Uma introdução (ingénua) à Criptografia

António Machiavelo e Rogério Reis

Departamentos de Matemática e Ciência de Computadores da
Faculdade de Ciências da Universidade do Porto

Num mundo de comunicações digitais como o de hoje, onde a omnipresença da transmissão de informação é quase absoluta, não temos muitas vezes consciência do quanto dependemos dos processos criptográficos. Para quase todos, a Criptografia, é uma obscura disciplina, difícil de enquadrar numa área de conhecimento, e de uso geralmente mais ou menos esotérico. Quando se fala de Criptografia, são as imagens de espiões, de mensagens diplomáticas e grandes segredos militares que imediatamente nos ocorrem. Não que este não tenha sido realmente o seu papel durante a esmagadora maioria da sua história, já de alguns milhares de anos, mas na segunda metade do século XX, quando a Criptografia passou a ser campo de estudo da Matemática, e as transmissões digitais se popularizaram, esta quebrou as fronteiras do seu nicho de aplicação e invadiu as nossas vidas. Dos comandos de televisão às próprias emissões de televisão, dos telemóveis às máquinas multibanco, na multitude das utilizações da internet, a Criptografia está lá, não só para garantir a segurança de segredos, quando é caso disso, mas para identificar e garantir identidades de interlocutores, garantir pagamentos e integridade da transmissão de mensagens, efectuando tarefas das mais simples às mais complexas. Podemos dizer, que grande parte das soluções que foi necessário encontrar para transpor para uma realidade onde os interlocutores não se encontram fisicamente no mesmo local, transações que damos como garantidas no "mundo físico", foram dadas pela Criptografia. E no entanto, tudo começou, há muito tempo, com o problema de preservar segredos. Um interlocutor A quer enviar uma mensagem a um outro interlocutor B, sem ter que lha comunicar pessoalmente, querendo que, apesar da mensagem poder ser eventualmente interceptada por terceiros, se mantenha legível somente para o seu legítimo destinatário. Este é o problema fundamental da Criptografia clássica. Não é razoável, em tão curto espaço expor qualquer das técnicas criptográficas que hoje são usadas, e muito menos a Matemática em que estas assentam. Mas podemos descrever os princípios que foram dominantes na Criptografia até à dois séculos atrás.

Esteganografia

Para poder enviar uma mensagem de forma a que o seu conteúdo não seja legível para terceiros, a criptografia oculta o método (a cifra) com que foi codificada a mensagem, ou oculta simplesmente a chave que foi utilizada, sendo a cifra pública. Apesar de não dever ser fácil ler o conteúdo da mensagem, é evidente que de uma mensagem se trata, e que esta está cifrada para ocultar o seu conteúdo. Mas esta não é a única solução. A esteganografia tenta

ocultar o próprio facto de que se está a transmitir informação. Tenta-se que a própria transmissão da informação não seja evidente, ou então dissimula-se a verdadeira mensagem no suporte de uma outra mensagem sem importância. O nome de esteganografia está ligado a Johannes Trithemius que publica um livro que aparentemente versa a Magia Negra, mas que de facto consiste num tratado sobre criptografia. Os exemplos de recurso à estenografia ao longo da História são muitos:

- **Escrita no crânio de um escravo**. Segundo Heródoto, quando Histiaeus quis comunicar ao seu genro Aristagoras de Mileto que estava na altura de se revoltar contra a ocupação persa, tatuou essa mensagem no crânio de um escravo de confiança, a quem previamente havia rapado o cabelo, e enviou-o através das linha inimigas depois de esperar que o cabelo tivesse voltado a crescer [Kah67].

- **Mensagens engolidas.** Os chineses faziam transportar as mensagens mais sensíveis por mensageiros, que as engoliam depois de as colocar em pequenas bolas de cera [Gai39].

- **Escrita em ovos cozidos.** Giovanni Porta (1535–1615) descreve a receita de uma solução de alúmen e vinagre que escrita na casca de um ovo cozido, penetra através da casca e pode ser lida somente depois desta removida [Sin99].

- **Micro-perfuração.** Para evitar pagar as altas taxas postais para a correspondência privada e passar a pagar a taxa de envio de materiais impressos (muito mais baixa), generalizou-se em Inglaterra, durante algum tempo no século passado, a utilização de um estranho meio de comunicação: Num qualquer jornal, produziam-se com o auxílio de uma agulha, pequenos orifícios sobre algumas letras do texto impresso, por forma a que essas letras assim escolhidas formassem a mensagem que se queria enviar! [Gai39].

