA BDRSJFNDFA. UMNA BDECAH MH LDQQDWHI UNQQ MH WJA LNLUHHF YHJCA DQI, WNUMDEU GNVNFG MNA RNFI UD JFY EAHLEQ SECAENU, DC UMH QHJAU CHLQHBUNDF DF WMJU WDEQI KHBDRH DL MNR. JA MH WJA DFH IJY SQJYNFG, JBBDCINFG UD BEAUDR, NF UMH AUCHHU WNUM MNA HVNQ JAADBNJUHA, J AUCJFGHC SJAANFG KY AUDDI UD DKAHCVH MNR.UMNA AUCJFGHC WJA J ADCBHCHC, PFDWF JA UMH JLCNBJF RJGNBNJF, JA MH MJI KHHF KEU UWD IJYA JCCNVHI LCDR JLCNBJ, MNA FJUNVH BDEFUCY.UMH JLCNBJF RJGNBNJF, DKAHCVNFG NF JQJIINF'A BDEFUHFJFBH ADRHUMNFG WMNBM JAAECHI MNR UMJU MH WJA J LNU KDY LDC MNA SECSDAH, NFTENCHI MNA FJRH JFI MNAUDCY DL ADRH DL MNA BDRSJFNDFA; JFI WMHF MH MJI QHJCFHI JQQ MH IHANCHI UD PFDW, WHFU ES UD MNR, JFI UJPNFG MNR JANIH LCDR MNA BDRCJIHA, AJNI, "BMNQI, WJA FDU YDEC LJUMHC BJQQHI REAUJSMJ UMH UJNQDC?" "YHA, ANC," JFAWHCHI UMH KDY; "KEU MH MJA KHHF IHJI J QDFG UNRH."JU UMHAH WDCIA UMH JLCNBJF RJGNBNJF UMCHW MNA JCRA JKDEU JQJIINF'A FHBP, JFI PNAAHI MNR AHVHCJQ UNRHA, WNUM UHJCA NF MNA HYHA, JFI AJNI, "N JR YDEC EFBQH. YDEC WDCUMY LJUMHC WJA RY DWF KCDUMHC. N PFHW YDE JU LNCAU ANGMU; YDE JCH AD QNPH MNR.â€ UMHF MH GJVH JQJIINF J MJFILEQ DL ARJQQ RDFHY, AJYNFG, "GD, RY ADF, UD YDEC RDUMHC, GNVH RY QDVH UD MHC, JFI UHQQ MHC UMJU N WNQQ VNANU MHC UD-RDCCDW, UMJU N RJY AHH WMHCH RY GDDI KCDUMHC QNVHI AD QDFG, JFI HFIHI MNA IJYA."JQJIINF CJF UD MNA RDUMHC, DVHCODYHI JU UMH RDFHY MNA EFBQH MJI GNVHF MNR. "RDUMHC," AJNI MH, "MJVH N JF EFBQH?" "FD, BMNQI," CHSQNHI MNA RDUMHC, "YDE MJVH FD EFBQH KY YDEC LJUMHC'A ANIH DC RNFH." "N JR OEAU FDW BDRH," AJNI JQJIINF, "LCDR J RJF WMD AJYA MH NA RY EFBQH JFI RY LJUMHC'A KCDUMHC. MH BCNHI JFI PNAAHI RH WMHF N UDQI MNR RY LJUMHC WJA IHJI, JFI GJVH RH RDFHY, AHFINFG MNA QDVH UD YDE, JFI SCDRNANFG UD BDRH JFI SJY YDE J VNANU, UMJU MH RJY AHH UMH MDEAH RY LJUMHC QNVHI JFI INHI NF." "NFIHHI, BMNQI," CHSQNHI UMH RDUMHC, "YDEC LJUMHC MJI FD KCDUMHC, FDC MJVH YDE JF EFBQH."UMH FHXU IJY UMH RJGNBNJF LDEFI JQJIINF SQJYNFG NF JFDUMHC SJCU DL UMH UDWF, JFI HRKCJBNFG MNR JA KHLDCH, SEU UWD SNHBHA DL GDQI NFUD MNA MJFI, JFI AJNI UD MNR, â€œBJCCY UMNA, BMNQI, UD YDEC RDUMHC. UHQQ MHC UMJU N WNQQ BDRH JFI AHH MHC UD-FNGMU, JFI KNI MHC GHU EA ADRHUMNFG LDC AESSHC; KEU LNCAU AMDW