UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
CURSO DE LICENCIATURA EM MATEMÁTICA

FELIPE QUEIROGA CAVALCANTI

É A MATEMÁTICA IMPORTANTE NA HISTÓRIA DA CRIPTOGRAFIA?

CAMPINA GRANDE - PB
2017

FELIPE QUEIROGA CAVALCANTI

É A MATEMÁTICA IMPORTANTE NA HISTÓRIA DA CRIPTOGRAFIA?

Trabalho de Conclusão de Curso apresentado ao curso de Graduação em Licenciatura Plena da Matemática da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Licenciado em Matemática.
Área de concentração: Educação Matemática.

Orientador: Prof. Dr. José Lamartine da Costa Barbosa.

CAMPINA GRANDE - PB
2017

C376e Cavalcanti, Felipe Queiroga.
É a matemática importante na história da criptografia? [manuscrito] : / Felipe Queiroga Cavalcanti. - 2017.
41 p. : il. colorido.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2017.
"Orientação : Prof. Dr. José Lamartine da Costa Barbosa, Coordenação do Curso de Matemática - CCT."

1. Matemática. 2. Criptografia. 3. Criptografia - História. 4. Teoria dos números.

21. ed. CDD 512.7

FELIPE QUEIROGA CAVALCANTI

É A MATEMÁTICA IMPORTANTE NA HISTÓRIA DA CRIPTOGRAFIA?

Artigo, apresentado ao Curso de Graduação em Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Licenciado em Matemática.

Área de concentração: Educação Matemática.

Aprovada em: 12/12/2017.

BANCA EXAMINADORA

Prof. Dr. José Lamartine da Costa Barbosa (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. Ms. Katia Suzana Medeiros Graciano
Universidade Estadual da Paraíba (UEPB)

Prof. Dra. Maria Isabelle Silva
Universidade Estadual da Paraíba (UEPB)

A minha mãe, pela dedicação, companheirismo e amizade e aos meus dois irmãos, os quais me deram forças e apoio para chegar até aqui, DEDICO.

AGRADECIMENTOS

Em primeiro lugar à Deus, por ser essencial em minha vida e permitiu que tudo isso acontecesse.

À Prof. Ms. Kátia Suzana Medeiros Graciano, coordenadora do curso de Licenciatura em Matemática, por seu empenho.

À meu orientador, Prof. Dr. José Lamartine da Costa Barbosa pelas leituras sugeridas ao longo dessa orientação e pela dedicação.

À minha mãe Maria José Queiroga, que me deu apoio, incentivo nas horas difíceis, de desânimo e cansaço.

Aos meus dois irmãos; Thiago e Emanuel, pois foram eles que me ajudaram a conquistar essa vitória, além de estarem ao meu lado batalhando junto para que eu realizasse este sonho.

Aos professores do Curso de Licenciatura em Matemática da UEPB, em especial, Prof. Ms. José Elias da Silva, Prof. Ms. Maria José Neves de Amorim Moura, que contribuíram ao longo desses anos, por meio das disciplinas e debates, para minha formação acadêmica.

Ao Prof. Dr. Vandenberg Lopes Vieira por ter comentado esse tema em suas aulas.

Aos colegas de classe e amigos pelos momentos de amizade e apoio.

"Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real."

(Lobachevsky)

"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, e 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, porque os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação." (Simon Singh)

LISTA DE FIGURAS

LISTA DE TABELA

LISTA DE SÍMBOLOS

$\forall$	qualquer que seja
$\rightarrow$	implica
$\leftrightarrow$	se, e somente se
$\in$	pertence
$\notin$	não pertence
$\emptyset$	o conjunto vazio
$\blacksquare$	fim de uma demonstração
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{N}$	conjunto dos números naturais
$a \mid b$	a divide b
$a \nmid b$	a não divide b
PBO	princípio da boa ordenação
min L	menor elemento do conjunto L
mdc	máximo divisor comum
mdc(a, b)	máximo divisor comem de a e b
$\equiv \pmod{m}$ ou $\equiv_m$	relação de congruência módulo m
$a \equiv b \pmod{m}$	a é congruente a b módulo m
$a \neq b \pmod{m}$	a não é congruente a b módulo m

SUMÁRIO

RESUMO

Nossa proposta de artigo pretende mostrar que a Criptografia na história do mundo não é uma linguagem exclusiva da matemática. Para atingirmos tal objetivo fizemos uma pesquisa bibliográfica considerando como fontes livros, dissertações e artigos. Concluímos que a Matemática ocupa um espaço fundamental na história da Criptografia.

Palavras-Chave: História. Criptografia. Matemática.

A HISTÓRIA DA CRIPTOGRAFIA

Felipe Queiroga Cavalcanti*

1. Introdução

A nossa intenção de compreender melhor a História da Criptografia é antiga. Daí levantar a seguinte questão de pesquisa, a Criptografia RSA é uma linguagem exclusiva da Matemática?

Justificamos nossa intenção por acreditarmos ser um tema de grande relevância na história e ser uma necessidade no cotidiano das pessoas sendo essencial compreender a importância da Criptografia. Estudar os métodos de codificar mensagens de tal forma que apenas o destinatário consiga decodifica-la e o funcionamento do sistema de criptografia RSA, discutindo toda a matemática necessária para a percepção, onde são demonstrados o Teorema de Fermat, o Teorema Chinês dos Restos e o Teorema de Euler, bem como são abordadas as questões de dificuldade de se fatorar números inteiros e de gerar números primos.

Portanto, o presente trabalho pretende mostrar a importância da Criptografia na história do mundo até os dias de hoje. Assim, como a influência da matemática na resolução dos cálculos e na quebra dos códigos. Partindo de como surgiu, onde foi utilizado nos grandes momentos históricos como a segunda guerra mundial e a linguagem matemática utilizada para desvendar os códigos que detalharemos o tema.

Registramos, a nossa pesquisa é de caráter qualitativo e do tipo bibliográfica, que segundo (GIL, 1994, P.72-73) são necessários os seguintes passos: a) determinar os objetivos; b) elaborar um plano de trabalho; c) identificar as fontes; d) localizar as fontes e obter o material; e) ler o material; f) fazer os apontamentos; g) confeccionas fichas; e h) redigir o trabalho.

Seguimos literalmente esses passos, sempre com o cuidado, de citarmos os autores quando de suas concepções. Concepções essas postas em livros e artigos, fontes de ossa investigação.

* Aluno de Graduação em Licenciatura Plena em Matemática na Universidade Estadual da Paraíba – Campus I. E-mail: filipeqc6@hotmail.com.

2. Evolução da Criptografia

A criptografia é tão antiga quanto a própria escrita, visto que já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. Com as guerras mundiais e a invenção do computador, a criptografia cresceu incorporando complexos algoritmos matemáticos (MORENO; PEREIRA; CHIARAMONTE, 2005).

Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos. Ao mesmo tempo, todos estavam cientes das consequências de suas mensagens caírem em mão erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo (SINGH, 2008).

O primeiro exemplo documentado da escrita cifrada relaciona-se aproximadamente ao ano de 1900 a.C, quando o escriba de Khnumhotep II teve a ideia de substituir algumas palavras ou trechos de texto. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome perdido nas catacumbas da pirâmide (KANH, 1967).

O sistema do escriba era simples, pois ele não usou nenhum código desenvolvido de substituições de símbolos hieroglíficos. Assim, KANH (1967, p. 65, tradução nossa) afirma: “Deste modo a inscrição não foi escrita secreta, mas incorporou um dos principais elementos considerados essenciais da criptografia: uma transformação deliberada da escrita. É o mais antigo texto conhecido a fazê-lo”.

A criptografia surgiu nestas ideias de sigilo e transformação de palavras. Indiscutivelmente a criptografia se desenvolveu, assim como muitas ciências, contudo é o Egito o berço dessa ciência. Outra civilização bastante importante é a Grécia, que desenvolveu alguns tipos de mensagens criptografadas, destacando-se para uns dos primeiros relatos sobre escritas secretas datam de Heródoto, “o pai da história”, de acordo com o filósofo e estadista romano Cícero. Segundo Heródoto, foi a arte da escrita secreta que salvou a Grécia de ser conquistada por Xerxes, Rei dos Reis, o déspota líder dos persas. O desafio era como enviar a mensagem sem que ela fosse interceptada pelas guardas. Heródoto escreveu:

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos. (SINGH, 2008, p. 20)

Um outro método de ocultação para garantir a transmissão segura de mensagem, foi 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 do mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo voltasse a crescer.

O mensageiro, que aparentemente não levava nada que fosse perigoso, pôde viajar sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça e a virou para o destinatário da mensagem (SINGH, 2008).

Essas estratégias de ocultação de mensagem, é conhecida como esteganografia, derivado das palavras gregas steganos, que significa coberto, e graphein, que significa escrever. Em paralelo com o desenvolvimento da esteganografia, houve a evolução da criptografia, Segundo COUTINHO (2015, p. 1) A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário consiga interpretá-la. É a arte dos "códigos secretos". Para tornar a mensagem incompreensível, o texto é misturado de acordo com um protocolo específico, que já foi estabelecido previamente por ambos transmissor e receptor. A vantagem da criptografia é que, se o inimigo interceptar a mensagem codificada, ela será ilegível e seu conteúdo não poderá ser percebido.

A princípio criptografia e esteganografia podem parecer o mesmo tipo de ciência/técnica, porém a grande diferença consiste que a esteganografia propriamente dita não altera a mensagem de alguma forma, apenas esconde em algum lugar previamente combinado para que a pessoa que deve recebe-la a encontre sem mais problemas, enquanto que a criptografia altera a disposição de escrita da mensagem mas não se importa em tentar esconder o fato de que há uma troca de informações entre pessoas ou instituições diferentes (COUTO, 2008).

Dos dois tipos de comunicação secreta a criptografia é o mais poderoso, devido a sua capacidade de impedir que a informação caia em mãos inimigas. Por sua vez, a criptografia pode ser dividida em dois ramos, conhecidos como transposição e substituição. Na transposição, as letras da mensagem são simplesmente rearranjadas, gerando, efetivamente, um anagrama. (SINGH, 2008). Por exemplo, a palavra SER, pode ser cifrada em 5 (3! -1) anagramas distintos: RES, RSE, ERS, ESR e SRE. Já a palavra TEORIA pode originar 719 (6! – 1) anagramas diferentes. Se considerarmos a frase: RONALDO REGRESSA AO SPORTING, existem mais de 1,87 × 1020 formas de combinar as letras desta curta frase ($\frac{25!}{4!\,x4!x2!x3!x2!x3!}$). À medida que o número de letras aumenta no texto, o número de combinações das letras trocadas de uma forma aleatória aumenta de uma forma exponencial, o que dificulta a recuperação da mensagem original por qualquer intruso (FIARRESGA, 2010).

Como não podia deixar de ser, os gregos são responsáveis também pelo primeiro registro do uso da criptografia de transposição para fins militares: o Citale espartano. O citale consiste num bastão de madeira em volta do qual é enrolada uma tira de couro ou pergaminho. O remetente escreve a mensagem ao longo do comprimento do citale e depois desenrola a tira, que agora parece conter uma série de letras sem sentido. A mensagem foi misturada. O mensageiro então leva a tira de couro, e num toque esteganográfico ele às vezes pode escondê-la usando-a como cinto, com as letras ocultas na fase de dentro. Para decodificar a mensagem, o destinatário simplesmente enrola a tira de couro em torno de um citale de mesmo diâmetro do que foi usado pelo remetente (SINGH, 2008).

