ATLANTE
Cuadernos de Educación y Desarrollo (2ª Época)

Mayo 2018 - ISSN: 1989-4155

A RELAÇÃO CIENTÍFICA ENTRE A CRIPTOGRAFIA E OS NÚMEROS PRIMOS

Ivan De Oliveira Holanda Filho[1]
Marcos Paulo Mesquita Da Cruz[2]
Prof. M. Sc. Rickardo Léo Ramos Gomes[3]

Para citar este artículo puede utilizar el siguiente formato:

Ivan De Oliveira Holanda Filho, Marcos Paulo Mesquita Da Cruz y Rickardo Léo Ramos Gomes (2018): "A relação científica entre a criptografia e os números primos", Revista Atlante: Cuadernos de Educación y Desarrollo (mayo 2018). En línea:

https://www.eumed.net/rev/atlante/2018/05/criptografia-numeros-primos.html

RESUMO

Para o homem, de modo geral, durante toda sua evolução, sempre foi muito importante salvaguardar informações sempre que lhes pareceu conveniente. Tais informações passaram por vários processos ou procedimentos que tornavam estas informações inacessívveis para a maioria das pessoas, tornando-as informações valorizadas e, é claro, conferindo ao procedimento adotado grande valorização. A presente pesquisa tratará da Criptografia, também conhecida como Ciência do Sigilo. Trata-se de uma Ciência que, por vezes, chegou a ser fundamental nos períodos de guerra que o homem enfrentou, chegando mesmo, muitas vezes, a mudar o rumo de guerras, como aconteceu nas grandes guerras mundiais ou mesmo antes, com as técnicas de criptografia usadas pelos gregos da antiguidade. Fundamentada com o seu rico passado histórico, hoje em dia a Criptografia tornou-se ferramenta essencial na prevenção de fraudes em comércios eletrônicos quando fazemos uso da Internet, para além da segurança na Internet, há, também, a atuação na garantia da segurança de transações bancárias. Neste ponto é que é possível demonstrar a relação científica entre a Criptografia e os números primos, ressaltando a grandiosidade da Matemática que unida a outras Ciências contribuirá, e muito, no avanço da modernidade. Ao longo do trabalho mostra-se o desenvolvimento da Teoria dos Números, um ramo da Matemática que estuda a propriedade dos

1 Licenciado em Matemática (UECE), Pós-Graduação em Ensino de Matemática. Professor da Rede Básica de Maracanaú e do Estado.

2 Bacharel em Ciências Contábeis (UECE), Mestrando em Economia Rural. Professor de cursos Técnicos.

3 Professor da Disciplina de Metodologia do Trabalho Científico (Orientador) – Faculdade Ateneu. Dr. (Tít. Cult.) em Ciências Biológicas pela FICL; M. Sc. em Fitotecnia pela Universidade Federal do Ceará (UFC); Spec. em Metodologia do Ensino de Ciências pela Universidade Estadual do Ceará (UECe); Spec. (Tít. Cult.) em Paleontologia Internacional pela Faculdade Internacional de Cursos Livres (FICL). Graduado em Agronomia pela Universidade Federal do Ceará (UFC); Licenciado em Matemática, Biologia, Física e Química pela Universidade Estadual Vale do Acaraú (UVA); Consultor Internacional do BIRD para Laboratórios Científicos.

números, mais especificamente dos números inteiros, no qual abordaremos muitas questões de números envolvendo os números primos como: primos gêmeos, probabilidade de números primos, a grande busca de entender os números primos e a correlação dessa busca com implicações em outras Ciências. Fica claro que com o desenvolvimento da Internet que muitos problemas surgirão com relação a segurança de dados e o futuro estará na capacidade do homem em bem usar a Criptografia. Garantir acesso a informação será de suma importância as futuras gerações.

Palavras-chave: Matemática. Criptografia. Aplicações.