RH UMH MDEAH WMHCH YDE QNVH."JQJIINF AMDWHI UMH JLCNBJF RJGNBNJF UMH MDEAH, JFI BJCCNHI UMH UWD SNHBHA DL GDQI UD MNA RDUMHC, WMD WHFU DEU JFI KDEGMU SCDVNANDFA; JFI, BDFANIHCNFG AMH WJFUHI VJCNDEA EUHFANQA, KDCCDWHI UMHR DL MHC FHNGMKDCA. AMH ASHFU UMH WMDQH IJY NF SCHSJCNFG UMH AESSHC; JFI JU FNGMU, WMHF NU WJA CHJIY, AJNI UD MHC ADF, â€œSHCMJSA UMH AUCJFGHC PFDWA FDU MDW UD LNFI DEC MDEAH; GD JFI KCNFG MNR, NL YDE RHHU WNUM MNR."JQJIINF WJA OEAU CHJIY UD GD, WMHF UMH RJGNBNJF PFDBPHI JU UMH IDDC, JFI BJRH NF QDJIHI WNUM WNFH JFI JQQ ADCUA DL LCENUA, WMNBM MH KCDEGMU LDC J IHAAHCU. JLUHC MH MJI GNVHF WMJU MH KCDEGMU NFUD JQJIINF'A MJFIA, MH AJQEUHI MNA RDUMHC, JFI IHANCHI MHC UD AMDW MNR UMH SQJBH WMHCH MNA KCDUMHC REAUJSMJ EAHI UD ANU DF UMH ADLJ; JFI WMHF AMH MJI IDFH AD, MH LHQQ IDWF JFI PNAAHI NU AHVHCJQ UNRHA, BCYNFG DEU, WNUM UHJCA NF MNA HYHA, "RY SDDC KCDUMHC! MDW EFMJSSY JR N, FDU UD MJVH BDRH ADDF HFDEGM UD GNVH YDE DFH QJAU HRKCJBH!" JQJIINF'A RDUMHC IHANCHI MNR UD ANU IDWF NF UMH AJRH SQJBH, KEU MH IHBQNFHI."FD," AJNI MH, "N AMJQQ FDU ID UMJU; KEU GNVH RH QHJVH UD ANU DSSDANUH UD NU, UMJU, JQUMDEGM N AHH FDU UMH RJAUHC DL J LJRNQY AD IHJC UD RH, N RJY JU QHJAU KHMDQI UMH SQJBH WMHCH MH EAHI UD ANU."WMHF UMH RJGNBNJF MJI RJIH BMDNBH DL J SQJBH, JFI AJU IDWF, MH KHGJF UD HFUHC NFUD INABDECAH WNUM JQJIINF'A RDUMHC. "RY GDDI ANAUHC," AJNI MH, "ID FDU KH AECSCNAHI JU YDEC FHVHC MJVNFG AHHF RH JQQ UMH UNRH YDE MJVH KHHF RJCCNHI UD RY KCDUMHC REAUJSMJ DL MJSSY RHRDCY. N MJVH KHHF LDCUY YHJCA JKAHFU LCDR UMNA BDEFUCY, WMNBM NA RY FJUNVH SQJBH, JA WHQQ JA RY QJUH KCDUMHC'A; JFI IECNFG UMJU UNRH MJVH UCJVHQQHI NFUD UMH NFINHA, SHCANJ, JCJKNJ, AYCNJ, JFI HGYSU, JFI JLUHCWJCI BCDAAHI DVHC NFUD JLCNBJ, WMHCH N UDDP ES RY JKDIH. JU QJAU, JA NU NA FJUECJQ LDC J RJF, N WJA IHANCDEA UD AHH RY FJUNVH BDEFUCY JGJNF, JFI UD HRKCJBH RY IHJC KCDUMHC; JFI LNFINFG N MJI AUCHFGUM HFDEGM UD EFIHCUJPH AD QDFG J ODECFHY, N RJIH UMH FHBHAAJCY SCHSJCJUNDFA, JFI AHU DEU. FDUMNFG HVHC JLLQNBUHI RH AD REBM JA MHJCNFG DL RY KCDUMHC'A IHJUM. KEU GDI KH SCJNAHI LDC JQQ UMNFGA! NU NA J BDRLDCU LDC RH UD LNFI, JA NU WHCH, RY KCDUMHC NF J ADF WMD MJA MNA RDAU CHRJCPJKQH LHJUECHA."