Figura 1- **Scytale Espartano**

Fonte: Wikipédia, disponível em https://en.wikipedia.org/wiki/File:Skytale.png. Acesso em 08/11/2017.

Na substituição, as letras do alfabeto são emparelhadas ao acaso. Esse método foi usado bastante pelo imperador Júlio César que trocavam as mensagens secretas com seus generais. A cifra de César como é conhecido, consistir em substituir cada letra da mensagem por outra letra três posições à frente. Esse método é conhecido como *Cifras Monoalfabéticas.* Segundo SINGH (2008, p.26) A cifra é o nome dado a qualquer forma de substituição criptográfica, no qual cada letra é substituída por outra letra ou símbolo.

Figura 2 - **Cifra de César**

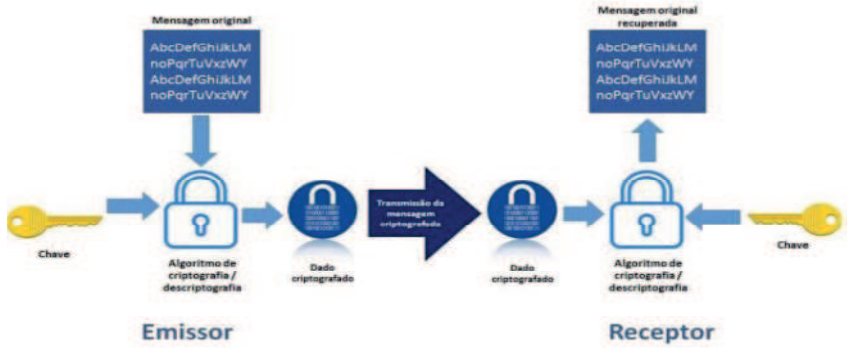
A cifra de César aplicada a uma mensagem curta. Esta cifra é baseada num alfabeto cifrado, deslocado um determinado número de casas (neste caso, três) em relação ao alfabeto original. Por convenção, na criptologia escreve-se o alfabeto correto em minúsculas e o alfabeto criptografado em maiúsculas. Da mesma forma, a mensagem original, o texto correto, é grafado em minúsculas e a mensagem cifrada, em maiúsculas.

Fonte: SINGH, 2008, p. 27.

Com a cifra de César pode-se deslocar as letras entre uma e 25 casas, o que é possível criar 25 códigos distintos, assim existem mais de 400.000.000.000.000.000.000.000.000 rearranjos. Segundo SINGH (2008, p. 27) Cada cifra pode ser considerada em termos de um método geral de codificação como *algoritmo* e uma *chave*, que especifica os detalhes exatos de uma codificação em particular. Neste caso, o algoritmo consiste em substituir cada letra do alfabeto original por uma letra do alfabeto cifrado, e o alfabeto cifrado pode consistir em qualquer rearranjo do alfabeto original. A chave define o alfabeto exato que será usado em uma codificação em particular.

A importância da chave, em oposição ao algoritmo, é um princípio constante da criptografia, como foi definido de modo definitivo em 1883 pelo linguista holandês Auguste Kerckhoff von Nieuwenhof, em seu livro La Cryptographie Militaire. Este é o Princípio de Kerckhoff: "A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave." (SINGH, 2008).

Figura 3 - **Diagrama de uma transmissão segura / criptografada**



Fonte: Google, disponível em https://www.embarcados.com.br/intel-edison-comunicacao-segura-openssl/
Acesso em 10/11/2017

A aplicação da chave e do algoritmo a uma mensagem resultará em uma mensagem cifrada, ou texto cifrado. O texto cifrado pode ser interceptado pelo inimigo enquanto é transmitido ao receptor, mas o inimigo não conseguirá decifrar a mensagem. O receptor, contundo, que conhece a chave e o algoritmo utilizados pelo emissor, pode converter o texto cifrado na mensagem original (SINGH, 2008).

Assim, se numa mensagem foi usado o algoritmo de substituição que consista em qualquer rearranjo do alfabeto original, a verificação das chaves possíveis seria 400.000.000.000.000.000.000.000.000 a cada segundo, o que levaria aproximadamente um bilhão de vezes o tempo de existência do universo para verificar todas elas e decifrar a mensagem.

Foi sua simplicidade e força que fizeram com que a cifra de substituição dominasse a arte da escrita secreta durante o primeiro milênio. Os criadores de códigos tinham desenvolvido um sistema para garantir a segurança das comunicações e portanto não havia necessidade de novos desenvolvimentos – e sem a necessidade, não surgem novas invenções. Contudo, os decifradores de códigos iriam, mais tarde, encontrar um atalho no processo de procurar exaustivamente entre todas as chaves possíveis. E no lugar de levar bilhões de anos para se quebrar uma cifra, o atalho revelava o conteúdo da mensagem em questão de minutos. Essa descoberta foi feita no Oriente, e exigiu uma brilhante combinação de linguística, estatística e devoção religiosa (SINGH, 2008).

2.1. Idade Média: Descobrimento da Criptoanálise

Na idade média, a criptologia teve início 800 anos d.C., época em que o mundo islâmico ultrapassa o europeu nos avanços científicos, devido ao fato dos mulçumanos darem importância a ciência. A chamada Idade de Ouro islâmica (750 d.C. até 1258 d.C.) proporcionou avanços em várias áreas, como nas Artes, na Medicina e na Matemática. Dessa última destacamos os progressos feitos na Trigonometria e na Combinatória, além do

desenvolvimento da álgebra (nome oriundo do termo al-jabr) e dos números indo-arábicos (SINGH, 2001).

Eles (árabes) inventaram a *criptoanálise*, a ciência que permite decifrar uma mensagem sem conhecer a chave. Enquanto o criptógrafo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta. Os criptoanalistas árabes tiveram sucesso na descoberta de um método para quebrar a cifra de substituição monoalfabética, uma cifra que tinha permanecido invulnerável durante vários séculos. A criptoanálise só pode ser inventada depois que a civilização atingiu um nível suficientemente sofisticado de estudo, em várias disciplinas, incluindo matemática, estatística e linguística (SINGH, 2008).

O surgimento da criptoanálise dependia também do crescimento dos estudos religiosos, pois os teólogos interessados em estabelecer a cronologia das revelações o fez contando a frequência das palavras contida na mesma. Em cada língua, quando se faz a contagem do número de vezes que cada letra aparece em textos longos, observamos que cada letra tem uma determinada *frequência relativa*. Através deste fato, os árabes abriram as portas para a criptoanálise (FIARRESGA, 2010).

Figura 4 - **Frequências relativas das letras nos idiomas (adaptado)**

Letra	Francês [8]	Alemão [9]	Espanhol [10]	Português [11]	Esperanto [12]	Italiano[13]	Inglês
a	7.636%	6.51%	12.53%	14.63%	12.12%	11.74%	8.167%
b	0.901%	1.89%	1.42%	1.04%	0.98%	0.92%	1.492%
c	3.260%	3.06%	4.68%	3.88%	0.78%	4.5%	2.782%
d	3.669%	5.08%	5.86%	4.99%	3.04%	3.73%	4.253%
e	14.715%	17.40%	13.68%	12.57%	8.99%	11.79%	12.702%
f	1.066%	1.66%	0.69%	1.02%	1.03%	0.95%	2.228%
g	0.866%	3.01%	1.01%	1.30%	1.17%	1.64%	2.015%
h	0.737%	4.76%	0.70%	1.28%	0.38%	1.54%	6.094%
i	7.529%	7.55%	6.25%	6.18%	10.01%	11.28%	6.966%
j	0.545%	0.27%	0.44%	0.40%	3.50%	0.00%	0.153%
k	0.049%	1.21%	0.01%	0.02%	4.16%	0.00%	0.772%
l	5.456%	3.44%	4.97%	2.78%	6.14%	6.51%	4.025%
m	2.968%	2.53%	3.15%	4.74%	2.99%	2.51%	2.406%
n	7.095%	9.78%	6.71%	5.05%	7.96%	6.88%	6.749%
o	5.378%	2.51%	8.68%	10.73%	8.78%	9.83%	7.507%
p	3.021%	0.79%	2.51%	2.52%	2.74%	3.05%	1.929%
q	1.362%	0.02%	0.88%	1.20%	0.00%	0.51%	0.095%
r	6.553%	7.00%	6.87%	6.53%	5.91%	6.37%	5.987%
s	7.948%	7.27%	7.98%	7.81%	6.09%	4.98%	6.327%
t	7.244%	6.15%	4.63%	4.34%	5.27%	5.62%	9.056%
u	6.311%	4.35%	3.93%	4.63%	3.18%	3.01%	2.758%
v	1.628%	0.67%	0.90%	1.67%	1.90%	2.10%	0.978%
w	0.114%	1.89%	0.02%	0.01%	0.00%	0.00%	2.360%
x	0.387%	0.03%	0.22%	0.21%	0.00%	0.00%	0.150%
y	0.308%	0.04%	0.90%	0.01%	0.00%	0.00%	1.974%
z	0.136%	1.13%	0.52%	0.47%	0.50%	0.49%	0.074%

Fonte: Google, disponível em https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras
Acesso em 10/11/2017

Analisando a tabela da língua portuguesa, podemos agrupar as letras com o nível de frequências:

1º a, e, o	2º s, r, i
3º n, d, m, u, t, c	4º l, p, v, g, h, q, b, f
5º z, j, x, k, w, y	

Um criptoanalista para decifrar uma mensagem, em que foi utilizada uma cifra monoalfabética e cujo texto original foi escrito em português, começa por fazer uma tabela de frequências das letras ou símbolos do texto em cifra. E comparando o valor das frequências relativas das diferentes letras ou símbolos, com os valores da tabela anterior, pode ir substituindo as letras ou símbolos pelas letras que têm percentagens semelhantes até a mensagem fazer sentido (FIARRESGA, 2010).

2.2. Destaques dos Matemáticos Mulçumanos na Evolução da Criptologia

Entre os mulçumanos várias pessoas se destacaram na evolução da criptologia. O filósofo, cientista e matemático al-Kindi é conhecido como o "filósofo dos árabes'', autor do livro intitulado "Um Manuscrito sobre Decifração de Mensagens Criptográficas". Outro destaque é o autor do Kitab al Mu'amma (Livro das Mensagens Criptográficas), chamando al-Khalil. Outro estudioso foi Ibn Dunainir (1187 - 1229) escreveu uma obra intitulada *Maqasid al-Fusul al-Mutarjamah an Hall at-Tarjamah* (Explicações claras para a solução de mensagens secretas). O livro contém uma inovação importante: *cifras algébricas*, ou seja, a substituição de letras por números que podem ser transformados aritmeticamente. Por fim, o professor Ibn Ad-Duraihim (1312 - 1361), famoso por sua engenhosidade em aritmética, criptoanálise, e em resolver enigmas e caça-palavras. Ele é o autor do livro *Miftah al-Kunuz fi Idah al-Marmuz* (Chaves para a Elucidação de Mensagens Secretas) que contém uma classificação das cifras, análises de frequência em várias línguas (SILVA; MARTINS, 2011).

