Um pouco da história da criptografia

Fernanda Taline da Silva [1], Fabiana Garcia Papani [2]

[1] Acadêmica do Curso de Matemática – Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste do Paraná
Caixa Postal 711 – 85.819-110 – Cascavel – PR – Brasil
fertalinesilva@hotmail.com

[2] Colegiado do Curso de Matemática – Centro de Ciências Exatas e Tecnológicas da Universidade Estadual do Oeste do Paraná
Caixa Postal 711 – 85.819-110 – Cascavel – PR – Brasil
fgarciapapani@gmail.com

Resumo. *Este trabalho traz um breve resumo da história da criptografia e, mostra a relevante presença da matemática na Teoria dos códigos.*

Palavras chaves. *Criptografia, História dos códigos, Cifra.*

1. Introdução

Generais, reis e rainhas, durante milênios, buscavam formas eficientes de comunicação, de comandar seus exércitos e de governar seus países. A importância de não revelar segredos e estratégias às forças inimigas, motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem, possibilitando apenas ao destinatário ler o conteúdo. As nações passaram a criar departamentos para elaborar códigos, por outro lado, surgiram os decifradores de códigos, criando uma corrida armamentista intelectual. As diversas formas e utilidades dadas aos códigos ao longo do tempo mostram a presença fundamental da matemática na evolução de tal teoria. E evolução é um termo bem apropriado, já que todo código sempre está sob o ataque dos decifradores. Ao desenvolver uma nova arma, relevando a fraqueza de um código, este deixa de ser útil, sendo necessário então, a criação de um novo código que prospera até que decifradores identifiquem suas fraquezas, e assim por diante.

Ao longo da história, os códigos decidiram o resultado de batalhas. À medida que a informação se torna cada vez mais valiosa, o processo de codificação de

mensagens tem um papel cada vez maior na sociedade.

> *Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. .(SINGH, 2007, p.13).*

É comum encontrar relatos na história, de episódios envolvendo os códigos em operações durante guerras, onde criptoanalistas desvendaram o código dos criptógrafos "inimigos", mas mantiveram tal informação em sigilo, a fim de impedir que novos códigos fossem criados para substituir o decifrado. Assim podiam obter informações extremamente importantes para e táticas de defesa e ataque.

2. Esteganografia e Criptografia

A comunicação secreta, constituída da ocultação da mensagem, é conhecida como *esteganografia,* do grego, *steganos,* que significa coberto, e *graphein,* que significa escrever. Um exemplo interessante de *esteganografia* é encontrado em "*As histórias",* onde Heródoto narrou os conflitos entre Grécia e Pérsia, ocorridos no século V a.C.. Uma das histórias é a de Histaeu, que queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para transmitir suas instruções em segurança, Histaeu raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo crescesse. O mensageiro, que aparentemente não levava nada que o comprometesse, viajou sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça, possibilitando a leitura da mensagem pelo destinatário. É evidente que a época tolerava tamanha lentidão.

O grande período em que a esteganografia perdurou, demonstra que ela certamente oferece certa segurança, embora sofra de uma fraqueza fundamental: Se o mensageiro for revistado e a mensagem descoberta, então o conteúdo da comunicação secreta é imediatamente revelado. A interceptação da mensagem compromete toda a sua segurança.

Juntamente com o desenvolvimento da *esteganografia,* houve a evolução da *criptografia,* do grego *kriptos*, que significa oculto. Ao contrário da esteganografia, a criptografia tem como objetivo ocultar o significado da mensagem e não a mensagem propriamente dita. Um bom exemplo de criptografia é a brincadeira infantil, onde crianças mandam bilhetes codificados. Suponhamos que desejamos enviar a seguinte mensagem: "Temos prova de matemática, o que acha de estudarmos hoje à tarde?". Intercalamos então, as letras da mensagem e as letras do nome do remetente, por exemplo: Fernanda, escondendo assim seu significado. Desta forma, a mensagem codificada fica: "Fteermnoas npdraofvea rdne amnadtaefmeartniacna, daamfaenrhna ao nqduae faecrhna adne deasfteurdnaarnmdoas fheorjne aa ntdafredren?", a qual enviamos, sem ocultar.