- **A "escrita simpática".** Escrita de uma mensagem com sumo de um citrino (normalmente limão) nas entrelinhas de uma outra mensagem. Quando o papel é submetido ao calor a mensagem até aí invisível aparece em tons de castanho. Martin Gardner [Gar72] descreve para além desta algumas outras receitas de tintas "invisíveis".

- **Microponto.** Um microfilme do formato de um ponto final de uma máquina de escrever pode transportar informação assim dissimulada numa carta absolutamente inócua. Este método foi usado desde 1870. Durante a segunda guerra mundial foi usado com regularidade pelas embaixadas alemãs na América Latina [Kah67].

- **Grelhas de leitura.** O cardeal Richelieu (1585–1642) usava na comunicação com os seus agentes, uma grelha de papel que sobreposta a uma mensagem escrita, ocultava todas as palavras excepto aquelas que constituíam verdadeiramente a informação a transmitir [Gai39].

- **Variação de tipos impressos.** Francis Bacon (1561–1626) colocava uma mensagem oculta num texto impresso, fazendo variar entre duas fontes muito semelhantes as diversas letras de um texto [Gai39, Kah67].

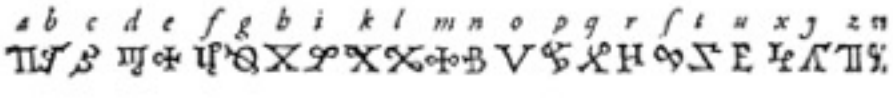
Para todos este métodos não há muito a dizer de como os descobrir, a criptanálise não pode dar grandes ajudas! Mas a utilização da esteganografia assenta sempre na convicção que terceiros não suspeitam que informação, para além da evidente, está a ser enviada. No momento em que uma forte suspeita se instala estes métodos revelam-se quase sempre desastrosos. O principal problema, contudo, é a possibilidade da descoberta fortuita da informação secreta, sem que nenhum esforço tenha sido desenvolvido nesse sentido: o ovo parte-se por acidente, a mensagem com "escrita simpática" é aquecida por uma lâmpada, o mensageiro tem um problema de intestinos, etc ...

A esteganografia não é, no entanto, uma coisa do passado. As imagens digitalizadas que "circulam" na Internet constituem um campo fácil de utilização de processo esteganográficos. Podemos então adaptar o método usado por Francis Bacon às novas tecnologias e usar dois tons muito próximos de branco (por exemplo) em vez de duas fontes de caracteres. A alteração das imagens é imperceptível, e como se trata de um meio digital, tanto o processo de codificação como de descodificação, automatizados não necessitam um esforço excessivo.

Cifras monoalfabéticas

O mais simples dos sistemas criptográficos consiste na substituição de cada uma das letras que formam uma mensagem pelas letras correspondentes de um outro alfabeto, a estas cifras chamamos cifras monoalfabéticas. O alfabeto correspondente ao texto cifrado não tem que usar os símbolos do alfabeto original como é exemplo a cifra usada por Conan Doyle em "The Adventure of a Dancing Man" (uma das aventuras do Sherlock Holmes):

Cifras deste género não são só produto literário. Carlos Magno usava também uma cifra deste género:



As cifras mais usuais, e aquelas que vamos analisar com mais detalhe, usam no entanto os mesmos caracteres para o texto cifrado e para o original. A mais simples cifra monoalfabética deste tipo é chamada cifra de César, que apesar da sua inocente simplicidade, foi (como o nome indica) usada por Júlio César (100–44BC). Como qualquer cifra monoalfabética, fica caracterizada pela correspondência entre o alfabeto original e cifrado. Como convenção vamos

usar caracteres minúsculos para representar o texto original e caracteres maiúsculos para representar 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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

O alfabeto cifrado é o resultado da aplicação de um deslocamento de três letras para a esquerda ao alfabeto original.

Para se cifrar um texto (por exemplo "veni vidi vinci"), basta substituir cada um dos caracteres do alfabeto de cima pelo correspondente caracter do alfabeto de baixo. Representemos o resultado a aplicação da cifra a um texto qualquer T por E(T). O resultado é:

E(`veni vidi vinci`) = `YHQL YLGL YLQFL.`

Para decifrar basta executar o processo de forma inversa, i.e., substituir cada letra do alfabeto de baixo pela correspondente letra do alfabeto de cima.