RESUMEN

Para el hombre, en general, durante toda su evitación, siempre fue muy importante salvaguardar informaciones siempre que les pareció conveniente. Tales informaciones pasaron por varios procesos o procedimientos que hacían estas informaciones inaccesibles para la mayoría de las personas, haciéndolas informaciones valoradas y, por supuesto, dando al procedimiento adoptado gran valoración. La presente investigación tratará de la Criptografía, también conocida como Ciencia del Sigilo. Se trata de una ciencia que a veces llegó a ser fundamental en los períodos de guerra que el hombre enfrentó, llegando a menudo a cambiar el rumbo de guerras, como ocurrió en las grandes guerras mundiales o incluso antes, con las técnicas de criptografía utilizadas por los griegos de la antigüedad. Fundamentada con su rico pasado histórico, hoy en día la Criptografía se ha convertido en una herramienta esencial en la prevención de fraudes en los comercios electrónicos cuando hacemos uso de Internet, además de la seguridad en Internet, hay también la actuación en la garantía de la seguridad de transacciones bancaria. En este punto es que es posible demostrar la relación científica entre la Criptografía y los números primos, resaltando la grandiosidad de la Matemática que unida a otras ciencias contribuirá, y mucho, en el avance de la modernidad. A lo largo del trabajo se muestra el desarrollo de la Teoría de los Números, una rama de la Matemática que estudia la propiedad de los números, más específicamente de los números enteros, en el que abordaremos muchas cuestiones de números envolviendo los números primos como: primos gemelos, probabilidad de números primos, la gran búsqueda de entender los números primos y la correlación de esa búsqueda con implicaciones en otras ciencias. Es claro que con el desarrollo de Internet que muchos problemas surgir con relación a la seguridad de datos y el futuro estará en la capacidad del hombre en bien usar la Criptografía. Garantizar el acceso a la información será de suma importancia para las futuras generaciones.

Palabras-clave: Matemáticas. Encriptación. Aplicaciones.

ABSTRACT

For man, in general, throughout his evolution, it was always very important to safeguard information whenever it seemed convenient. Such information went through several processes or procedures that made this information inaccessible to most people, making it valuable information and, of course, giving the procedure adopted great value. The present research will deal with Cryptography, also known as Science of Secrecy. It is a Science that has sometimes become fundamental in the periods of war that man faced, often even changing the course of wars, as happened in the great world wars or even before, with the techniques cryptography used by ancient Greeks. Based on its rich past history, today Cryptography has become an essential tool in the prevention of fraud in electronic commerce when we use the Internet, in addition to Internet security, there is also the role of guaranteeing the security of transactions banking services. At this point it is possible to demonstrate the scientific relationship between Cryptography and prime numbers, highlighting the grandeur of Mathematics which, together with other Sciences, will contribute much to the advance of modernity. Throughout the work we show the development of Number Theory, a branch of Mathematics that studies the property of numbers, more specifically of integers, in which we will address many questions of numbers involving prime numbers such as: twin cousins, number probability cousins, the great quest to understand the prime numbers and the correlation of this search with implications in other Sciences. It is clear that with the development of the Internet that many problems will arise with respect to data security and the future will be in man's ability to use Cryptography well. Ensuring access to information will be of great importance to future generations.

Subject Descriptor: MAC0336 Criptografia para Segurança de Dados (BCC-IME-USP)

Keywords: Mathematics. Encryption. Applications.

1 INTRODUÇÃO

Na grande invenção dos números existe um tipo especial deles que há tempos são estudados e merecem destaque desde a Grécia Antiga aos dias atuais. Esses números são chamados de números primos e com a multiplicação deles podemos formar de ,forma única, todos os demais números,esse é um dos teoremas mais conhecidos da matemática e é conhecido como teorema fundamental da aritmética. Com o passar dos anos o mistério dos números primos aumentava cada vez mais, de modo que grandes matemáticos não conseguiam uma formula que gerasse os números primos.