# 2. Análise de frequência

Em primeira análise, vamos analisar o gráfico de frequência das letras em texto em inglês e a análise de frequência com que cada letra cifrada aparece no texto.

## 2.1. Gráfico de Frequência de Letras no Inglês

O gráfico a seguir representa a frequência de cada letra em textos no inglês.

|  |
| --- |
| Gráfico de Frequência de Letras no Inglês |

## 2.2. Tabela de frequência de ocorrência

A tabela abaixo representa a frequência de ocorrência de cada letra do texto cifrado.

| H | 471 | 11.07% |
| --- | --- | --- |
| J | 397 | 9.33% |
| D | 335 | 7.87% |
| N | 326 | 7.66% |
| U | 326 | 7.66% |
| M | 308 | 7.24% |
| A | 288 | 6.77% |
| F | 285 | 6.70% |
| C | 251 | 5.90% |
| I | 230 | 5.40% |
| Q | 146 | 3.43% |
| R | 138 | 3.24% |
| E | 106 | 2.49% |
| W | 99 | 2.33% |
| Y | 96 | 2.26% |
| B | 93 | 2.19% |
| L | 87 | 2.04% |
| G | 81 | 1.90% |
| K | 61 | 1.43% |
| S | 58 | 1.36% |
| V | 48 | 1.13% |
| P | 20 | 0.47% |
| O | 4 | 0.09% |
| T | 1 | 0.02% |
| X | 1 | 0.02% |
| Z | 0 | 0.00% |

A tabela a seguir representa a frequência com que cada uma das três letras mais frequente do texto cifrado, isto é, **H**, **J** e **D** aparece antes ou depois de cada letra do alfabeto original.

|  | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| H | 58 | 23 | 120 | 0 | 0 | 59 | 9 | 18 | 74 | 22 | 11 | 11 | 131 | 14 | 0 | 4 | 36 | 33 | 10 | 0 | 27 | 44 | 12 | 1 | 12 | 0 |
| J | 57 | 24 | 45 | 1 | 1 | 88 | 15 | 22 | 40 | 0 | 11 | 24 | 46 | 28 | 0 | 3 | 61 | 30 | 15 | 0 | 55 | 16 | 24 | 0 | 17 | 0 |
| D | 26 | 22 | 61 | 10 | 53 | 56 | 10 | 0 | 13 | 1 | 12 | 35 | 21 | 7 | 2 | 2 | 19 | 38 | 6 | 0 | 86 | 7 | 30 | 0 | 0 | 0 |

As vogais que representam H e J provavelmente são **e** e **a,** tendo em vista que são as duas vogais mais populares do idioma inglês. No entanto, não sabemos se **H = e** e **J = a** ou **H = a** e **J = e**. Note que no texto cifrado a combinação **HH** aparece 18 vezes, enquanto **JJ** não aparece nenhuma vez. Sabemos que as letras **ee** tendem a aparecem juntas com uma maior frequência em um texto em inglês do que as letras **aa.** Logo, é provável que **H = e** e **J = a.** Nossa conclusão de que **J = a** é apoiada pelo o fato de que o **J** aparece sozinho no texto cifrado, e o **a** é uma das duas únicas palavras do inglês formadas por uma única letra. Além disso, apenas outra letra aparece sozinha no texto cifrado e esta é o **N**. Isso torna altamente provável que ela represente a outra palavra inglesa de uma letra que no nosso caso é o **i.**

Após ter identificado a letra **e** podemos identificar a letra **h**. No idioma inglês a letra **h** aparece com frequência antes da letra **e**, mas raramente ele ocorre depois do **e**. A tabela a seguir mostra com que frequência o **H**, que pensamos representar o **e**, aparece antes e depois de todas as letras do texto cifrado.

|  | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Depois do H | 23 | 7 | 84 | 0 | 0 | 34 | 2 | 18 | 50 | 22 | 0 | 4 | 1 | 1 | 0 | 0 | 11 | 6 | 5 | 0 | 8 | 6 | 3 | 1 | 6 | 0 |
| Antes do H | 35 | 16 | 36 | 0 | 0 | 25 | 7 | 18 | 24 | 0 | 11 | 7 | 130 | 13 | 0 | 4 | 25 | 27 | 5 | 0 | 19 | 38 | 9 | 0 | 6 | 0 |