A vantagem da criptografia é que, se o inimigo interceptar a mensagem codificada, ela está, a princípio, ilegível e seu conteúdo não poderá ser descoberto de

imediato. Nasce então a *criptoanálise,* ciência que permite decifrar uma mensagem sem conhecer a chave.

3. Cifra de substituição monoalfabética

Por volta do século X, os administradores árabes usavam a criptografia para codificar os segredos de Estado e proteger o registro de impostos. Geralmente, utilizavam um alfabeto cifrado apenas rearranjando o alfabeto original, mas também empregavam alfabetos que continham outros símbolos, a essa cifra se dá o nome de *Cifra de substituição monoalfabética,* onde cada letra do alfabeto original é substituída por outra letra ou por um símbolo. Esta cifra permaneceu invulnerável por séculos.

Era comum deslocar as letras do alfabeto, por exemplo, como na tabela 1, o alfabeto utilizado para cifrar uma mensagem tem início na letra H.

Tabela 1. Alfabeto cifrado

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

Desta forma, a mensagem “Esta é a cifra de substituição monoalfabética” após codificação se torna “Lzah l h jpmyh kj zbizapabpjhv tvuvhemhilapjh”. Vale observar que às pontuações também podem ser atribuídos símbolos ou números, assim como aos espaços entre as palavras.

Foram os estudiosos árabes que inventaram a criptoanálise, definida anteriormente, ao obterem sucesso na descoberta de um método para quebrar a cifra de substituição monoalfabética.

4. Análise de freqüência

No século IX, Al-Kindi, um cientista conhecido como “o filósofo dos árabes”, inspirado em técnicas utilizadas por teólogos para examinarem as revelações contidas no Corão, descreveu a técnica de estudar a freqüência das letras para quebrar códigos. O sistema consistia basicamente em conhecendo seu idioma, encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página. Então contar a freqüência com que cada letra aparece. Em seguida examinar o criptograma que se deseja decifrar e também classificar seus símbolos, com relação à freqüência com que aparecem na mensagem. É coerente fazer uma correspondência entre as letras e os símbolos mais freqüentes.

Analisando, por exemplo, uma mensagem codificada na língua portuguesa, pode-se dizer que o símbolo mais freqüente na mensagem corresponde é letra A.

Analogamente, o segundo símbolo mais freqüente corresponde à letra E, e assim por diante. Vale observar que há letras que aparecem com a mesma freqüência, mas substituindo os símbolos mais freqüentes torna-se mais fácil decifrar o restante, justamente por conhecer o idioma da mensagem e, conseqüentemente, suas palavras.

5. Cifra de Vigenère

Os criptoanalistas estavam vencendo a guerra contra os criptógrafos. Cabia aos criptógrafos criar uma nova cifra, mais forte, algo que pudesse vencer os criptoanalistas. Por volta de 1460, o italiano Leon Battista Alberti (1404 – 1472), escreveu um ensaio sobre o que ele acreditava ser uma nova forma de cifra: Naquela época todas as cifras de substituição exigiam um único alfabeto cifrado para codificar cada mensagem. Alberti propôs o uso de pelo menos dois alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial. A grande vantagem do sistema de Alberti é que a mesma letra do texto original não aparece necessariamente como uma única letra no texto cifrado. Embora houvesse descoberto o avanço mais relevante das cifras num período de um milênio, Alberti não conseguiu desenvolver sua idéia: de transformá-la num sistema completo de cifragem. Esta tarefa coube a um grupo de intelectuais que aperfeiçoaram a idéia original, o alemão Johannes Trithemius (1462 – 1516), depois o italiano Giovanni Porta (1541 - 1615), e por fim o francês Blaise de Vigenère (1523 - 1596). Este último tomou conhecimento dos trabalhos e examinou em detalhes as idéias de Alberti, Trithemius e Porta, mesclando-as para formar uma nova cifra, coerente e poderosa. A cifra ficou conhecida como cifra de Vigenère em homenagem ao homem que a desenvolveu em sua forma final.

A cifra de Vigenère consiste em até 26 alfabetos distintos (tabela 2) para criar a mensagem cifrada. O primeiro passo é montar o chamado quadrado de Vigenère, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. Em resumo, o remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante.