Os gregos já sabiam que eles eram infinitos, mas como saber o próximo primo em uma sequência? Qual o maior primo conhecido? Os primos gêmeos são também infinitos? Teoremas e conjecturas foram feitas com base nos estudos dos números, e nesse ramo desenvolve-se a teoria dos números, disciplina que estuda a propriedade dos números, mais especificamente os números inteiros

Este trabalho apresentará a história dos números primos e nesse contexto fazer analise das principais contribuições com a criação desses números. Muitos dos nossos estudos que fazemos no ensino fundamental e médio foram feitos com base nos estudos nos números primos como MMC(Mínimo Múltiplo Comum) e MDC(Máximo Divisor Comum)

O trabalho apresentará matemáticos importantes como Euclides, Fermat, Mersene, Euler entre outros que contribuíram significamente para o desenvolvimento dos números primos e da matemática. Vamos analisar as principais descobertas e contribuições deixadas pelos matemáticos a respeito dos números primos, problemas que até estão longe de serem respondidos.

Na modernidade vamos analisar o estudo da criptografia que com o desenvolvimento da teoria dos números possibilitou o crescimento da criptografia que nos dias atuais é muito importante para a segurança de informações na internet. Ao final mostraremos uma ciência que está em desenvolvimento, a criptografia, que utiliza princípios matemáticos como base para proteger a segurança de informações importantes quando usufruímos a internet.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Porque do Nome Primo

O processo de criação dos números sem dúvida nenhuma foi muito importante para a humanidade. No Egito a Matemática era vista como uma ferramenta auxiliar para obras de engenharia e agricultura. Através dos sacerdotes egípcios, Tales de Mileto introduziu a Matemática dos egípcios á Grécia e lá se desenvolveu, enormemente, tanto que na antiguidade a lógica Matemática era vista como uma Filosofia e mais do que isso, estava realmente presente na mente de filósofos, comerciantes, engenheiros, enfim muitos tipos de pessoas valorizavam o raciocino e foi assim que a Matemática cresceu e se desenvolveu como poucas outras ciências naquela época.

Haja vista o que foi dito, os gregos expandiram e deram uma nova perspectiva a essa ciência,tanto que trouxeram uma nova abordagem aos números.

Nessa expansão e nova abordagem aos números, mereceram especial atenção àqueles conhecidos como números primos.

Números primos são os números naturais que têm apenas dois divisores diferentes o 1 (um) e ele mesmo.

Outra definição é o número inteiro, que tem somente quatro divisores. É preciso destacar que o número 0 (zero) e o número 1 (um) não são primos nem compostos.

Mas porque o nome primo?

Os Pitagóricos uniram a Geometria a Aritmética através dos números figurados.

Esses números eram representados por pontos, em uma ordem organizada Geometricamente.

Ex:

• • • •

• • • •

• • • •

Representação do número 12.

Outros não poderiam ser representados como o 12 acima, e eram representados por uma única linha ou várias, mas nunca seriam representados por um retângulo.

Ex

• • • • • • •

Representação do número 7.

O sete só poderia ser representado por uma única fila.

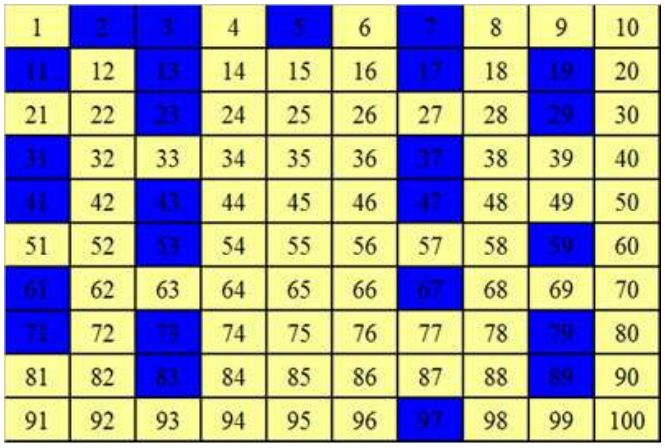
Esses números eram considerados primários dando assim a idéia do nome primo.

Tais números já eram conhecidos dos antigos gregos e até hoje fazem parte do nosso presente.

2.2 Números Primos: Os átomos da Matemática

A primeira pessoa a produzir tabelas com números primos foi Erastóstenes, diretor da biblioteca da Antiga Grécia, localizada em Alexandria. Tal tabela ficou conhecida como Crivo de Erastóstenes (276 a.C) no qual ele escreveu uma sequência de números naturais e em seguida ele retirava os números que não eram primos. A razão para o nome Crivo e que ele furava, ou seja, “crivava” os números para eliminá-los deixando assim somente os primos.