A tabela acima sugere que o **M** representa o **h**, porque ele aparece antes do **H** em 130 ocasiões, e, apenas, uma vez depois dele. Nenhuma outra letra na tabela teve esse relacionamento com o **H**. Dessa forma, identificamos com confiança quatro letras, **H = e, J = a, N = i, e M = h**. Em complemento a isso, considerado as cincos letras que mais repetem-se no texto cifrado, isto é, **H = 471, J = 397, D = 335, N = 326 e U = 326** e o gráfico de frequência de letras em inglês. Sabemos que em todo alfabeto a repetição de vogais é algo comum em toda linguagem, tendo base nisso, podemos considerar que algumas das letras que mais se repetem no texto cifrado podem ser equivalentes às vogais (**A,E,I,O,U**) no texto original.Analisando a estimativa da letra **E** na língua inglesa, podemos concluir que ela tem uma grande quantidade de ocorrências, podemos considerar **H = e**. Já o **J** é a segunda letra que mais se repete, tendo base que a letra **A** seja a segunda vogal mais frequente do idioma inglês, podemos considerar **J** = **a**.

A tabela abaixo que representa o alfabeto descifrado vai ser preenchida conforme as letras do texto cifrado forem decodificadas. **Alfabeto Decifrado**

| Alfabeto original | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto cifrado | **J** |  |  |  | **H** |  |  | **M** | **N** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Logo, podemos começar a substituir algumas das letras do texto cifrado por suas equivalentes no texto original. Vamos manter a convenção de deixar as letras do texto cifrado em maiúsculas enquanto as letras do texto decodificado ficam em minúsculas.

Sabemos que uma das palavras de três letras mais comuns em inglês são “**the”** e **"and".** Após ter realizado a substituição no passo anterior e ter analisado a ocorrência das palavras cifradas **aFi** e **Uhe**, podemos supor que, provavelmente, o **U** representa o **t,** devido ao fato de que no idioma inglês o **t** tende a aparecer antes do **h** e , consequentemente, forma o **th**. Tal argumento também pode ser justificado pelo fato da vogal **U** na língua inglesa não se repetir tanto como esperado para letra **U** no texto cifrado , podemos descartar a possibilidade da mesma ser uma vogal no alfabeto original. Assim , podemos analisar as consoantes que mais se repetem na língua inglesa, onde temos o **T**, e como a letra **U** do texto cifrado é uma das que têm maiores ocorrências, podemos supor que a letra **U** do texto cifrado seja letra **t** do alfabeto original. Já o **aFI** é o que mais repete-se, provavelmente o **F** representa a letra **n** e o **I** a letra **d**. Vamos destacar a palavra **MNR** do texto cifrado, como sabemos que **M** = **h** e **N** = **i** , temos **hiR**, como são 3 letras não podemos induzir que seja **hi** do inglês, e como é uma palavra que se repete bastante com 3 letras do inglês a que é mais compatível seria **him**, um pronome pessoal da língua inglesa que é costumeiro sua constante repetição. Logo, podemos concluir que o **R** = **m**. Logo, temos:

**Alfabeto Decifrado**

| Alfabeto original | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto cifrado | J |  |  | **I** | H |  |  | M | N |  |  |  | **R** | **F** |  |  |  |  |  | **U** |  |  |  |  |  |  |

Analisando a palavra **theCe** podemos supor que a letra **C** do texto cifrado seria a letra **r** do texto simples e, consequentemente, teríamos a palavra decifrada “**there”.** Pelos estudos de criptoanálise, sabemos que “**one”** e “**his”** também são uma das palavras de três letras que mais repete-se em texto em inglês. Logo, podemos analisar as seguintes palavras do texto cifrado: **Dne** e **hiA**. Dessa forma, também podemos deduzir que o **D** refere-se ao **o** e o **A** refere-se ao **s** do texto claro.