Nada nos obriga a usar exactamente esta cifra (com um deslocamento de três letras), podemos obter uma cifra diferente escolhendo um qualquer número de deslocamentos que constituem a chave da cifra. Portanto, com uma cifra deste género temos um universo de 25 chaves. O que não é propriamente um dissuasor de uma "ataque de força bruta"!

Não faz sequer sentido falar em criptanálise deste tipo de cifras. Basta tentar decifrar o criptograma com as 25 chaves possíveis[1] , para imediatamente reconhecermos a chave usada.

Se se optar por ter uma chave que não seja necessariamente obtida por deslocamento do alfabeto original, então temos um universo de chaves um pouco maior:

26! - 1 = 403291461126605635583999999

o que afasta definitivamente a hipótese de um ataque de "força-bruta"! Claro que a chave passa a ser mais difícil de decorar, mas podemos tentar obviar esse problema usando a seguinte técnica:

1. Escolhemos uma palavra ou frase que vai servir de chave (senha), por exemplo `Gomes Teixeira`.
2. Começamos por retirar as ocorrências repetidas de cada letra, a partir da segunda: `gomestixra`.
3. Adicionamos à palavra assim obtida as restantes letras do alfabeto, pela respectiva ordem. Obtemos assim a cifra:

```
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
G O M E S T I X R A B C D F H J K L N P Q U V W Y Z
```

[1] E para este ataque basta decifrar um pedaço de uma dezena de caracteres para termos imediatamente a percepção se acertamos na chave ou não.

Apesar deste método não ser perfeito[2] vai permitir que não tenhamos que manter escrita a chave de um canal de comunicações, diminuindo o risco da descoberta da chave por meios não criptográficos[3].

Criptanálise de uma cifra monoalfabética

Consideremos o seguinte criptograma:

```
IWLPY SITSB SDSID QHQJY RLWKS TSADR IWNMR AQIYS TDSNU SMRWA
SMUSC SDQZP JMRHP JDSJS RIQIS LQDQR JDQHR RWDQW ANSDR DSQIY
TSDSD QWEWS YTRCP JRYQI XTRYQ IMRIQ KRPQJ XSTTS KSTIQ IPNQJ
MPRIS QAQIQ TSHQN JSHSN QYSDR RWYTR NSDRN RXRWA SLSYQ XSHST
TQWSQ IYTSD SRIUR AQJIB SQJMU STMSD RICQN RIMUW HPIMR IEWQM
SPSAD QIDQR SNHRT QMQTC TRMWT STSAS LTPXR BWJYR SRIYT RJMRI
QILQN YRIDR ICPJU QPTRI IRDRP ITSCS ZPYRI IQDQP VSTSA KPMST
SLTPY STCQD TSTPJ DRDRI URAQJ IEWQK WXPSA SMUWH S
```

Comecemos por notar que foram eliminados todos os espaços, capitalização de palavras e sinais de pontuação. A razão é simples... se tal não tivesse sido feito muita informação sobre o tamanho das palavras, as letras que ocorrem no início ou do fim das mesmas, etc.., seria uma informação valiosa para simplificar o trabalho do criptanalista. A razão porque os criptogramas se apresentam tradicionalmente com os caracteres agrupados em grupos de cinco tem que ver somente com limitações históricas das transmissões telegráficas.

Procedendo a uma contagem dos caracteres obtemos o seguinte resultado:

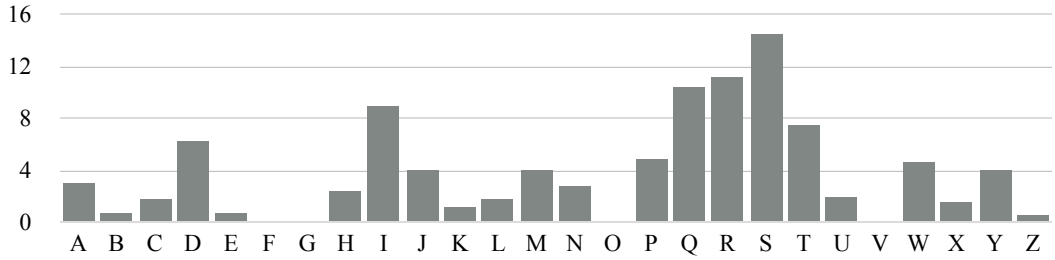
Ocorrências dos diversos caracteres, e respectivas percentagens.