Figura 1: Crivo de Erastóstenes



1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fonte: Google imagem.

Do ponto de vista Multiplicativo os números primos são os mais simples dentre os números e com eles podemos gerar todos os outros números naturais chamados, muitas vezes, de composto. Esse é um dos Teoremas mais estudados atualmente e é conhecido como Teorema Fundamental Da Aritmética, em que Euclides (360 a.C-295 a.C) enunciou no livro IX dos Elementos de Euclides, esse Teorema diz que todo número inteiro positivo maior que um, pode ser decomposto de uma única forma em fatores de números primo.

Considere o número n um número composto qualquer, logo ele é divisível por outro número p, sendo q o seu quociente.

Mas sendo n= pxq em que p,q são menores que n.

Se p e q forem primos o Teorema está demonstrado e n esta decomposto em fatores de números primo.

Se p e q não forem primos iremos decompor em outros fatores.

Assim seja p=p1x p2 e q=q1xq2.

Logo podemos dizer que n= p1xp2x q1xq2

Se esses mesmos fatores forem primos, novamente, o teorema esta demonstrado do contrário repetimos o processo de decomposição até termos uma forma fatorada de números primos.

Podemos observar que os fatores decrescem em relação aos números de vezes que se fez o processo de decomposição, permanecendo sempre maior que um.

Muitos dos nossos estudos ainda no ensino Fundamental e ensino Médio, por exemplo, como o MMC(mínimo múltiplo comum) e o MDC(Maximo divisor comum) foram descobertas com base nos estudos de números primos.

Quando o educando vai se aprofundando no estudo dos números primos, percebe que apesar de serem simples, estão envoltos por uma complexidade que fascina e provoca novos estudos a respeito deles.

2.3 Primos Gêmeos

Um problema que já deixou muitos frustrados com uma prova definitiva são os Primos Gêmeos. Números cuja diferença entre eles são dois, e ambos sejam primos, é conhecido como primos gêmeos, alguns exemplos são (3,5); (5,7); (11,13); (17,19); (29,31). Essa é a famosa conjectura dos números primos gêmeos, de primos da forma (p,p+2). Cabe aqui destacar a diferença entre Teorema e Conjectura.

Teorema: È uma afirmação feita com base em uma prova em que, muitas vezes, outros Teoremas são utilizados (já demonstrados) para se fazer a demonstração de tal prova.

Conjectura: È uma idéia ou frase que não se pode dizer que é uma afirmação verdadeira, é uma estimativa que uma determinada afirmação pode ser verdadeira.

Muitos tentaram provar que os primos gêmeos são infinitos, mas até hoje ninguém conseguiu fazer uma prova conclusiva a respeito. Euclides provou que os números primos são infinitos, mas o mesmo não se pode afirmar dos primos gêmeos.

Em 2002 foi feita uma descoberta de números desse tipo com mais de cinqüenta mil dígitos, mas ainda sim não é uma prova concreta de se mostrar a infinitude de tais números. Em 2004, T. Tao e B. Green provaram progressões aritméticas arbitrariamente com números primos.

O grande avanço dos computadores ajudou bastante o homem na descoberta de pares de primos com valores tão altos, o que mostra que o homem evolui e ainda poderá evoluir e fazer novas descobertas com ajuda dos computadores.

Alem disso, outro fato além dos primos gêmeos são os números em que a diferença entre eles sejam quatro ou, mesmo, oito como ocorre ente (11,19).Tais números também são infinitos?Claro que esses números não são tão conhecidos como os primos gêmeos, mas estão associados ao mesmo problema existe uma infinitude deles?

Perguntas como essas são respondidas em longo prazo e hoje tudo leva a crer que sim, que existem infinitos números primos gêmeos.

Existe ainda um fato curioso é que os únicos primos consecutivos são o 2 e3 e, é claro, não são considerados primos gêmeos, pois fogem da definição.

A grande verdade é que os primos gêmeos são um dos muitos problemas que envolvem os números primos e quem descobrir uma prova definitiva sobre a infinitude desses números terá seu nome lembrado e falado durante muitos e muitos anos, o que é o desejo de muitos matemáticos da atualidade.