2.3. Idade Moderna: O Surgimento da Cifra Polialfabético

Na Idade Moderna, os europeus começaram a redescoberta pelas velhas cifras de substituição e inventaram novas. No século XIII, o monge franciscano, Roger Bacon, escreveu o livro A Epístola sobre as obras de Arte Secretas e a Nulidade da Magia; o primeiro livro europeu que descreve o uso da criptografia (FIARRESGA, 2010). Um dos casos mais emblemáticos das mudanças ocorridas na concepção de segurança na comunicação dessa época é o da condenação e morte da rainha da Escócia, Maria Stuart, em 1587. A mandante da execução foi a também rainha Elizabeth I, da Inglaterra, que era prima de Maria. A situação toda fora consequência de disputas internas entre Católicos e Protestantes na Inglaterra. Elizabeth temia que sua prima pudesse roubar-lhe o trono por ela ser considerada a herdeira legítima, pela parte católica do país. Por isso a manteve presa por quase duas décadas, até o seu primeiro-secretário, Francis Walsingham, contratar um espião-duplo para contrabandear cartas de simpatizantes de Maria para ela própria e a resposta dela para eles.

As cartas, que eram cifradas, continham detalhes da armação que estava sendo arquitetada para um suposto o assassinato de Elizabeth e a libertação de Maria. No entanto, por ser um nomenclator, sua decifração era bastante fácil através de uma análise de frequência, e a Inglaterra já dispunha nessa época de criptoanalistas trabalhando para a Corte Real. Dessa forma, Walsingham pôde comprovar que Maria compactuava com as ideias de

seus simpatizantes, fornecendo assim provas suficientes para que ela pudesse ser executada. Em 8 de fevereiro de 1587, depois de alguns dias de julgamento e decisão, a rainha da Escócia foi decapitada para uma plateia de 300 pessoas (SILVA; MARTINS, 2011).

Figura 5 - **Execução da Rainha dos escoceses em Fotheringhay, 1587, por autor desconhecido.**

.

Fonte: Google, disponível em https://rainhastragicas.com/2012/07/17/mary-stuart-martir-catolica-ou-dissimulada-conclusao/. Acesso em 14/11/201

A maior evolução da criptografia na Idade Moderna foi: o Disco de Cifra, o primeiro sistema polialfabético conhecido. Leon Battista Alberti publicou, em 1446. O livro Modus scribendi in ziferas, no qual fala sobre o mesmo. O disco de cifra era constituído por dois discos concêntricos e de raios diferentes. O disco maior era fixo, e o menor móvel (FIARRESGA, 2010). Seu sistema de encriptação usava dois discos concêntricos de metal, cujas circunferências eram divididas e 24 partes iguais (COUTO, 2008). Uma das desvantagens deste método, é que emissor e receptor têm que ter dois discos iguais e muito bem guardados; pois a segurança deste sistema depende de ocultar os discos de olhos indiscretos (FIARRESGA, 2010).

Figura 6 - **Disco de Alberti**

Fonte: Google, disponível em https://horaciobacon.wordpress.com/2014/01/03/la-escritura-secreta-parte-iv/
Acesso em 14/11/2017

Embora houvesse descoberto o avanço mais significativo das cifras num período de mil anos, Alberti não conseguiu desenvolver sua ideia, transformando-a num sistema completo de cifragem. Esta tarefa coube a um grupo diferente de intelectuais que

aperfeiçoaram a ideia original. Primeiro apareceu Johannes Trithemius, um abade alemão nascido em 1462, depois Giovanni Porta, um cientista italiano nascido em 1535, e finalmente o diplomata francês Blaise de Vigenère, nascido em 1523 (SINGH, 2008). Como pudemos ver, Alberti, Trithemius e Della Porta deram suas contribuições para o desenvolvimento da cifra polialfabética. No entanto a pessoa que ficou conhecida como quem organizou e simplificou os avanços desses estudiosos foi Blaise de Vigenère (1523 – 1596).

Precisamos, porém, tomar cuidado com essa afirmação. Vigenère, como falamos, ficou conhecido como o responsável pela versão final da cifra, mas o verdadeiro autor dessa façanha foi Giovanni Battista Bellaso (1549 - desconhecido). Fato é que Vigenère produziu uma cifra polialfabética mais robusta que a de Bellaso, porém essa segunda é que foi a mais utilizada após ser criada, por ser mais simples. Equivocadamente essa cifra foi atribuída à Vigenère, sendo reconhecida até hoje como de sua autoria. A cifra que foi realmente criada por Vigenère é a *cifra de Autochave* (SILVA; MARTINS, 2011).

A grande importância do surgimento e desenvolvimento das cifras polialfabéticas é que elas foram as primeiras a causar um desafio realmente notável para os criptoanalistas da época (SILVA; MARTINS, 2011). A força da cifra de Vigenère consiste em que ela usa não apenas um, e sim 26 alfabetos cifrados distintos para criar a mensagem cifrada (SINGH, 2008).

Figura 7 - **Cifra(Quadrado) de Vigenère**

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	W	V	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	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W
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	W	V
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z

Fonte: Google, disponível em http://galileu.globo.com/edic/118/imagens/eureca_01.gif
Acesso em 14/11/2017

As cifras polialfabéticas eram consideradas muito complexas e inapropriadas para serem usadas em guerras, por exemplo. Nesse tipo de situação a agilidade e rapidez no envio de mensagens são essenciais (SILVA; MARTINS, 2011). Em consequência disso, os criptógrafos buscaram uma cifra intermediária, mais difícil de quebrar do que a cifra monoalfabética direta, mas que fosse mais simples de usar do que a cifra polialfabética (SINGH, 2008). Foi onde criou-se a Cifra de Substituição Homofônica, na qual cada letra é

substituída por uma variedade de símbolos proporcional à sua frequência. Por exemplo, a letra "e" na língua portuguesa poderá ser substituída por 12 símbolos distintos, pois sua frequência é de 12,57%, cada vez que a letra "e" for aparecer no texto cifrado, será escolhido ao acaso qual dos 12 símbolos usar, e assim ocorrendo com as demais letras, de modo que no final do texto, cada símbolo representará 1% do texto cifrado, despistando a técnica da análise da frequência (GANASSOLI; SCHANKOSKI, 2015).

Tabela 1 - Cifra de Substituição Homofônica com Frequência do Alfabeto da Língua Portuguesa (Figura 04)

Letra	Freq.%	Cifrante	Letra	Freq.%	Cifrante
A	14,63	00, 26, 52, 78, 104, 130, 156, 182, 208, 234, 260, 286, 312, 490	N	5,05	39, 91, 143, 195, 247
B	1,04	27	O	10,73	67, 92, 118, 144, 170, 196, 222, 248, 274, 300
C	3,88	02, 28, 132, 210	P	2,52	119, 249
D	4,99	55, 107, 159, 185, 263	Q	1,20	172
E	12,57	30, 56, 82, 108, 134, 160, 186, 212, 238, 264, 290, 316	R	6,53	17, 69, 95, 147, 225, 277, 329
F	1,02	83	S	7,81	44, 96, 122, 174, 200, 252, 278, 304
G	1,30	292	T	4,34	71, 149, 227, 331
H	1,28	137	U	4,63	20, 46, 124, 254
I	6,18	112, 138, 164, 190, 216, 242	V	1,67	203
J	0,40	09	W	0,01	100
K	0,02	62	X	0,21	179
L	2,78	37, 89, 167	Y	0,01	24
M	4,74	12, 116, 194, 272, 324	Z	0,47	233

Cifrante é o sistema que substitui cada um dos caracteres do alfabeto por outros caracteres (letras, números, símbolos, etc.).

Tabela 2 - Exemplo da Cifra de Substituição Homofônica

Mensagem	Texto Cifrado
A Matemática é Linda!	26, 272, 490, 71, 212, 12, 104, 149, 190, 02, 156, 160, 89, 112, 91, 159, 00

Um dos melhores exemplos é a *Grande Cifra*, desenvolvida por Antoine Rossignol e seu filho Bonaventure em 1619. Essa cifra era tão forte que só foi quebrada no fim do século XIX. Elaborada para guardar os segredos do rei Luís XIV da França, a cifra dispunha de 587 números diferentes, e continha várias formas de armadilhas, para eventuais criptoanalistas. A dificuldade de decifração era grande porque Rossignol atribuiu números para sílabas, e não para letras individuais. Além disso, quando os criadores faleceram, as regras de decifração foram rapidamente perdidas (SINGH, 2008).

Este método foi mais utilizado do que a Cifra de Vigenère, por ser mais simples de ser usado e por representar certo grau de segurança para a época. Porém, os criptoanalistas também conseguiram quebrá-lo, estudando as letras que apresentam um único símbolo para

representá-la e que fazem parte de dígrafos ou trígrafos comumente usados na língua, deixando evidente que a Cifra de Vigenère oferecia maior segurança. Porém, em 1854, Charles Babbage, matemático britânico já tinha decriptado a Cifra de Vigenère analisando em que frequência as letras se repetiam e descobrindo a palavra-chave usada, mas ele não publicou sua descoberta. Em 1863, Friedrich Kasiski publicou a técnica e então a Cifra de Vigenère não era mais segura oficialmente (GANASSOLI; SCHANKOSKI, 2015).

As cifras monoalfabéticas só foram definitivamente abandonadas após o início do século XVIII, com a criação das chamadas Câmaras Escuras. Segundo Couto (2008) elas consistiam em "grupos ligados aos governos que se dedicam ao estudo e aplicação dos métodos criptográficos". A mais famosa delas é *Geheime Kabinettskanzlei* de Viena, que era liderada pelo barão Ignaz Von Koch. Ela recebia diariamente centenas de cartas, às 7 da manhã, que deveriam ser entregues às embaixadas da cidade. Até as dez da manhã todas elas eram copiadas e seladas novamente, de forma a chegar a seus destinos finais. A partir daí começava a decifração das mensagens pela equipe de criptoanalistas profissionais. As informações descobertas serviam tanto para o governo austríaco como para outras nações dispostas a pagar pelo valioso significado delas (SILVA; MARTINS, 2011).

2.4. Idade Contemporânea: A Revolução na Criptografia

A invenção do Telégrafo elétrico revolucionou as formas de se comunicar, no século XIX. O Telégrafo ajudou ainda a popularizar a criptografia, visto que pessoas comuns que necessitavam utilizar a tecnologia precisavam aprender formas simples de criptografar suas mensagens, para escondê-las pelo menos dos telegrafistas (SILVA; MARTINS, 2011). Essa popularização pode ser vista claramente na Inglaterra Vitoriana, período que vai de 1837 a 1901, onde casais (que eram proibidos de expressar o seu amor em público) mandavam mensagens cifradas através dos jornais de grande circulação nacional (SILVA, MARTINS, 2011).

Segundo SILVA; MARTINS (2011, p. 38) Nessa época, porém, outra grande (e talvez mais importante, para a criptologia) revolução estava acontecendo: a quebra da cifra de Vigenère. Isso aconteceu no ano de 1854, mas só veio à tona em 1863. O responsável por essa façanha foi Charles Babbage (1791 – 1871), que hoje é considerado o pai do computador moderno. Charles Babbage foi a primeira pessoa a conseguir quebrar a cifra de Vigenère. Ele percebeu que uma cifra polialfabética se tratava de nada mais que um conjunto de diferentes cifras monoalfabéticas organizadas em uma sequência, e que, dessa forma, poder-se-ia aplicar também a técnica conhecida como análise de frequências. Portanto, Babbage tinha acabado com um paradigma que já durava havia séculos (SILVA; MARTINS, 2011).

2.5. O Aparecimento da Criptografia Mecânica

No fim do século XIX, a criptografia vivia uma época de confusão. Desde que Babbage e Kasiski tinham destruído a segurança da cifra de Vigenère, os criptógrafos buscavam por uma nova cifra, algo que pudesse restabelecer as comunicações secretas, permitindo que os homens de negócios e os militares explorassem a rapidez do telégrafo sem que seus comunicados fossem roubados ou decifrados (SINGH, 2008). Enquanto isso, outra descoberta mudaria o rumo da história: a possibilidade de comunicação via rádio.