A	B	C	D	E	F	G	H	I	J	K	L	M
12	3	7	25	3	0	0	9	35	16	5	7	16
3.0	0.7	1.7	6.3	0.7	0.0	0.0	2.3	8.9	4.0	1.2	1.7	4.0

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	0	19	41	44	57	30	8	1	18	6	16	2
2.8	0.0	4.8	10.4	11.2	14.5	7.6	2.0	0.2	4.6	1.5	4.0	0.5

[2] Para além de diminuir drasticamente o espaço combinatório das possíveis cifras, para grande parte das palavras (chaves) deixa inalteradas uns quantos caracteres no fim do alfabeto. A solução pode ser melhorada se em vez de colocarmos as restantes letras pela sua ordem natural o fizermos por ordem inversa.

[3] Como por exemplo, bisbilhotando nos cadernos de apontamentos ou na carteira de um dos interlocutores.

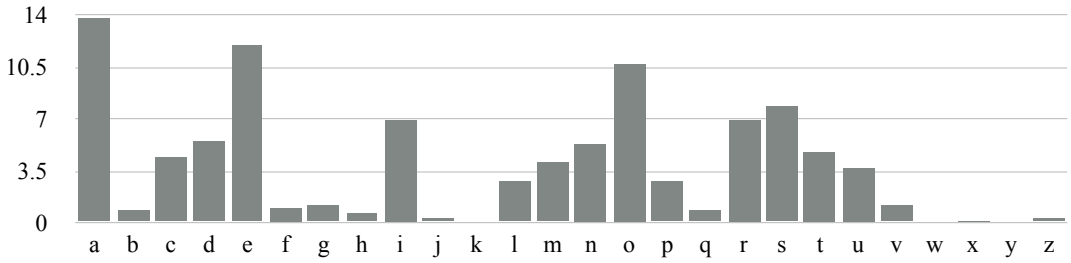


Como o que ocorre numa cifra monoalfabética é a substituição de cada carácter por um outro de um alfabeto, a frequência relativa das ocorrências vai ser preservada pelo processo de cifra. Portanto se soubermos qual é a língua em que está expressa a mensagem original, podemos comparar as frequências relativas de ocorrência de cada carácter do criptograma com as frequências relativas de ocorrência na língua de origem.[4]

Frequências relativas dos diversos caracteres no Português actual.

a	b	c	d	e	f	g	h	i	j	k	l	m
13.8	0.9	4.5	5.6	12.0	1.0	1.2	0.6	7.0	0.3	0.0	2.8	4.1

n	o	p	q	r	s	t	u	v	w	x	y	z
5.3	10.8	2.9	0.8	6.9	7.8	4.9	3.8	1.3	0.0	0.2	0.0	0.3



Os caracteres mais frequentes no português, são então o `a`, `e` e `o`, com 13.8% , 12.0% e 10.8%, respectivamente. No texto do criptograma os caracteres com percentagens comparáveis são o `S` (14.5%), o `R` (11.2%) e o `Q` (10.4%). Portanto temos muito provavelmente que

$$\{E(\texttt{a}), E(\texttt{e}), E(\texttt{o})\} = \{\texttt{S}, \texttt{R}, \texttt{Q}\}.$$

Infelizmente no português, as três letras mais frequentes são todas vogais pelo que provavelmente vamos ter que tentar todas as possibilidades (que são só 6).

---

[4] Para conhecer valores das frequências típicas noutras línguas europeias, assim como alguns outros valores estatísticos sobre a língua inglesa, basta ver o apêndice do livro de Gaines [Gai39]. Os resultados enfermam, para fins práticos, do facto de se referirem à realidade linguística da primeira metade do sec.XX. Estes valores assim como outros actuais, em especial sobre a língua portuguesa podem ser consultados em http://www.dcc.fc.up.pt/~rvr/naulas/tabelasPT/

Podemos apostar que neste criptograma a ordem da frequência destes caracteres se mantinha (o que não é nada garantido) e portanto supor que

$$E(\texttt{a}) = \texttt{S},\ E(\texttt{e}) = \texttt{R} \text{ e } E(\texttt{o}) = \texttt{O}.$$

As letras que têm uma ocorrência média superior a 4 no português, são:

$$\texttt{c}, \texttt{d}, \texttt{i}, \texttt{m}, \texttt{n}, \texttt{r}, \texttt{s}, \texttt{t}.$$