2.4. A Grande Busca de Entender os Números Primos

Na grande busca de fórmulas que geram números primos, muitos matemáticos investiram tempo e esforço com o intuito de conseguirem enfim solucionar um dos problemas que atormenta há tempos os grandes estudiosos da Matemática.

A ordem irregular dos números primo de aparecerem aleatoriamente, não nós dá nenhuma pista de encontrar uma fórmula específica que gere tais números.

Euler (apud Sautoy, 2010, p.55) afirmou que:

> Há alguns mistérios nos quais a mente humana jamais penetrará. Para nos convencermos desse fato, basta fitarmos as tabelas de primos que os objetos fundamentais sobre os quais construímos nosso organizado mundo

matemático se comportem de maneira tão irregular e imprevisível.

Ainda na obra de Sautoy (2010, p.14)

> Ainda sim, apesar de sua aparente simplicidade e de seu caráter especial, os números primos penduram como os objetos mais misteriosos já estudados pelos matemáticos. Em uma disciplina dedicada a encontrar padrões e ordem, os primos representam o desafio supremo. Observe uma lista de números primos, e você descobrirá que é impossível prever quando o próximo surgirá deles. A lista parece caótica, aleatória, não nos fornece qualquer pista sobre como determinar o próximo número. A sequência de primos é a pulsação da matemática, mas é uma pulsação tonificada por uma forte coquetel de cafeína.

Justamente pelo seu caráter contraditório é que faz dos números primos objeto de estudo de vários estudiosos não somente matemáticos, mas além disso curiosos,biólogos,criptoanalistas,entre outros que em seus estudos tentam descobrir o grande mistério dos números primos.

2.4.1 Probabilidade dos números primos

Já sabemos que os números primos são infinitos, mas se observamos bem, grandes números primos são mais raros de se obter que números primos pequeno

Exemplo: há 25 números primos até 100.

16 números primos entre 1000 e 1100

11 números primos entre 10000 e 10100 e seis entre 100000 e 100100

Figura 2: Números Primos de menores que 1000.

2	3	5	7	11	13	17	19	23	29	31	37	41	43
47	53	59	61	67	71	73	79	83	89	97	101	103	107
109	113	127	131	137	139	149	151	157	163	167	173	179	181
191	193	197	199	211	223	227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503	509	521
523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977	983	991	997

Fonte: https://www.estudopratico.com.br/numeros-primos/

Em Derbyshire (2012, p. 50) contata-se o fato da raridade de números primos grandes.

> Se examinarmos com cuidado a lista de primos, veremos que eles vão rareando a medida que avançamos. Entre 1 e 100, existem 25 números

> primos; entre 401 e 500,17; e entre 901 e 1000, apenas 14. O número de primos em qualquer bloco de cem números inteiros parece declinar. Se eu continuasse a lista para mostrar todos os números primos até um milhão, veríamos que existem apenas oito primos no último bloco de cem (isto é, de 999.901 a 1.000.000). Se eu prosseguisse até um trilhão, haveria apenas quatro no último bloco de cem (são eles: 999.999.999.937; 999.999.999.959; 999.999.999.961; e 999.999.999.989).

Quando falamos em infinidade de números temos uma idéia de quantidade indefinida, mas se fizermos a razão entre os números primos e os compostos entre um e P essa razão tende a diminuir quando o valor de P é grande.

Nos estudos sobre a probabilidade de números primos destacaram-se os matemáticos Gauss e Legendre. Ambos estabeleceram a relação entre logaritmo e probabilidade para encontrar números aproximados de números primos em sequências finitas.

A diferença é que Gauss utilizou o logaritmo na base e para seus cálculos e Legendre utilizou logaritmo decimal. È bem verdade que eles não descobriram formulas com extrema precisão, mas com elas temos uma boa aproximação.

O grande problema para gerar fórmulas para números primos e que não existe um padrão para isso. Grandes matemáticos tentaram e falharam no processo.