O físico italiano Guglielmo Marconi desenvolveu um sistema no qual poderia enviar mensagens entre longas distâncias sem a necessidade de um fio que ligasse emissor e receptor. Uma vez tendo provada a eficiência da tecnologia, Marconi encantou os militares que viam o sistema como um excelente aliado durante a Primeira Guerra Mundial (SILVA; MARTINS, 2011). Em 1894, com a descoberta do rádio, um importante meio de comunicação que serviu na época para enviar mensagens militares através do código Morse, e sem fios interligando remetente e destinatário, ficou mais fácil a interceptação das mensagens e consequentemente concedeu várias vitórias para os criptoanalistas na Primeira Guerra Mundial (GANASSOLI; SCHANKOSKI, 2015).

A cifra ADFGVX, muito famosa na Primeira Guerra Mundial e que inclui os dois métodos de criptografar, transposição e substituição, foi decifrada em 3 meses de utilização. Seu processo de criptografia consistia em construir um quadro com as 6 letras ADFGVX na horizontal e na vertical e escrever aleatoriamente as 26 letras do alfabeto e mais os 10 dígitos. A escolha das letras ADFGVX, deve-se ao fato de que, as mesmas em código Morse são muito diferentes (GANASSOLI; SCHANKOSKI, 2015).

Figura 8 - **Cifra ADFGVX**

	A	D	F	G	V	X
A	O	1	S	E	G	F
D	2	0	H	A	Y	D
F	R	B	Z	P	4	N
G	Q	9	8	C	T	K
V	3	X	I	7	5	W
X	J	U	6	M	V	L

Fonte: Google, disponível em https://culturacientifica.com/app/uploads/2015/03/imagen-15.png. Acesso em 18/11/2017

Texto Simples: Teoria dos Números
Texto em Cifra: VG GA AA AF FV GA XD AA FA XF DX GX GA AF AA FA
Utilizamos a cifra de substituição, agora utiliza-se uma palavra chave: VOCE para aplicar a cifra de transposição, do seguinte modo:

V	O	C	E
V	G	G	A
A	A	A	F
F	V	G	A
X	D	A	A
F	A	X	F
D	X	G	X
G	A	A	F
A	A	F	A

Tabela 3 - Organização da Cifra ADFGVX com palavra chave

Agora, ordena-se a tabela com a palavra-chave escrita por ordem alfabética, que ficará do seguinte modo:

C	E	O	V
G	A	G	V
A	F	A	A
G	A	V	F
A	A	D	X
X	F	A	F
G	X	X	D
A	F	A	G
F	A	A	A

Tabela 4 - Transposição da Cifra ADFGVX

A mensagem a ser enviada neste caso será a seguinte:

GAGVAFAAGAVFAADXXFAFGXXDAFAGFAAA

2.6. A Máquina Enigma

Em 1918, Arthur Scherbius patenteou uma máquina elétrica e mecânica com rotores, qual pode ser considerada uma versão elétrica da máquina de Alberti, chamada de Enigma, que servia tanto para criptografar como para decriptografar, e foi amplamente usada pelas forças militares alemãs (GANASSOLI; SCHANKOSKI, 2015).

Figura 9 - **Máquina Enigma**

Fonte: Google, disponível em http://s2.glbimg.com/gQV-gn_q-mepGt3zN6vj2AhWHQ0=/s.glbimg.com/jo/g1/f/original/2015/07/15/maquina-enigma-g1.jpg Acesso em 18/11/2017

FIARRESGA (2010, p.22), descreve o funcionamento da máquina Enigma da seguinte maneira:

> *A máquina Enigma utilizada pelos alemães, era formada pelas seguintes componentes: um teclado, uma unidade de cifragem e um painel de visionamento. O operador para cifrar uma mensagem, utilizava o teclado para introduzir as letras do texto simples uma a uma; na unidade de cifragem, cada letra era transformada numa outra; a letra transformada era então comunicada ao operador através do painel de visionamento, onde era acesa a lâmpada correspondente. A unidade de cifragem era composta por três cilindros móveis, que podiam alternar a sua posição dentro da máquina, e um fixo, que se chamava espelho. Cada um dos cilindros contém as vinte e seis letras do alfabeto. Entre o teclado e o primeiro cilindro existe um painel de ligação, que permite a troca de seis pares de letras das vinte e seis do alfabeto. O que eleva bastante o número de chaves que se pode utilizar. Por cada letra cifrada, o primeiro cilindro roda um sexto sempre no sentido direto, quando dá uma volta completa, o segundo cilindro roda também um sexto, após seis voltas do primeiro cilindro, o segundo dá uma volta completa e o terceiro roda um sexto. Ou seja, por cada seis letras cifradas, o segundo cilindro move-se e por cada 36 letras move-se o terceiro, o que permite o uso de 17576 alfabetos de cifra diferentes. Mas não é só no número de alfabetos de cifra que esta máquina é forte, o número de chaves é muito grande. O seu verdadeiro número pode ser calculado da seguinte maneira:*
>
> *1) Para começar, os cilindros podem permutar entre si, como são três, temos 3! = 6;*
> *2) Cada um dos três cilindros pode ser regulado de vinte e seis maneiras diferentes, o que dá* $26^3 = 17576$*;*
> *3) No painel de ligação podem-se trocar seis pares de letras a partir das vinte e seis do alfabeto, o que pode ser feito de*
> $\frac{(26x25)x(24x23)x(22x21)x(20x19)x(18x17)x(16x15)}{2^6x\ 6!} = 100391791500$
> *maneiras diferentes*
>
> *4) Por fim, o número de chaves é dado por: 17576 × 6 × 100391791500 = 1058691676442400.*
> *A colocação dos cilindros, a sua regulação inicial e o conhecimento da troca dos seis pares de letras determinam a chave a usar.*

2.7. Decifrando a Enigma

Durante a Segunda Guerra Mundial, em Blethcheley Park, travou-se uma batalha silenciosa, cujo alvo era quebrar a chave da Enigma (FIARRESGA, 2010). Em 1931, o Biuro Szyfrów, departamento de códigos do Serviço Secreto da Polônia, depois de conseguir uma cópia do projeto da Máquina Enigma, por um traidor alemão, decide contratar matemáticos para decriptografá-la. Entre eles, Marian Rejewski, que dedicou-se muito na quebra da Enigma, depois das suas descobertas, as comunicações da Alemanha ficaram acessíveis.

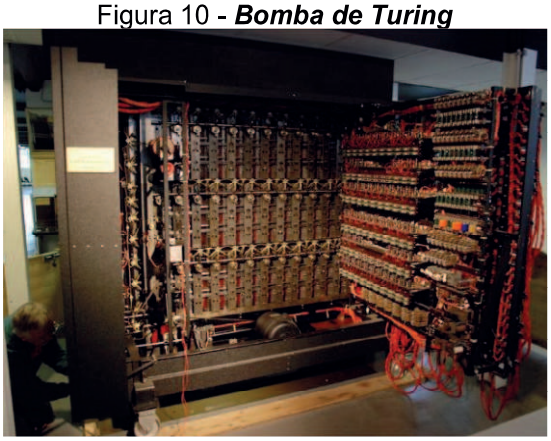
Os Poloneses usaram por vários anos as técnicas de Rejewski, até que os alemães fizeram alterações na transmissão de suas mensagens, em contrapartida, Rejewski, consegue construir outra máquina, chamada de Bomba e decriptografa a Enigma sem os alemães saberem (GANASSOLI; SCHANKOSKI, 2015). Porém, os alemães foram aperfeiçoando a Enigma usando uma combinação maior de rotores e ligações elétricas e em 1939, a Bomba de Rejewski estava ultrapassada e então, os poloneses passaram tudo o que sabiam aos ingleses e franceses antes de serem invadidos pela Alemanha (GANASSOLI; SCHANKOSKI, 2015).

Existe uma figura que deve ser destacada: foi Alan Turing quem identificou a maior franqueza da Enigma e a explorou sem piedade. Graças a Turing tornou-se possível quebrar a cifra da Enigma mesmo sob as circunstâncias mais difíceis (SINGH, 2008).

Em Bletchley Park, Turing empenhou-se em achar outras fraquezas da cifra da Enigma, pois os britânicos imaginavam que os alemães corrigiriam as que eles estavam usufruindo, até então. Por várias semanas o cientista pensou em como poderia realizar essa tarefa, analisando arquivos antigos de mensagens decifradas da Enigma. Notou então que o modo de uso da máquina possuía certos padrões que facilitavam a sua quebra, como mensagens mandadas diariamente, no mesmo horário, com informação sobre o clima, por exemplo.

Elas poderiam ser usadas como cola, porque como eram comunicações militares, obrigatoriamente seguiam um padrão, e certas palavras como “tempo” sempre estariam localizadas em locais específicos. Também descobriu que os alemães nunca usavam os misturadores nas mesmas posições do dia anterior, o que reduzia pela metade as possibilidades para o próximo dia, além de que uma letra nunca poderia ser cifrada por ela mesma ou pelas duas seguintes. Ou seja, a letra “d” não poderia ser cifrada por “d”, “e” ou “f”. Os alemães acreditavam estar dificultando o trabalho dos Aliados com essas medidas, no entanto estavam na verdade tornando suas cifras mais vulneráveis (SINGH, 2008). Alan Turing, criou uma máquina conhecida por Bomba também, devido a semelhança da máquina de Rejewski, após aperfeiçoamentos a nova máquina conseguia encontrar a chave de uma Enigma em uma hora (GANASSOLI; SCHANKOSKI, 2015).

Figura 10 - ***Bomba de Turing***



Fonte: Google, disponível em
https://upload.wikimedia.org/wikipedia/commons/e/ef/Bomba_turninga2.jpg
Acesso em 18/11/2017

2.8. Surgimento da Criptografia Computadorizada

SILVA; MARTINS (2011, p. 47, 48) descreve o surgimento da criptografia computadorizada. Como podemos perceber, as máquinas foram decisivas na Segunda Guerra Mundial. Algumas delas que tinham como função a cifragem de mensagens, e outras a decifragem. Apesar da Enigma ser a mais conhecida, a Alemanha dispunha de outra máquina: a Lorenz SZ40. Ela responsável pela comunicação direta de Hitler e seus generais, e sua cifra era mais complexa que a da Enigma. A quebra dessa cifra não era páreo para as bombas de Turing, pois exigiam certa flexibilidade para as sutilezas da Lorenz. Foi então que o matemático Max Newman projetou um mecanismo de decifragem da máquina de Hitler, baseando-se no conceito criado por Alan Turing. Tratava-se de um computador programável. A partir daí a evolução dos computadores só fez crescer, e com isso, a criptografia e, consequentemente, a criptoanálise também.

3. A Matemática – Teoria dos Números

Os processos pelos quais informações enviadas eletronicamente são codificadas dependem, de maneira crucial, do uso da matemática. O mais curioso é que até os anos 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que destituída de utilidade prática (COUTINHO, 2013).

O entendimento do método RSA depende de alguns conceitos e ideias matemáticas. Destacamos a Teoria dos Números, pois tem por objetivo geral estudar as propriedades dos números inteiros. Segundo VIEIRA (2015) podemos assim apresentá-la:

3.1. Divisibilidade

3.1.2 Definição. Diremos que b **divide** a, em símbolos $b \mid a$, se existir um inteiro c tal que $a = bc$.

Neste caso, diremos também que a é **divisível** por b, que b é um **divisor** de a ou ainda que a é um **múltiplo** de b.