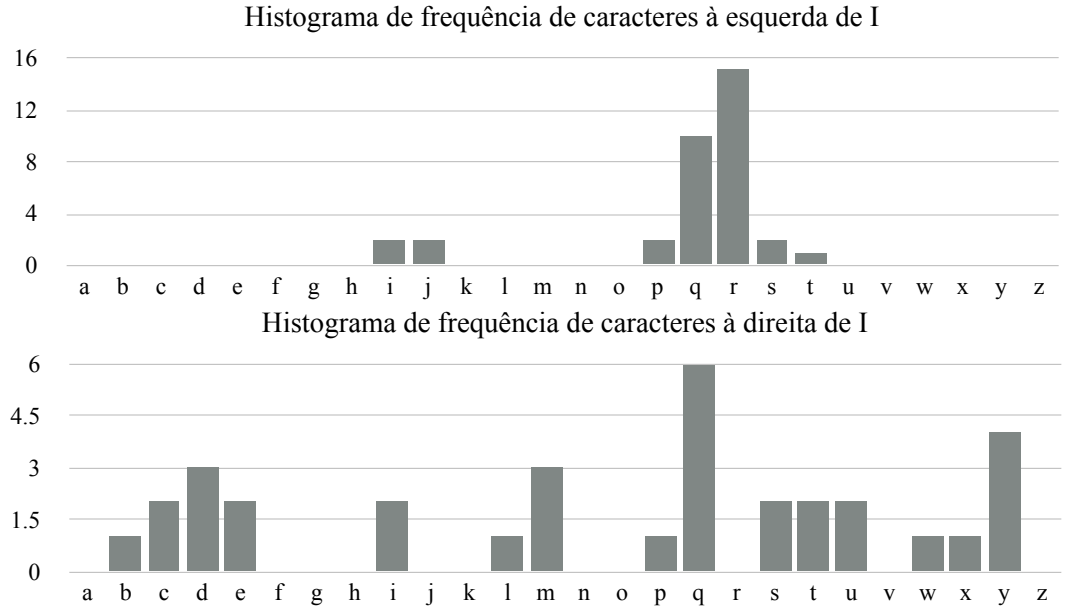
As 8 letras mais frequentes no criptograma são:

$$\texttt{D}, \texttt{I}, \texttt{J}, \texttt{M}, \texttt{P}, \texttt{T}, \texttt{W}, \texttt{Y}.$$

Podemos-nos sentir tentados a atribuir

$$E(\texttt{i}) = \texttt{I}$$

dado ser a letra que resta com maior frequência. Mas se observarmos, imediatamente ao lado de I aparece predominantemente um pequeno grupo de letras:

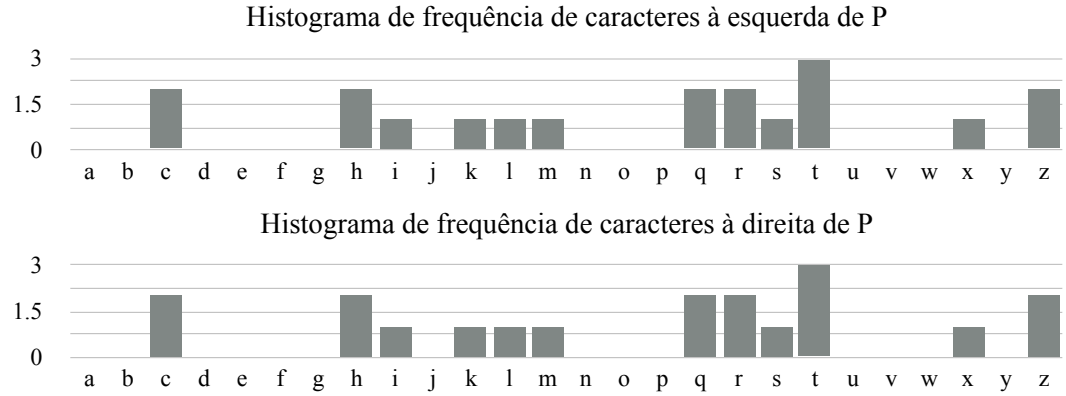


Este tipo de distribuição de caracteres à esquerda e direita é mais compatível com uma consoante (que tem predominantemente na sua vizinhança vogais) do que com uma vogal (que tem predominantemente na sua vizinhança consoantes). Assim tomando a consoante mais frequente, provavelmente temos

$$E(\texttt{s}) = \texttt{I}.$$

Existem duas ocorrências de `II` (que também podendo ser produto da concatenação das palavras) é compatível com a existência de `ss` na língua portuguesa.