**Alfabeto Decifrado**

| Alfabeto original | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto cifrado | J |  |  | I | H |  |  | M | N |  |  |  | R | F | **D** |  |  | **C** | **A** | U |  |  |  |  |  |  |

Em relação às palavras de duas letras, sabemos que **“of”, “or”** e **“on”** são muito frequentes em textos em inglês. Nesse sentido, vamos analisar a palavra **oL** do texto cifrado. Note que **L** não pode ser **r** ou **n**, haja vista que **r** refere-se a **C** no texto cifrado e **n** a **F.** Dessa forma, **L**, provavelmente, refere-se a **f**. Sabemos também que os dígrafos **to**, **so**, **do**, **go** e **no** são muito frequentes em textos em inglês. Nessa perspectiva, vamos analisar a palavra cifrada **Go**. Note que **G** não pode ser **t**, **s**, **d** e **n**, tendo em vista que todas essas letras do texto simples estão associados às seguintes letras do texto cifrado: **U**, **A**, **I** e **F**, respectivamente. Logo, podemos supor que a letra **G** do texto cifrado refere-se a letra **g** do alfabeto original. Logo, teremos a seguinte configuração na tabela do alfabeto descifrado:

**Alfabeto Decifrado**

| Alfabeto original | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto cifrado | J |  |  | I | H | **L** | **G** | M | N |  |  |  | R | F | D |  |  | C | A | U |  |  |  |  |  |  |

A ordem de frequência dos duplos mais comuns é **ss**, **ee**, **tt**, **ff**, **ll**, **mm** e **oo**. Nesse contexto, vamos analisar a palavra cifrada **aQQ**. Note que **Q** não pode ser **s**, **e**, **t**, **f**, **m**, tendo em vista que todas essas letras do texto simples estão associados às seguintes letras do texto cifrado: **A**, **H**, **U**, **L** e **R** respectivamente. Logo, podemos supor que a letra **Q** do texto cifrado refere-se a letra **L** do alfabeto original. Analisando também a palavra **mY** do texto cifrado, sabemos **Y** não poderia ser “**e”**, haja vista que tal palavra não poderia ser **me** devido ao fato que **H = “e”** e, por conseguinte, **Y não poderia ser igual a “e”**. Logo, poderíamos considerar o pronome possessivo **my**, sendo que **mY** possui *18 ocorrências* e é natural que seja comumente utilizado na maioria dos textos da língua inglesa, sem contar que apenas traduzindo o **mY** temos a palavra **my** que, inclusive, já é uma palavra da língua inglesa.

Analisando o trecho do texto cifrado **LJUMHC JFI RDUMHC**, temos traduzindo a seguinte sequência **father and RDther**, logo podemos deduzir que seria **father and mother**. Logo, isso reforça o fato que **R** = **m** e **D** = **o**. Por fim, destacando o seguinte trecho do texto cifrado, temos **WJA**, com o que sabemos até então, obteremos **Was**. Logo, podemos concluir que pode ser **Was** que seria o verbo do passado simples na língua inglesa. Assim , **W** = **w**

Portanto, o Alfabeto decodificado ficou da seguinte forma:

## 2.3. Alfabeto Decifrado

| Alfabeto original | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto cifrado | J |  |  | I | H | L | G | M | N |  |  | **Q** | R | F | D |  |  | C | A | U |  |  | **W** |  | **y** |  |

# 3. Texto descifrado pela a análise de frequência

the story of aladdin and his magiBal lamS

there onBe liVed,in one of the large and riBh Bities of Bhina,a tailor,named mEstaSha.he was Very Soor.he BoEld hardly,Ky his daily laKor,maintain himself and his family,whiBh Bonsisted only of his wife and a son.

his son,who was Balled aladdin,was a Very Bareless and idle fellow.he was disoKedient to his father and mother,and woEld go oEt early in the morning and stay oEt all day,Slaying in the streets and SEKliB SlaBes with idle Bhildren of his own age.

when he was old enoEgh to learn a trade,his father tooP him into his own shoS,and taEght him how to Ese his needle;KEt all his father's endeaVors to PeeS him to his worP were Vain, for no sooner was his KaBP tErned than he was gone for that day. mEstaSha Bhastised him; KEt aladdin was inBorrigiKle, and his father, to his great grief, was forBed to aKandon him to his idleness, and was so mEBh troEKled aKoEt him that he fell siBP and died in a few months.

aladdin, who was now no longer restrained Ky the fear of a father, gaVe himself entirely oVer to his idle haKits, and was neVer oEt of the streets from his BomSanions. this BoErse he followed till he was fifteen years old, withoEt giVing his mind to any EsefEl SErsEit, or the least refleBtion on what woEld KeBome of him. as he was one day Slaying, aBBording to BEstom, in the street with his eVil assoBiates, a stranger Sassing Ky stood to oKserVe him.