Assim, $b \mid a \leftrightarrow a = bc$ para algum $c \in \mathbb{Z}$.

3.2.1 Teorema. A divisibilidade tem as propriedades:

1) Se $a \mid b$ e $b \mid c$, então $a \mid c$.
2) Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.
3) Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, $\forall\, m, n \in \mathbb{Z}$.

Demonstração: 1) Por hipótese, $b = a\lambda_1$ e $c = b\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Substituindo o valor de b em $c = b\lambda_2$, obtemos $c = a(\lambda_1\lambda_2)$, ou seja, $a \mid c$.

2) Sendo $b = ak_1$ e $d = ck_2$, temos $db = (ac)(k_1k_2)$, isto é, $ac \mid bd$.

3) Temos por hipótese que $b = ak_1$ e $c = ak_2$. Logo, dados inteiros m e n, $mb = amk_1$ e $nc = ank_2$, de modo que $mb + nc = a(mk_1 + nk_2)$. Assim, $a \mid (mb + nc)$.

■

3.2.2 Algoritmo da Divisão. Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$.

Demonstração: Consideremos o conjunto $L = \{a - bq : q \in \mathbb{Z} \text{ e } a - bq \geq 0\}$. Uma primeira coisa a ser verificada é que L é não vazio. De fato, desde que $b \geq 1$, então $a \cdot b \geq a$. logo,

$a - (-a) \cdot b = a + a \cdot b \geq a + a \geq 0$. Como $x = a - (-a) \cdot b$ é da forma $a - bq$, com $q = -a$, segue que $x \in L$. agora, vamos mostrar a existência e unicidade dos inteiros q e r.
(**Existência**) Sendo L limitado inferiormente (por zero, por exemplo) e não vazio, temos pelo PBO que L possui menor elemento, digamos $r = \min L$. Como $r \in L$, então $r \geq 0$ e $r = a - bq$, com $q \in \mathbb{Z}$. Asseguramos que $r < b$. De fato, se isto não ocorrer, então $r - b \geq 0$ e $r - b = a - bq - b = a - b(q + 1)$. Portanto, $r - b \in L$ e $r - b < r$, o que contraria a minimalidade de r. Por conseguinte, $a = qb + r$, com $q \in \mathbb{Z}$ e $0 \leq r < b$, o que prova a existência dos inteiros q e r.
(**Unicidade**) Para a unicidade, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que $a = bq_1 + r_1$, com $0 \leq r < b$. Assim, $bq + r = bq_1 + r_1$, o que implica em $r - r_1 = b(q_1 - q)$, ou seja, $b \mid (r - r_1)$. Como $r - r1 < b$, segue que $r - r_1 = 0$, isto é, $r = r_1$. Por isso, $q_1 = q$, uma vez que $b \neq 0$.

■

3.2.3 Máximo Divisor Comum. Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é o **máximo divisor comum** de a e b quando as seguintes condições são satisfeitas:
a) $d \mid a$ e $d \mid b$.
b) Se $c \mid a$ e $c \mid b$, então $c \mid d$.
Em outras palavras, o máximo divisor comum de a e b é um número natural que os divide e é divisível por todo divisor comum de a e b.

3.2.4 Teorema (Bachet-Bézout). Se $d = mdc(a,b)$, então existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.

Demonstração: Consideremos o conjunto $W = \{ax + by : x, y \in \mathbb{Z} \text{ e } ax + by > 0\}$. Notemos de início que W não é vazio, pois para $x = y = 1$, $a \cdot 1 + b \cdot 1 = a + b > 0 \rightarrow a + b \in W$. Desse modo, pelo PBO, W possui menor elemento, digamos $\lambda = \min W$. Vamos mostrar que $\lambda = mdc(a,b)$. Como $\lambda \in W$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $\lambda = ax_0 + by_0$. *
Usando o Algoritmo da Divisão com os elementos a e λ, temos $a = \lambda q + r$, com $0 \leq r < \lambda$. Substituindo o valor de λ em * na igualdade de $0 \leq r < \lambda$, segue que: $r = a - \lambda q = a - (ax_0 + by_0)q = a - aqx_0 - bqy_0$. Daí, $r = a(1 - qx_0) + b(-qy_0)$.
Isso nos mostra que $r = au + bv$, com $u = 1 - qx_0$ e $v = -qy_0$. Por conseguinte, $r = 0$, pois do contrário, $r > 0$ e, assim, $r \in W$, o que contraria o fato de λ ser o mínimo de W, visto que $r < \lambda$. Portanto, $a = \lambda q$, ou seja, $\lambda \mid a$. Similarmente, prova-se que $\lambda \mid b$. Sendo $d = mdc(a,b)$, então $a = d\lambda_1$ e $b = d\lambda_2$. Logo, por *, $\lambda = (d\lambda_1)x_0 + (d\lambda_2)y_0 = d(\lambda_1 x_0 + \lambda_2 y_0)$, ou seja, $d \mid \lambda$, e como $\lambda \mid d$, pois $d = mdc(a,b)$, segue que $d = \lambda$. Logo, $d = ax_0 + by_0$.

■

3.2.5 Algoritmo de Euclides. Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.

Demonstração: É suficiente mostrar que $D_a \cap D_b = D_b \cap D_r$, pois se estes conjuntos forem iguais, seus máximos também serão iguais. Se $d \in D_a \cap D_b$, então $d \mid a$ e $d \mid b$; mas como $r = a - qb$, segue que $d \mid r$ e, por isso, $d \in D_b \cap D_r$. Por outro lado, se $d \in D_b \cap D_r$, então $d \mid b$ e $d \mid r$, de modo que $d \mid bq + r = a$, isto é, $d \in D_a \cap D_b$. Logo, $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc(a,b) = mdc(b,r)$.

Consideremos os inteiros a e b, com $a > b > 0$. Pela Divisão Euclidiana, temos $a = b.q_1 + r_1$, com $0 \leq r_1 < b$.

De acordo com a demonstração anterior, $mdc(a, b) = mdc(b, r_1)$. Temos dois casos a considerar:
1) Se $r_1 = 0$, então $mdc(a, b) = mdc(b, r_1) = mdc(b, 0) = b$.
2) Se $r_1 \neq 0$, então efetuando a divisão de b por r_1, obtemos $b = r_1 \cdot q_2 + r_2$, com $0 \leq r_2 < r_1$.
Da mesma forma,

3) Se $r_2 = 0$, segue que $mdc(a, b) = mdc(b, r_1) = mdc(r_1, 0) = r_1$.
4) Se $r_2 \neq 0$, então efetuando a divisão de r_1 por r_2, temos $r_1 = r_2 \cdot q_3 + r_3$, com $0 \leq r_3 < r_2$.

Mais uma vez, procedendo como antes, $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3)$, e assim sucessivamente. Deve, portanto, existir um índice n tal que $r_n \neq 0$ e $r_{n+1} = 0$, pois caso contrário, obteríamos uma sequência infinita b, r_1, r_2, ..., com $b > r_1 > r_2 > \cdots > 0$, o que não é possível. Por isso, $mdc(a, b) = mdc(b, r_1) = \cdots = mdc(r_n, r_{n+1}) = mdc(r_n, 0) = r_n$. Assim, o último resto não nulo r_n é o mdc de a e b.

3.2.6 Definição. Dois inteiros a e b são ditos **primos entre si** ou **relativamente primos** quando $mdc(a, b) = 1$.

3.2.7 Corolário. Os inteiros a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.

Demonstração: Se $mdc(a, b) = 1$, então pelo Teorema de Bézout assegura a existência de inteiros x e y tais que $1 = ax + by$. Reciprocamente, vamos supor que $1 = ax + by$ para $x, y \in \mathbb{Z}$, e seja $d = mdc(a, b)$. Como $d \mid a$ e $d \mid b$, então $d \mid ax + by = 1$. Como $d > 0$, temos que $d = 1$, ou seja, a e b são relativamente primos.

3.2.8 Corolário. Sejam $a, b \in \mathbb{Z}$ tais que $mdc(a, b) = 1$. Se $a \mid c$ e $b \mid c$, então $ab \mid c$.
Demonstração: Como $mdc(a, b) = 1$, então pela identidade de Bachet-Bézout, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.**

Por outro lado, existem $\lambda_1, \lambda_2 \in \mathbb{Z}$ satisfazendo $c = a\lambda_1 = b\lambda_2$, de modo que $cb = ab\lambda_1$ e $ca = ab\lambda_2$. Logo, multiplicando os lados da igualdade em ** por c, obtemos $c = cax + cby = ab\lambda_2 x + ab\lambda_1 y = ab(\lambda_2 x + \lambda_1 y)$, isto é, $ab \mid c$.

■

3.3 Números Primos

3.3.1 Definição. Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é chamado **primo** quando seus únicos divisores positivos são 1 e p. Caso contrário, dizemos que p é **composto.**

3.3.2 Teorema Fundamental da Aritmética – TFA. Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de primos. Especificamente, $a = p_1 p_2 \ldots p_n$, em que $p_1, p_2, \ldots, p_n$ são primos.

Demonstração: (**Existência**) Tomemos o conjunto $M = \{a \in \mathbb{N}: a > 1 \text{ e } a \neq p_1 p_2 \ldots p_n\}$ para primos $p_1, p_2, \ldots, p_n$. Se mostrarmos que $M = \emptyset$, então a existência dos números primos estará provada. Por absurdo, se $M = \emptyset$, então pelo PBO, M possui um menor elemento m. É claro que m não pode ser primo e, por isso, é composto. Assim, podemos escrevê-lo na forma $m = b \cdot c$, com $1 < b, c < m$. Como $b < m$ e $c < m$, então $b \notin M$ e $c \notin M$, pois $m = \min M$. Assim, sendo $b > 1$ e $c > 1$, segue que estes números são primos ou são produtos de primos. Logo, $m = b \cdot c$ é um produto de primos, o que é uma contradição. Desse modo, $M = \emptyset$.
(**Unicidade**) Suponhamos que $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$, ***
sendo $p_1, \ldots, q_n, q_1, \ldots, q_m$ todos primos. Logo, $p_1 \mid q_1 q_2 \ldots q_m$ e, por Corolário, temos que $p_1 = q_j$, para algum $j = 1, \ldots, m$, digamos que $p_1 = q_1$. Pela lei do cancelamento, segue de *** que $p_2 \ldots p_n = q_2 \ldots q_m$. Da mesma forma, temos $p_2 = q_j$ para algum $j = 2, \ldots, m$. Assumindo que $p_2 = q_2$, obtemos $p_3 \ldots p_n = q_3 \ldots q_m$. Continuando este processo, e assumindo que $n > m$,

temos $1 = p_{m+1} \dots p_n$, o que é impossível. Similarmente, se $n < m$, então $1 = p_{n+1} \dots p_m$, o que também é uma impossibilidade. Portanto, $m = n$ e $q_i = p_i$ para cada $i = 1, \dots, n$.

■

3.3.3 Corolário. Todo número natural $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma $a = p_1^{r1} p_2^{r2} \dots p_k^{rk}$, #

em que $p_1, p_2, \dots, p_k$ são primos distintos e $r_1, r_2, \dots, r_k$ são números naturais. A representação de um inteiro $a > 1$ dada em # é sua **fatoração** ou **decomposição canônica** em fatores primos.