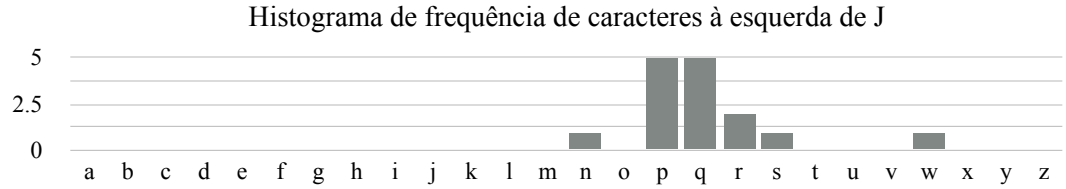
Se fizermos o mesmo tipo de análise para as ocorrências na vizinhança de `P` obtemos:



Esta distribuição muito mais homogénea, especialmente quanto à vizinhança à esquerda, indica que provavelmente corresponde a uma vogal. Então provavelmente teremos

$$E(\texttt{i}) = \texttt{P}.$$

O facto de `J` ocorrer relativamente frequente à direita de `P` (que por hipótese representa `i`) leva a suspeitar que se trate da substituição de `n`. Vejamos que caracteres ocorrem à esquerda de `J`.



O que é compatível com uma consoante (`P`, `Q`, `R` e `S` correspondem a vogais) e com as ocorrências de `n`. Para além disso a percentagem de ocorrências de `J` no criptograma (5.3%) não é muito diferente da percentagem de ocorrências de `n` na língua portuguesa (4.0%).

Do conjunto de letras mais frequentes que ainda restam `T` (7.6%) e `r` (6.9%), são as de frequência mais elevada e portanto mais prováveis de estarem relacionadas, e reforçando esta suspeita existe o facto de ocorrerem dois pares `TT`. Suponhamos portanto

$$E(\texttt{r}) = \texttt{T}.$$

Procedendo da mesma forma como fizemos para `P` podemos concluir que, muito provavelmente, `W` representa uma vogal, e a que resta é `u`.

$$E(\texttt{u}) = \texttt{W}.$$

Falta-nos associar `D` (6.3%), `M` (4.0%) e `Y` (4.0%) a `c` (4.5%), `d` (5.6%), `m` (4.1%) ou `t` (4.9%). Parece que

$$E(\texttt{d}) = \texttt{D}.$$

Observemos que existem 7 ocorrências de `TR` e somente 1 de `TQ`. Isto corresponde, segundo as nossas suposições a muito mais ocorrências de `re` do que de `ro` o que não é natural na

língua portuguesa. Portanto, provavelmente escolhemos mal os valores associados a `Q` e `R`. Refaçamos essas escolhas tomando agora

$$E(\texttt{e}) = \texttt{Q} \text{ e } E(\texttt{o}) = \texttt{R}.$$

Recapitulando temos até agora a seguinte chave "descoberta":

```
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
S     D Q       P         J R     T I   W
```

O que corresponde à seguinte decifração parcial:

```
IWLPY SITSB SDSID QHQJY RLWKS TSADR IWNMR AQIYS TDSNU SMRWA
su i  asra  adasd e en  o u a ra do su  o  es a rda   a ou
SMUSC SDQZP JMRHP JDSJS RIQIS LQDQR JDQHR RWDQW ANSDR DSQIY
a  a  ade i n o i ndana osesa  edeo nde o oudeu   ado daes
TSDSD QWEWS YTRCP JRYQI XTRYQ IMRIQ KRPQJ XSTTS KSTIQ IPNQJ
radad eu ua  ro i no es  ro e s ose  oien  arra  arse si en
MPRIS QAQIQ TSHQN JSHSN QYSDR RWYTR NSDRN RXRWA SLSYQ XSHST
 iosa e ese ra e  na a  e ado ou ro  ado  o ou  a a e  a ar
TQWSQ IYTSD SRIUR AQJIB SQJMU STMSD RICQN RIMUW HPIMR IEWQM
reuae s rad aos o  ens  aen   ar ad os e  os  u  is o s ue
SPSAD QIDQR SNHRT QMQTC TRMWT STSAS LTPXR BWJYR SRIYT RJMRI
aia d esdeo a  or e er  ro ur ara a  ri o  un o aos r on os
QILQN YRIDR ICPJU QPTRI IRDRP ITSCS ZPYRI IQDQP VSTSA KPMST
es e  osdo s in  eiros sodoi sra a  i os sedei  ara  i ar
SLTPY STCQD TSTPJ DRDRI URAQJ IEWQK WXPSA SMUWH S
a ri  ar ed rarin dodos  o en s ue  u ia  a  u  a
```