Em Peruzzo (2012, p. 9)

> A aparente ausência de qualquer ordem na distribuição e sucessão dos números primos sempre atormentou os matemáticos, ao mesmo tempo que os deixavam e ainda deixam fascinados. Se os primos são os blocos constituintes dos números inteiros e estes são a base de nossa compreensão do universo, porque a sua forma não é determinada por uma lei, ou neste caso, por uma fórmula matemática?

Nomes como Gauss, Euler, Mersene, Fermat entre tantos outros se dedicaram bastante, porém não tiveram o êxito que almejavam. O matemático e ou pesquisador que descobrir uma fórmula que gere números primos certamente terá seu nome marcado na história.

2.4.2 Primos na Sequência de Fibonacci

Leonardo Fibonacci (1170 – 1250) foi um matemático italiano que se destacou no período da Idade Média. Uma das sequência mais conhecidas atualmente e estudas na Matemática foi criada por ele.

Figura 3: Leonardo Fibonacci

Fonte: Google Imagens.

Os números da sequência de Fibonacci obedecem à seguinte função.

0, se n = 0;

F(n)= 1, se n = 1;

$F_{n+1}=F_n+ F_{n-1}$, se n≥1

n	0	1	2	3	4	5	6	7	8
F(n)	0	1	1	2	3	5	8	13	21

No quadro exprimimos os primeiros valores de n da sequência de Fibonacci

Dentro dessa sequência temos também uma sequência de números primos que fazem parte da sequência de Fibonacci.

Os primeiros números primos são:

2, 5,13, 89, 23,1597, 28657, 514229.

Se prolongarmos essa sequência, a sequência de números primos continuará, claro, com valores muito maiores.

Em Sautoy (2013, p.55)

> Há uma intrigante conexão entre a sequência de Fibonacci e os protagonista deste capitulo, os primos. Olhemos para os primeiros números de Fibonacci.:
>
> 1,1,2,3,5,8,13,21,34,55,89,144...
>
> Todo p-ésimo número de Fibonacci, onde p é um número primo é ele próprio primo. Por exemplo, 11 é primo e o 11º número de Fibonacci é 89, também primo. Se isso sempre funcionasse seria um ótimo modo de gerar primos

> cada vez maiores. Infelizmente não funciona. O 19º número de Fibonacci é 4.181, e embora 19 seja primo, 4,181 não é: vale 37x113. Nenhum matemático até hoje provou se existe uma quantidade infinitamente grande de números de Fibonacci primos. Esse é outro dos muitos mistérios não solucionados dos números primos na matemática.

Essa intrigante conexão que foi relatada acima é objeto de estudos de vários pesquisadores e não somente matemáticos mais também cientistas da computação e outros pesquisadores amantes dos números primos.

2.4.3 Números de Fermat

Pierre de Fermat (1601-1665) foi matemático e cientista francês. Em 1640 Fermat escreveu em uma carta em que ele achava que números da fórmula $Fn=2^{2n}+1$ eram primos.

Figura 4: Pierre de Fermat.

Fonte: Google Imagens.

Mais tarde Euler mostrou que Fermat estava equivocado, pois para F1 temos 5; F2=17;F3=257,F4=65537,mas para F5 temos 6416700417 um número composto.

Alguns matemáticos da geração de Fermat e Mersenne estudaram as propriedades dos números. Fermat não fornecia suas provas matemáticas em muitas descobertas feitas por ele só foram enunciadas muito tempo depois. De fato, naquela época a Matemática tinha uma abordagem mais experimental e pode ser por isso que as provas matemáticas não eram tão valorizadas e importantes quanto eram para os gregos.

Ainda sobre Fermat no século XVII, deu outra contribuição ao mundo ao introduzir o Teorema que tem seu nome a respeito dos números primos, o chamado pequeno teorema de Fermat.

2.4.4 A Busca por Geração de Números Primos

Na busca por encontrar funções que gerassem números primos um matemático se destacou dos demais, e deu inúmeras contribuições a Teoria dos Números.

Leonhard Euler (1707-1783) descobriu um polinômio no qual gerava uma sucessão longa de números primos, mas para um certo valor F(n) a função resultava em um número composto.Euler encontrou outros polinômios desse tipo,porém o mais conhecido deles é o $F(n)= n^2+ n+41$

Figura 4: Leonhard Euler

Fonte: Google Imagens.