this stranger was a sorBerer, Pnown as the afriBan magiBian, as he had Keen KEt two days arriVed from afriBa, his natiVe BoEntry.

the afriBan magiBian, oKserVing in aladdin's BoEntenanBe something whiBh assEred him that he was a fit Koy for his SErSose,inTEired his name and history of some of his BomSanions;and when he had learned all he desired to Pnow,went ES to him,and taPing him aside from his Bomrades,said,"Bhild, was not yoEr father Balled mEstaSha the tailor?" "yes, sir," answered the Koy;"KEt he has Keen dead a long time."

at these words the afriBan magiBian threw his arms aKoEt aladdin's neBP, and Pissed him seVeral times, with tears in his eyes, and said, "i am yoEr EnBle. yoEr worthy father was my own Krother. i Pnew yoE at first sight; yoE are so liPe him." then he gaVe aladdin a handfEl of small money, saying, "go, my son, to yoEr mother, giVe my loVe to her, and tell her that i will Visit her to-morrow, that i may see where my good Krother liVed so long, and ended his days."

aladdin ran to his mother, oVerOoyed at the money his EnBle had giVen him. "mother," said he, "haVe i an EnBle?" "no, Bhild," reSlied his mother, "yoE haVe no EnBle Ky yoEr father's side or mine." "i am OEst now Bome," said aladdin, "from a man who says he is my EnBle and my father's Krother. he Bried and Pissed me when i told him my father was dead, and gaVe me money, sending his loVe to yoE, and Sromising to Bome and Say yoE a Visit, that he may see the hoEse my father liVed and died in." "indeed, Bhild," reSlied the mother, "yoEr father had no Krother, nor haVe yoE an EnBle."

the next day the magiBian foEnd aladdin Slaying in another Sart of the town, and emKraBing him as Kefore, SEt two SieBes of gold into his hand, and said to him, "Barry this, Bhild, to yoEr mother. tell her that i will Bome and see her to-night, and Kid her get Es something for sESSer; KEt first show me the hoEse where yoE liVe."

aladdin showed the afriBan magiBian the hoEse, and Barried the two SieBes of gold to his mother, who went oEt and KoEght SroVisions; and, Bonsidering she wanted VarioEs Etensils, Korrowed them of her neighKors. she sSent the whole day in SreSaring the sESSer; and at night, when it was ready, said to her son, “SerhaSs the stranger Pnows not how to find oEr hoEse; go and Kring him, if yoE meet with him."aladdin was OEst ready to go, when the magiBian PnoBPed at the door, and Bame in loaded with wine and all sorts of frEits, whiBh he KroEght for a dessert. after he had giVen what he KroEght into aladdin's hands,he salEted his mother,and desired her to show him the SlaBe where his Krother mEstaSha Esed to sit on the sofa;and when she had done so,he fell down and Pissed it seVeral times,Brying oEt,with tears in his eyes,"my Soor Krother! how EnhaSSy am i, not to haVe Bome soon enoEgh to giVe yoE one last emKraBe!" aladdin's mother desired him to sit down in the same SlaBe, KEt he deBlined.

"no," said he, "i shall not do that; KEt giVe me leaVe to sit oSSosite to it, that, althoEgh i see not the master of a family so dear to me, i may at least Kehold the SlaBe where he Esed to sit."

when the magiBian had made BhoiBe of a SlaBe, and sat down, he Kegan to enter into disBoErse with aladdin's mother."my good sister," said he,"do not Ke sErSrised at yoEr neVer haVing seen me all the time yoE haVe Keen married to my Krother mEstaSha of haSSy memory. i haVe Keen forty years aKsent from this BoEntry, whiBh is my natiVe SlaBe, as well as my late Krother's; and dEring that time haVe traVelled into the indies, Sersia, araKia, syria, and egySt, and afterward Brossed oVer into afriBa, where i tooP ES my aKode. at last, as it is natEral for a man, i was desiroEs to see my natiVe BoEntry again, and to emKraBe my dear Krother; and finding i had strength enoEgh to EndertaPe so long a OoErney, i made the neBessary SreSarations, and set oEt. nothing eVer affliBted me so mEBh as hearing of my Krother's death. KEt god Ke Sraised for all things! it is a Bomfort for me to find, as it were, my Krother in a son who has his most remarPaKle featEres.