A simples observação desta semi-decifração e as letras que nos faltam atribuir levam-nos (depois de algumas tentativas falhadas) a concluir que

$$E(\texttt{t}) = \texttt{Y} \text{ e } E(\texttt{m}) = \texttt{A}.$$

Agora, simplesmente pelo sentido, consegue-se completar o texto, e completar a chave:

```
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
S L M D Q K X U P B   N A J R C E T I Y W H       Z
```

Este tipo de ataque a uma cifra monoalfabética é conhecido desde há muito. Um livro redescoberto em 1987 do matemático árabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi (801-873) com o título "Um manuscrito sobre como decifrar mensagens criptográficas" discute pormenorizadamente o ataque a uma cifra mono-alfabética

com recurso a tabelas de frequência de caracteres. Apesar disso, na Europa, só no século XVI é que as cifras monoalfabéticas caiem em desuso pela evidência da sua fragilidade.

Para poderem pôr em prática as técnicas que aqui descrevemos, para "quebrar" criptogramas destas cifras seguem-se 4 desafios criptográficos (de dificuldade crescente):

1) Como foram mantidos os espaços e pontuações, este é muito simples de resolver, até por se tratar de uma cifra de César:

`Jcnxyjr xjruwj ywjx qfitx szrf inxhzxxft: t rjz qfit, t yjz qfit j t qfit htr wfeft!`

2) Neste, foram removidos os espaços e pontuações:

`QGZMA FQZTA YQPAP MYADF QEAZM ACGQD`

`AQEFM DBDQE QZFQZ QEEQY AYQZF A`

3) Mais uma vez, mantendo os espaços e pontuações, mas com uma cifra que necessita dos ensinamentos de Al Kindi.

`Db ugoqj thg ebearg osbng kgmg hb rbaxgm ebegrj. Pj ltb itiog hb fbhemj pb b g rboahg qbmobamg jt g rboahg ltgmqg.`

4) Finalmente um criptograma mais complicado de "quebrar", especialmente porque não é particularmente longo.

`SHOWH MSABP JAWGE SAHMS ARAAH KPAQR WSHES WPYWD NSTWM`

`SWIYJ LWZQJ GHWQM SAJAV BEAYA TJGRW IJAVW DRJHJ HAIRJ`

`AHMSA DJHAD WWDNJ TAP`

Como havia sido avisado no início, este minúsculo passeio pela Criptografia, e neste caso pela criptografia histórica, quase nada trouxe das profundas e profícuas ligações com a Matemática. Essas pressupõem conhecimentos de Teoria da Complexidade, Teoria dos Números e Teoria da Informação, ficando portanto muito para lá dos propósitos de um pequeno texto como este. Fica, no entanto, a esperança de se ter suscitado a curiosidade sobre uma matéria de inegável actualidade e que viu desenvolvimentos absolutamente espetaculares nas últimas décadas. Para os mais curiosos, recomenda-se para além da consulta dos livros já citados para o que respeita à criptografia histórica, a leitura de [CM13] e [Gal12] para um estudo mais aprofundado da Criptografia de hoje.

Referências Bibliográficas

[CM13] Margaret Cozzens and Steven J. Miller. The Mathematics of Encryption. An Ellementary Introduction. American Mathematical Society, 2013.

[Gai39] Helen Fouché Gaines. Cryptanalysis. A study of ciphers and their resolution. Dover Publications, 1939.

[Gal12] Steven D. Galbraith. Mathematics of Public Key Cryptography. Cambridge University Press, 2012.

[Gar72] Martin Gardner. Codes, Ciphers and Secret Wrinting. Dover Publications, 1972.

[Kah67] David Kahn. The Codebreakers. The Story of Secret Writing. Scribner, 1967.

[Sin99] Simon Singh. The Code Book. Fourth Estate, 1999.