3.3.4 Teorema (Teste de Primalidade). Se $n > 1$ for composto, então n possui, necessariamente, um divisor primo p tal que $p \leq \overline{n}$. Ou seja, se n não possui divisores diferentes de 1, menores ou iguais a $\overline{n}$, então n é primo.

Demonstração: Sendo n um número composto, então $n = a \cdot b$, com $1 < a, b < n$. Se $a > \overline{n}$ e $b > \overline{n}$, então $n = a \cdot b > \overline{n} \cdot \overline{n} = n$, o que é impossível. Logo, $a \leq \overline{n}$ ou $b \leq \overline{n}$. Suponhamos que $a \leq \overline{n}$. Com $a > 1$, existe um primo p, com $p \mid a$. Desde que $a \mid n$, temos que $p \mid n$ e $p \leq a \leq \overline{n}$.

■

3.3.5 Fatoração de Fermat. Se p é um primo e a é um inteiro que não é divisível por p, então: $a^{p-1} \equiv 1 \bmod m$.

Apresentando o Método de Fermat. Determinar divisores para divisor ímpar b de a, considerando a solução inteira m e n da equação $b = m^2 - n^2$.

Vejamos então. Primeiramente, se $b = m^2 - n^2$, temos que $b = (m + n)(m - n)$. Reciprocamente, se $b = dc$, com $c \geq d \geq 1$, então $b = \left(\frac{c+d}{2}\right)^2 - \left(\frac{c-d}{2}\right)^2$, ##

Em que $\left(\frac{c+d}{2}\right)$ e $\left(\frac{c-d}{2}\right)$ são inteiros não negativos, pois d e c são ambos ímpares. Por isso, a equação $b = m^2 - n^2$ tem sempre solução inteira.

Determinando n e m tais que $m^2 - b = n^2$, por determinar o menor inteiro positivo k tal que $k^2 \geq b$. Após isso, consideremos os números $k^2 - b$, $(k + 1)^2 - b$, $(k + 2)^2 - b$, ... até que um valor de $m \geq \overline{b}$ é encontrado de modo que $m^2 - b$ é um quadrado perfeito. Obviamente, esse processo não pode continuar indefinidamente, em conformidade com ##. Além disso, $\left(\frac{b+1}{2}\right)^2 - b = \left(\frac{b-1}{2}\right)^2$, ou seja, $m = \left(\frac{b+1}{2}\right)$ e $n = \left(\frac{b-1}{2}\right)$, de modo que, $m + n = b$ e $m - n = 1$. Todavia, se isso ocorrer sem que uma diferença de quadrados tenha ocorrido antes, então os únicos divisores de b são 1 e o próprio b, isto é, b é um número primo.

Se b for primo, então a fatoração de a como produto de primos é $a = 2^r \cdot b$. Caso contrário, procedemos da seguinte forma:

Passo 1. Seja $m = \overline{b}$ (o maior inteiro menor ou igual a $\overline{b}$).

Passo 2. Se $m^2 - b = n^2$, então $b = (m - n)(m + n)$.

Passo 3. Se $m^2 - b \neq n^2$, então somamos 1 a m e voltamos ao passo 2.

3.3.6 Teorema (Euclides). O conjunto P dos números primos é infinito.

Demonstração: Suponhamos por absurdo que P é um conjunto finito, e sejam $p_1, p_2, \dots, p_n$ todos os primos. Consideremos $a \in \mathbb{N}$ dado pelo produto dos p_i's somado ao número 1, isto é, $a = p_1 p_2 \dots p_n + 1$. Como $a > 1$, então existe um primo p que divide a, ou seja, $a = pk$. Como por hipótese $p_1, p_2, \dots, p_n$ são os únicos primos, então $p = p_i$ para algum $i = 1, \dots, n$, digamos

que $p = p_1$. Assim, $pk = pp_2 \ldots p_n + 1$, isto é, $p \mid 1$, o que é uma contradição. Assim, P é infinito.

■

3.4 Congruências

3.4.1 Propriedades Básicas das Congruências. Sejam m um número natural e a e b inteiros quaisquer. Dizemos que a é **congruente** a b **módulo** m, em símbolos $a \equiv b \pmod m$, quando m divide a – b. O número m é chamado o **módulo** da congruência. Se m não divide a – b, então dizemos que a **não é congruente** a b **módulo** m ou que a é **incongruente** a b **módulo** m. Neste caso, escrevemos $a \not\equiv b \pmod m$.
Notemos que $a \equiv b \pmod m$ significa afirmar que existe um inteiro k tal que $a = b + km$.
3.4.2 Exemplo. Temos que $4 \equiv 1 \pmod 3$, $16 \equiv -4 \pmod 5$, $-7 \equiv 5 \pmod 2$, pois, $3 \mid (4 - 1)$, $5 \mid (16 + 4)$ e $2 \mid (-7 - 5)$.

■

3.4.3 Proposição. Dados a e b inteiros, temos que $a \equiv b \pmod m$ se, e somente se, a e b têm o mesmo resto quando divididos por m.

Demonstração. Se $a \equiv b \pmod m$, então $a = b + km$, com k. Pelo Algoritmo da Divisão, $b \equiv qm + r$, com $0 \leq r < m$. Assim, $a = b + km = qm + r + km = (q + k)m + r$, ou seja, r também é o resto da divisão de a por m. Reciprocamente, suponhamos que $a = q_1m + r$ e $b = q_2m + r$, em que $0 \leq r < m$. Logo, $a - b = (q_1 - q_2)m$, de modo que $m \mid a - b$, isto é, $a \equiv b \pmod m$.

3.4.4 Congruências Lineares. Dados a e b inteiros, com $a \neq 0$, uma congruência da forma $ax \equiv b \pmod m$ é chamada **congruência linear**, em que x é uma incógnita. Queremos determinar todas as soluções inteiras de $ax \equiv b \pmod m$, isto é, todos os inteiros x_0 para os quais $ax_0 \equiv b \pmod m$.
Se x_0 é uma solução da congruência $ax \equiv 1 \pmod m$, então dizemos que a é **invertível** módulo m, e que x_0 é um **inverso** de a módulo m.

3.4.5 Proposição. Um inteiro a é invertível módulo m se, e somente se, $mdc(a, m) = 1$. Ademais, quaisquer dois inversos de a módulo m são congruentes módulo m.

Demonstração: Se a é invertível módulo m, então existe um inteiro b tal que $ab \equiv 1 \pmod m$. Logo, existe $c \in \mathbb{Z}$, com $ab = 1 + cm$, ou seja, $ab + (-c)m = 1$, o que implica em $mdc(a, m) = 1$. Para a recíproca, se $mdc(a, m) = 1$, então pela identidade de Bachet-Bézout, existem inteiros x e y tais que $ax + my = 1$, isto é, $ax \equiv 1 \pmod m$, o que mostra que a é invertível módulo m. Finalmente, se x_0 e y_0 são inversos de a módulo m, então $ax_0 \equiv 1 \pmod m$ e $ay_0 \equiv 1 \pmod m$, ou seja, $ax_0 \equiv ay_0 \pmod m$. Desde que $mdc(a, m) = 1$, segue que $x_0 \equiv y_0 \pmod m$.

3.4.6 Teorema Chinês dos Restos. Sejam $n_1, n_2, \ldots, n_k$ números naturais tais que $mdc(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares possui uma solução, que é única módulo $n = n_1n_2 \ldots n_k$,

Demonstração: Sendo $n = n_1n_2 \ldots n_k$, então $N_i = \frac{n}{ni} = n_1n_2 \ldots n_{i-1}n_{i+1} \ldots n_k$, ou seja, N_i é o produto de todos os inteiros $n_i, n_2, \ldots, n_k$ excluindo n_i. Desde que $mdc(n_i, n_j) = 1$ para $i \neq j$, então $mdc(N_i, n_i) = 1$. Assim, pela identidade de Bachet-Bézout, existem inteiros r_i e s_i tais que $r_iN_i + s_in_i = 1$ ###

para cada i = 1, ..., k. Vamos provar que o inteiro $x_0 = \sum_{i=1}^{k} c_i r_i N_i = c_1r_1N_1 + c_2r_2N_2 + \ldots + c_kr_kN_k$ é uma solução do sistema dado. Inicialmente, se $i \neq j$, então $N_j \equiv 0 \pmod{n_i}$, desde que $n_i \mid N_j$. Logo, $c_jr_jN_j \equiv 0 \pmod{n_i}$, de modo que
$x_0 = c_1r_1N_1 + c_2r_2N_2 + \ldots + c_kr_kN_k \equiv c_ir_iN_i \pmod{n_i}$. Por outro lado, de ###, temos que $r_iN_i \equiv 1 \pmod{n_i}$ para cada i = 1, ... , k. Daí, $c_ir_iN_i \equiv c_i \pmod{n_i}$ e, por transitividade, $x_0 \equiv c_i \pmod{n_i}$ para todo i. Isso mostra que x_0 é uma solução do sistema. Por fim, se y_0 é outra solução, então $y_0 \equiv c_i \pmod{n_i}$ para cada i = 1, ... , k. Desse modo, $x_0 \equiv y_0 \pmod{n_i}$, isto é, $n_i \mid x_0 - y_0$. Desde que $mdc(n_i, n_j) = 1$, com $i \neq j$, segue do Lema de Euclides que $n = n_1n_2 \ldots n_k$ divide $x_0 - y_0$, ou seja, $x_0 \equiv y_0 \pmod{n}$, o que prova a unicidade de solução módulo n. Por isso, a solução geral do sistema é $x = x_0 + kn$, $k \in \mathbb{Z}$.

■

3.4.7 Definição. Um **equação diofantina** é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas. Uma equação da forma $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ é chamada **equação diofantina linear**, em que $a_1, \ldots, a_n$ são inteiros dados, chamados **coeficientes**, b que também é um inteiro dado, é chamado **termo constante** e $x_1, \ldots, x_n$ são as **incógnitas**.

3.5 Teorema de Fermat e Euler

3.5.1 Teorema (O Pequeno Teorema de Fermat) Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração: Consideremos os primeiros p – 1 múltiplos de a, ou seja, a, 2a, 3a, ... , (p - 1)a. ⌂
Observemos primeiramente que estes números são dois a dois incongruentes módulo p. De fato, se $ak_1 \equiv ak_2 \pmod{p}$, com $1 \leq k_1 < k_2 \leq p - 1$, então como mdc(a, p) = 1, segue que $k_1 \equiv k_2 \pmod{p}$, isto é, $p \mid k_2 - k_1$, o que é impossível. Além disso, se $1 \leq r \leq p - 1$ e $p \mid ra$, então $p \mid a$ ou $p \mid r$, o que também não é possível. Portando, $ra \equiv 0 \pmod{p}$ para todo r = 1, ... , p – 1. De acordo com o Algoritmo da Divisão, cada inteiro é congruente módulo p a um, e somente um, número da sequência 1, 2, 3, ... , p -1. ⌂⌂
Portanto, cada inteiro de ⌂ é equivalente a um número de ⌂⌂ numa determinada ordem, digamos $a \equiv b_1 \pmod{p}$,

$$2a \equiv b_2 \pmod{p},$$
$$\vdots$$
$$(p - 1)a \equiv b_{p-1} \pmod{p},$$

em que $b_i \in 1, 2, \ldots, p-1$ para i = 1,2, ... , p – 1. Multiplicando membro a membro estas congruências, temos que
$a \cdot 2a \ldots (p - 1)a \equiv 1 \cdot 2 \ldots (p - 1) \pmod{p}$, isto é, $a^{p-1}(p - 1)! \equiv (p – 1)! \pmod{p}$. Como $mdc((p – 1)!, p) = 1$, podemos cancelar (p - 1)! Desta última congruência, de modo que $a^{p-1} \equiv 1 \pmod{p}$.