Tabela 2. Quadrado de Vigenère

	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**
1	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	A
2	C	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
3	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
4	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	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

Para decifrar a mensagem, o destinatário precisa saber que linha do quadrado Vigenère foi usada para a cifragem de cada letra, por isso deve existir um sistema previamente combinado para a mudança entre linhas. Conseguia-se isso por intermédio do uso de uma palavra-chave. O comunicado “Caros, informo a todos que outra vez os criptógrafos estão na frente na corrida dos códigos”, pode ser codificado como “Eaick, knwcjoo r hgfoj emg olhjc vvn gu ciwhvoxfshoj skvaf bs hrvblg nr qgtrzrs foj qgfixck”, sendo que a palavra-chave é a primeira palavra, ou seja, toda a mensagem foi codificada usando cinco dos vinte e seis alfabetos de Vigenère. Mais especificamente, a primeira letra da mensagem foi codificada com o alfabeto que tem início em C, a segunda com o alfabeto que tem início na letra A, a terceira com o alfabeto que inicia em R, a quarta com o que inicia em O, a quinta com o que inicia em S, a sexta volta a ser codificada com o alfabeto que inicia em C e, assim por diante.

A grande vantagem da cifra de Vigenère é que ela é imune à análise de freqüência. Além disso, a cifra tem um número enorme de chaves. Um criptoanalista não conseguiria decifrar a mensagem procurando todas as chaves possíveis, porque o número de opções é simplesmente grande demais: 26^{26}. A cifra polialfabética de Vigenère era considerada indecifrável e tornou-se conhecida pela expressão francesa *Le chiffre indéchiffable.* Finalmente os criptógrafos estavam em vantagem sobre os criptoanalistas.

5. Criptografia na atualidade

A criptografia estuda métodos para codificar uma mensagem de forma que apenas seu destinatário legítimo consiga interpretá-la. A possibilidade de comunicação entre computadores pela internet trouxe novos desafios para a criptografia. Por ser relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis, como transações bancárias ou comerciais, ou até mesmo uma compra feita com cartão de crédito.

Imagine que uma empresa envia a um banco uma autorização para uma transação de milhões de reais. Dois problemas imediatamente surgem. Primeiro que é preciso proteger a mensagem para que não possa ser lida, mesmo que seja interpretada por uma concorrente, ou por um ladrão de bancos. Por outro lado, o banco precisa ter certeza de que a mensagem foi enviada por um usuário da empresa, ou seja, como se a mensagem estivesse assinada. Desta forma, tornou-se necessário inventar novos códigos, que mesmo com a ajuda de um computador, fossem difíceis de decifrar. Estes códigos não foram criados para a comunicação entre espiões e sim, para o uso em aplicações comerciais.

Na década de 70, surgiu na Califórnia, com Whitfield Diffie, Martin Hellman e Ralph Merkle, a idéia da cifra assimétrica, onde diferentemente dos códigos criados anteriormente, saber codificar não implica em saber decodificar. A fim de desenvolver esta forma de criptografia, a idéia era encontrar uma função de mão única que, como o nome sugere, fosse irreversível. É como quebrar um ovo: quebrar é fácil, mas impossível fazer o ovo voltar a sua condição inicial. Começou assim um frenético estudo para encontrar uma função matemática apropriada.

Diffie publicou um resumo de sua idéia em 1975, a partir daí, outros cientistas se uniram em busca de uma função de mão única que preenchesse os requisitos de uma cifra assimétrica. Inicialmente havia um grande otimismo, mas os meses se passavam e, parecia cada vez mais provável que as funções de mão única não existissem. A idéia do trio funcionaria na teoria, mas não na prática, já que apesar do esforço, não descobriram uma função apropriada e, conseqüentemente, a cifra assimétrica não se tornava realidade.

Em 1977, na costa Leste dos Estados Unidos, Ronald Rivest, Adi Shamir e Leonard Adleman, encontraram uma função capaz de colocar em prática a idéia do trio californiano. Surge assim, no Massachusetts Institute of Technology, a criptografia RSA, em homenagem a Rivest, Shamir e Adleman. Até hoje, o RSA é o mais conhecido dos métodos de criptografia de chave pública, nome dado ao sistema de criptografia assimétrica, onde são usadas duas chaves distintas e uma delas é disponibilizada publicamente, uma vez que a chave utilizada para cifrar uma mensagem não é capaz de decifrar a mesma.

7. Referências

SINGH, S. O livro dos códigos. São Paulo: Editora Record. 2001. 446p.