■

3.5.2 Definição (Função ϕ de Euler) Para cada inteiro $n \geq 1$, indiquemos por ϕ(n) o número de inteiros positivos menores ou iguais a n que são relativamente primos com n. A função ϕ assim definida é chamada **função fi de Euler**.
Para cada $n \in \mathbb{N}$, considerando $A_n = \{m \in \mathbb{N}: 1 \leq m \leq n \text{ e } mdc(m, n) = 1\}$, então ϕ(n) = car(An), em que car(An) indica a cardinalidade de Na.

3.5.3 Lema. Sejam a um inteiro tal que mdc(a, m) = 1. Se $a_1, a_2, \ldots, a_{\phi(m)}$ são os inteiros positivos menores do que m e relativamente primos com m, então $aa_1, aa_2, \ldots, aa_{\phi(m)}$ são congruentes módulo m a $a_1, a_2, \ldots, a_{\phi(m)}$, em alguma ordem.

Demonstração: Mostremos primeiramente que aa_1, aa_2, ... , $aa_{\phi(m)}$ são dois a dois incongruentes módulo m. De fato, se $aa_i \equiv aa_j \pmod m$ para $i \neq j$, então como mdc(a, m) = 1, podemos cancelar o fator a desta congruência e, assim, $a_i \equiv a_j \pmod m$, ou seja, $m \mid a_i - a_j$, o que é uma impossibilidade, pois $1 \leq a_i, a_j \leq m - 1$ e $a_i \neq a_j$. Além disso, como mdc(a, m) = 1 e mdc(a_i, m) = 1 para todo i = 1, ... , ϕ(m), então temos que mdc(aa_i, m) = 1. Desde que $0, 1, \ldots, m-1$ é um sistema completo de resíduos módulo m, então para cada aa_i, existe único inteiro b, como $0 \leq b < m$, tal que $aa_i \equiv b \pmod m$. Como mdc(b, m) = mdc(aa_i, m) = 1, então b deve necessariamente ser um dos inteiros a_1, a_2, ... , $a_{\phi(m)}$. Logo, $aa_i \equiv a_j \pmod m$ para algum j = 1, ... , ϕ(m).

■

3.5.4 Teorema (Euler). Sejam a e m inteiros, com $m \geq 1$ e mdc(a, m) = 1. Então, $a^{\phi(m)} \equiv 1 \pmod m$.

Demonstração: O caso m = 1 é imediato, pois $\phi(1) = 1$. Por isso, vamos considerar m > 1. Sejam a_1, a_2, ... , a_{ϕ}(m) os inteiros positivos menores do que m que são relativamente primos com m. Desde que mdc(a_i, m) = 1 para cada i = 1, ... , ϕ(m), segue do Lema acima que aa_1, aa_2, ... , $aa_{\phi(m)}$ são congruentes módulo m a a_1, a_2, ... , $a_{\phi(m)}$, em alguma ordem. Desse modo,

$$\begin{aligned} a \cdot a_1 &\equiv b_1 \pmod m, \\ a \cdot a_2 &\equiv b_2 \pmod m \\ &\vdots \\ a \cdot a_{\phi(m)} &\equiv b_{\phi(m)} \pmod m, \end{aligned}$$

em que b_1, b_2, ... , $b_{\phi(m)}$ são os inteiros a_1, a_2, ... , $a_{\phi(m)}$, não necessariamente nesta ordem. Multiplicando esta congruência, temos $(aa_1)\,(aa_2) \ldots (aa_{\phi(m)}) \equiv b_1 b_2 \ldots b_{\phi(m)}$, ou seja, $a^{\phi(m)}\,(a_1 a_2 \ldots a_{\phi(m)}) \equiv a_1 a_2 \ldots a_{\phi(m)} \pmod m$. Como mdc($a_i$, m) = 1 para todo i = 1, ... , ϕ(m), segue em decorrência que mdc($a_1 a_2 \ldots a_{\phi(m)}$, m) = 1. Por isso, podemos cancelar o fator $a_1 a_2 \ldots a_{\phi(m)}$ da última congruência e, assim, $a^{\phi(m)} \equiv 1 \pmod m$.

■

4. Criptografia RSA

Hoje em dia, a comunicação entre computadores pela Internet vem criando novos desafios para a criptografia. Como é relativamente fácil interceptar mensagens enviadas por linha telefônica, tonar-se necessário codifica-las, sempre que contenham informações sensíveis. Isto inclui transações bancárias ou comerciais, ou até mesmo uma compra feita com cartão de crédito (COUTINHO, 2005). Apesar da cifração e decifração de mensagens se ter tornado mais rápida e complexa, existia um velho problema que se agudizava com a generalização do uso da criptografia – **a distribuição da chave** (FIARRESGA, 2010).

Assim tornou-se necessário inventar novos códigos, que fossem dificeis de decifrar, mesmo com a ajudar de um computador. Estes códigos foram criados para o uso em aplicações comerciais, e não em comunicação entre espiões. Por isso os códigos modernos são todos de chave pública (COUTINHO, 2005). Em 1976, a dupla Whitfied Diffie e Martin Hellman encontraram uma forma de poder haver uma troca segura de chaves, sem as pessoas se encontrarem. Até então, as chaves utilizadas eram funções matemáticas injetivas – uma determinada função servia para cifrar uma mensagem, a sua inversa para decifrar (FIARRESGA, 2010).

Hellman colocou a Aritmética Modular ao serviço da criptografia. Diffie continuou a trabalhar no problema da distribuição da chave e teve uma ideia brilhante – A Cifra Assimétrica, ou seja, Diffie teve uma ideia que iria revolucionar o mundo da criptografia, o seu problema era não saber como pô-la em prática (FIARRESGA, 2010). Ronald Rivest, Adi

Shamir, cientistas informáticos, e Leonard Adleman, matemático, resolveram formar uma equipe para pôr a ideia de Diffie em prática. Durante um ano, os dois cientistas informáticos desenvolveram ideias para criar uma cifra assimétrica. Estas eram submetidas ao crivo matemático de Adleman, que as deitava fora devido às suas falhas. Até que, em Abril de 1977, numa noite de inspiração de Rivest, este resolveu de vez, o problema da distribuição da chave. No final do artigo que escreveu nessa noite colocou os nomes dos elementos da equipa por ordem alfabética. Os seus colegas concordaram em colocar o nome no seu artigo, mas o nome dele tinha que vir em primeiro lugar. E desta forma, se deu nome à cifra assimétrica **RSA** (Rivest, Shamir e Adleman) (FIARRESGA, 2010).

4.1 Funcionamento do Método RSA

COUTINHO, (2005, p. 4) descreve como utilizar o método RSA, ou seja:

> *Para poder implementar o RSA precisamos de dois parâmetros básicos: dois números primos que vamos chamar de p e q. Para codificar uma mensagem usando o RSA é suficiente conhecer o produto dos dois primos, que vamos chamar de n. Para decodificar uma mensagem precisamos conhecer os primos p e q. A chave de codificação do RSA é, portanto, constituída essencialmente pelo número n = pq. Cada usuário do método tem sua própria chave de decodificação. Esta chave é tornada pública: todos ficam sabendo que, para mandar uma mensagem para o banco Acme, deve ser usada a chave n. Por isso n também é conhecido como a 'chave pública'. Já a chave de decodificação é constituída pelos primos p e q.*

Você pode estar pensando que não deve ser tão difícil encontrar p e q conhecendo N uma vez que N é resultado de p e q. Em primeiro lugar, pelo teorema da fatoração única, enunciado primeiramente por Gauss no seu livro *Disquisitiones arithmetiae*, este produto tem a forma única $n = pj^{ej} \dots p_k^{ek}$, onde pj são fatores primos e ej suas multiplicidades. Portanto os únicos primos que geram N são p e q a única forma de obtê-los através de n é a fatoração.

Como os matemáticos têm tido grande dificuldade em encontrar um método rápido e eficiente para descobrir quais foram os números primos usados para gerar outros números, se N for um número suficientemente grande, será praticamente impossível deduzir os valores de p e q. É baseada nisso que a segurança da criptografia RSA é tida como plenamente satisfatória (SILVA; MARTINS, 2011). Uma chave segura de RSA é gerada a partir de números primos de cerca de 100 algarismos cada, de forma que n, que é o produto destes primos, terá cerca de 200 algarismos (COUTINHO, 2015).

No sistema RSA usamos a substituição por números, e esta é a primeira coisa a se fazer. Usam-se números de dois dígitos, para que não ocorra ambiguidade, pois se fizéssemos a letra A como 1 e a letra I como 9, a palavra AI fica 19 que pode ser confundida com a letra S, então elabora-se uma tabela para a substituição que deve ser conhecida por todos envolvidos (GANASSOLI; SCHANKOSKI, 2015).

Tabela 03: Substituição de Letras por Números em RSA

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

4.1.1 Aplicação do Sistema RSA

Para completar o sistema RSA de criptografia também devemos saber como escrever as cifras e depois decifrá-las, para isso se faz necessário, a chave pública e a chave privada (GANASSOLI; SCHANKOSKI, 2015).

GANASSOLI; SCHANKOSKI, (2015, p.66) descreve detalhadamente como aplicar o sistema RSA, isto é:

Escolhem-se dois números primos distintos p e q, considere $n = p \cdot q$, sendo n inteiro. Depois calcula-se a função de Euler $\phi(n) = (p - 1).(q - 1)$, que é a quantidade de números coprimos com n e escolhe-se um número inteiro e, chamado de potência de encifração, tal que $mdc(e, \phi(n)) = 1$. O par (e, n) é a chave pública. Outro par, (d, n), é a chave privada, d é um número inteiro chamado potência de decifração, onde, $e \cdot d \equiv 1 \mod \phi(n)$, com $1 \leq d < \phi(n)$. Para achar o valor de d , conhecidos $\phi(n)$ e e, aplica-se o algoritmo de Euclides estendido. Implementando o RSA, usamos a aritmética modular, onde C representa o texto cifrado e D o texto original. O texto original depois de convertido em números onde os espaços entre as palavras são completados pelo número 99, é separado em blocos, esses blocos são D1, D2, D3, ..., Dr e cada bloco deve ser menor que o número n = p . q, e não deverá começar com 0 para evitar problemas na decodificação. Para cifrar cada um dos blocos fazemos:

$$C \equiv D^e \bmod n$$

Depois de cifrados geram os blocos C1, C2, C3, ..., Cr. Observe que para esse processo usa-se somente a chave pública. Transmitida a mensagem, agora é hora de decifrar, para tal usa-se a chave privada, conhecida somente pela pessoa que recebe a mensagem, fazendo com cada um dos blocos cifrados: $D \equiv C^d \bmod n$.

Vejamos um exemplo com números primos de duas casas decimais apenas:
Mensagem: CIÊNCIA DO SIGILO.

<u>Codificamos a Mensagem:</u>

1) Substitui as Letras da Mensagem Conforme Tabela 03:

12181423121810991324992818161821 24

2) Escolher Dois Números Primos, p e q; Calcular n = p . q
Sejam p = 17 e q = 23, então n = 391

3) Separa em Blocos os Números Menores que n = 391

121 – 81 – 42 – 312 – 18 – 10 – 99 – 132 – 49 – 92 – 81 – 81 – 61 – 82 – 124

4) Escolhe $e \in \mathbb{N}$ tal que mdc (e, ϕ(n)) = 1
Como p = 17 e q = 23, temos: $\phi(n) = (p - 1) \cdot (q - 1) = (17 - 1) \cdot (23 - 1) = 16 \cdot 22 = 352 \rightarrow$ $\phi(n) = 352$; e = 3, onde mdc (3, 352) = 1

5) Calcular $C \equiv D^e \bmod n$:

- $C \equiv 121^3 \bmod 391 \rightarrow 121^3 = 121^2 \,.\, 121 \equiv 174 \,.\, 121 \equiv 331 \bmod 391$
- $C \equiv 81^3 \bmod 391 \rightarrow 81^3 = 81^2 \,.\, 81 \equiv 305 \,.\, 81 \equiv 72 \bmod 391$
- $C \equiv 42^3 \bmod 391 \rightarrow 42^3 = 42^2 \,.\, 42 \equiv 200 \,.\, 42 \equiv 189 \bmod 391$
- $C \equiv 312^3 \bmod 391 \rightarrow 312^3 = 312^2 \,.\, 312 \equiv 376 \,.\, 312 \equiv 12 \bmod 391$
- $C \equiv 18^3 \bmod 391 \rightarrow 18^3 \equiv 358 \bmod 391$
- $C \equiv 10^3 \bmod 391 \rightarrow 10^3 \equiv 218 \bmod 391$
- $C \equiv 99^3 \bmod 391 \rightarrow 99^3 = 99^2 \,.\, 99 \equiv 26 \,.\, 99 \equiv 228 \bmod 391$
- $C \equiv 132^3 \bmod 391 \rightarrow 132^3 = 132^2 \,.\, 132 \equiv 220 \,.\, 132 \equiv 106 \bmod 391$
- $C \equiv 49^3 \bmod 391 \rightarrow 49^3 = 49^2 \,.\, 49 \equiv 55 \,.\, 49 \equiv 349 \bmod 391$
- $C \equiv 92^3 \bmod 391 \rightarrow 92^3 = 92^2 \,.\, 92 \equiv 253 \,.\, 92 \equiv 207 \bmod 391$
- $C \equiv 81^3 \bmod 391 \rightarrow 81^3 = 81^2 \,.\, 81 \equiv 305 \,.\, 81 \equiv 72 \bmod 391$
- $C \equiv 81^3 \bmod 391 \rightarrow 81^3 = 81^2 \,.\, 81 \equiv 305 \,.\, 81 \equiv 72 \bmod 391$
- $C \equiv 61^3 \bmod 391 \rightarrow 61^3 = 61^2 \,.\, 61 \equiv 202 \,.\, 61 \equiv 201 \bmod 391$
- $C \equiv 82^3 \bmod 391 \rightarrow 82^3 = 82^2 \,.\, 82 \equiv 77 \,.\, 82 \equiv 58 \bmod 391$
- $C \equiv 124^3 \bmod 391 \rightarrow 124^2 \,.\, 124 \equiv 127 \,.\, 124 \equiv 108 \bmod 391$

Enviando a Mensagem Depois de Executar a Cifragem:

331 – 72 – 189 – 12 – 358 - 218 – 228 - 106 – 349 – 207 – 72 - 72 – 201 – 58 – 108

O Par (e, n) = (3, 391) é a Chave Pública.

<u>Decodificamos a Mensagem:</u>

Para decodificar precisamos de dois números: n e o inverso de "*e*" em $\phi(n)$, que denotaremos por d. O par (n, d) é a chave de decodificação(privada).

Temos: n = 391 e e = 3.

Aplicaremos o algoritmo de Euclides estendido para calcular o d. Calculando, $\phi(391) = 352$ dividido por 3, obtemos: $352 = 3 \,.\, 117 + 1$ donde $1 = 352 + (-117) \,.\, 3$.

Logo o inverso de 3 módulo 352 é –117. Como vamos usar d como expoente de potências, precisamos que d seja positivo. Portanto, $d = 352 - 117 = 235 \rightarrow d = 235$, que é o menor inteiro positivo congruente a -117 módulo 352. Assim, para decodificar o bloco 331 da mensagem codificada, calculamos a forma reduzida de 331^{235} módulo 391.

Se não tivéssemos Teorema de Fermat e Algoritmo Chinês do Resto, era impossível de um computador efetuar esta conta.

Calculando 331^{235} módulo 17 e módulo 23, que são os primos em que n se fatora.

Assim, $331^{235} \equiv 8 \pmod{17} \rightarrow 331^{235} \equiv (8^{16})^{14} \,.\, 8^{11} \pmod{17}$, pelo Teorema de Fermat, temos: $331^{235} \equiv 1^{14} \,.\, 8^{11} \pmod{17} \equiv 8^{11} \pmod{17} \rightarrow 331^{235} \equiv (8^3)^2 \,.\, 8^2 \pmod{17} \equiv 2^3 \,.\, 13 \pmod{17} \rightarrow 331^{235} \equiv 2 \pmod{17}$ de forma análoga;

$331^{235} \equiv 9 \pmod{23} \rightarrow 331^{235} \equiv (9^{22})^{10} \,.\, 9^{15} \pmod{23} \rightarrow 331^{235} \equiv 1^{10} \,.\, 9^{15} \pmod{23} \rightarrow 331^{235} \equiv 6 \pmod{23}$.

Portanto, $331^{235} \equiv 2 \pmod{17}$

$331^{235} \equiv 6 \pmod{23}$; corresponde ao sistema $X \equiv 2 \pmod{17}$

$X \equiv 6 \pmod{23}$.

Pelo Algoritmo Chinês do Resto, temos: $X = 6 + 23Y$, substituindo na 1º congruência, obtemos: $23Y + 6 \equiv 2 \pmod{17} \rightarrow 23Y \equiv 4 \pmod{17}$.

Assim, $6Y \equiv 13 \pmod{17}$, mas, 6 tem inverso 3 módulo 17, de forma que: $Y = 3.13 \equiv 5 \pmod{17}$. Logo, $X = 6 + 23.5 \rightarrow X = 121$, o que corresponde a 1º letra da mensagem (C) de forma análoga faz para os demais blocos.

O processo acima mostra que ao decodificar os blocos codificados, obtém-se os blocos originais e consequentemente o acesso a mensagem. Isso só é possível por que os números primos escolhidos foram de duas casas decimais.

4.1.2 Segurança do RSA

O RSA é um método de chave pública. Sejam p e q os parâmetros do sistema que estamos usando e n = pq. A chave de codificação corresponde à chave pública do sistema. Portanto o par (n, e) é acessível a qualquer usuário. O RSA só será seguro se for difícil calcular d quando n e e são conhecidos (COUTINHO, 2005). A força desta cifra reside no fato de não existirem, atualmente, algoritmos capazes de decompor em fatores primos, de uma forma rápida, um número enorme. Como escreve o Professor Jorge Buescu, referindo-se à segurança deste método, no seu livro *O Mistério do Bilhete de Identidade e Outras Histórias*: "O perigo não vem dos computadores. Na verdade, a evolução dos computadores vem tornar o método RSA mais seguro. A razão é que o tempo para a multiplicação de dois números cresce mais devagar (polinomialmente) do que o necessário para a sua fatorização (que, tanto quanto se sabe, cresce exponencialmente) … O perigo não vem dos computadores – vem da Matemática." (FIARRESGA, 2010).

Se escolhermos primos que resultassem em N na casa de 10^{308}, SINGH (2008, p. 303) afirma que "os esforços combinados de cem milhões de microcomputadores levariam mais de mil anos para quebrar esta cifra. Com valores suficientemente grande de p e q, a RSA é invencível". Contudo, a história da criptografia nos faz repensar sobre o fato que, muitas delas foram consideradas inquebráveis, mas mesmo assim sofreram ataques de criptoanalistas e foram decifradas. A criptoanálise desenvolveu técnicas como: tempest, a qual intercepta mensagens antes de cifradas; vírus, os quais conseguem anotar a chave utilizada e o cavalo de Tróia, o qual envia cópias dos textos originais. Todas essas são úteis para coleta de informações, mas o objetivo vai mais além: quebrar a cifra RSA. No futuro, provavelmente, teremos o computador quântico, que já é objeto de pesquisa, esse será capaz de quebrar a cifra RSA. Não se sabe quando os problemas de construir tais computadores serão superados, mas os criptógrafos já estudam a chamada criptografia quântica, um sistema que garantiria a segurança total das mensagens, sendo absolutamente inquebrável, porém esse sistema precisa ser aperfeiçoado para se tornar prático e operar através de longas distâncias (GANASSOLI; SCHANKOSKI, 2015).

5 CONCLUSÃO

Ao longo deste trabalho tive como objetivo mostrar que a criptografia surgiu com a necessidade de esconder informações, para assim, rei e rainhas se manterem em seus tronos e as guerras serem vencidas.

Fica claro que a cada novo método de criptologia, matemáticos teve presente para desvendar os códigos, destacando-se para Alan Turing (que conseguiu quebrar a máquina Enigma). Com a evolução dos computadores, surgiu a Criptograifa RSA usada até hoje. E é a área da matemática: teoria dos números que esse método teve seu desenvolvimento como um dos mais seguro. Sendo assim, a Cripografia RSA é uma linguagem exclusiva da matemática.

IS IMPORTANT MATHEMATICS IN THE HISTORY OF CRYPTOGRAPHY?

ABSTRACT

Our proposed article aims to show that encryption is not a language exclusive to mathematics. To achieve this goal we did a bibliographical research considering as sources books, dissertations and articles. We conclude that Mathematics occupies a fundamental space in the history of Cryptography.

Keywords: History. Cryptography. Mathematics.

REFERÊNCIAS

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA.** Rio de Janeiro (RJ): Instituto Nacional de Matemática Pura e Aplicada, 2005.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**, 2ª Edição, Rio de Janeiro (RJ): Instituto Nacional de Matemática Pura e Aplicada, 2013.

COUTINHO, Severino Collier. **Criptografia.** Rio de Janeiro (RJ): Instituto Nacional de Matemática Pura e Aplicada, 2015.

COUTO, Sérgio Pereira. **Códigos & Cifras: da antiguidade à era moderna.** Rio de Janeiro (RJ): Novaterra, 2008.

FIARRESGA, Victor Manuel Calharbrês. **Criptografia e Matemática.** 2010. Trabalho de Conclusão de Curso (Mestrado em Matemática para Professores) – Universidade de Lisboa, 2010.

GANASSOLI, Ana Paula; SCHANKOSKI, Fernanda Ricardo. **Criptografia e Matemática.** Dissertação (Dissertação em Matemática) – Universidade Federal do Paraná, 2015.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social.** 4. ed. São Paulo: Atlas, 1994.

KANH, David. **The Codebreakers: The Story of Secret Writing.** New York: The Macmillan Company, 1967.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware.** Novatec, 2005.

SILVA, Alexandre Ferreira; MARTINS, Renato Marinho. **Criptografia: aspectos históricos e matemáticos.** 2011. Trabalho de Conclusão de curso (Graduação de Licenciatura em Matemática) – Universidade do Estado do Pará, 2011.

SINGH, Simon. **O Livro dos Códigos:** A ciência do sigilo – do antigo Egito à criptografia quântica. Record, 2001.

SINGH, Simon. **O Livro dos Códigos:** A ciência do sigilo – do antigo Egito à criptografia quântica. Record, 2008.

VIEIRA, Vandenberg Lopes. **Um curso Básico em Teoria dos Números,** Campina Grande (PB): Eduepb, 2015.