Esse polinômio gera números primos para n=1,2,3,4...39,mas para n=40 temos

$F(40)=40^2+40+41$

$F(40)=40(40+1)+41$

$F(40)=40.41+41$

$F(40)=41(40+1)$

$F(40)=41.41$,um número composto.

Até mesmo Euler, o grande matemático, teve dificuldades em encontrar fórmulas que gerasse números primos e que até o presente momento nenhum matemático conseguiu.

Na obra de Peruzzo (2012, p. 65 e 66) podemos a importância pela busca dos números primos.

> Por mais de meio século o maior número primo encontrado foi 2^{127} -1, com 39 algarismos, descoberto pelo matemático francês Lucas em 1876, após 19 anos de trabalho. Este ficou sendo o maior primo testado por mais de 75 anos.
>
> Com o advento dos computadores encontrou-se números primos muito maiores como 180($2^{127}-1)^2$+1 em 1952, com 79 algarismos. Atualmente o maior número primo encontrado é: $2^{43112609}$ -1 descoberto em 2008, num projeto de computação distribuído pela Internet, o qual usa o tempo ocioso do processador de muitos computadores pessoais, procurando por números primos específicos do tipo primos de Mersene.

A ação conjunta de projetos de computação também foi e é importante, já que pessoas se unem em prol de uma ação maior e que pode trazer contribuições importantes.

2.5 Números Primos, além da Matemática

Uma curiosidade bastante interessante na Biologia acontece no reino animal, mais precisamente com duas espécies de cigarra chamadas *Magicada sependecim* e *Magicada tredecim*.

O ciclo de vida são respectivamente 17 e 13 anos. Mas, porque esses dois números são tão importantes no ciclo de vida das cigarras? Primeiramente a sincronia de vida delas é algo difícil de acontecer, pois 17 e 13 são números primos, logo elas só podem compartilhar o mesmo habitat em 221anos(221=17x13)

Dessa forma elas não competem entre si e com tanta frequência o que seriam prejudiciais a ambas as espécies.

Se o ciclo de vida das cigarras fossem números pares, por exemplo, haveria uma coincidência maior no ciclo de vidas delas, e, portanto uma maior competitividade entre elas, podendo ocasionar até mesmo a extinção de uma delas naquele território.

Este exemplo serve para mostra que existe a uma integração entre as ciências e até mesmo entre a Matemática dos números primos e a Biologia estão conectadas.

2.6 Um Passo Importante no Desenvolvimento dos Números, a Teoria dos Números

Com a invenção do zero e dos números negativos, posteriormente, novas estudos foram feitos em relação aos números. Nessa grande busca dos matemáticos de entenderem melhor as propriedades dos números criou-se a Teoria dos Números. Esse ramo da matemática estuda como já foi dito as propriedades dos números, mas principalmente dos números inteiros.

Por muitos a Teoria dos Números é considerada a rainha da Matemática e às vezes é chamado também de “alta Aritmética”, nomes consagrados da Matemática como: Gauss, Fermat, Euler, Mersene, entre outros se destacaram no estudo dos números.

Gauss (1777-1855) afirmou certa vez que “é exatamente isso o que da a maior aritmética que encanto mágico que tornou a ciência preferida dos matemáticos para não mencionar sua riqueza inesgotável, em que tão supera gradualmente outras partes da Matemática”

O mesmo Gauss considerado um dos maiores matemáticos de todos os tempos já era fascinado pelos estudos dos números e também deixou enormes contribuições a humanidade.

Os matemáticos que trabalham nessa área são chamados de teoristas dos números e em seus estudos tentam descobrir e estabelecer as relações que os diferentes tipos de números possuem entre si.

Não somente isso mais vale destacar a importância também das aplicações da teoria dos números a matemática aplicada. Tanto que com o desenvolvimento da tecnologia o estudo dos números passou a ter utilização prática, cada vez, mais constantes e hoje é empregada em áreas como: criptografia, ciência da computação, teoria dos códigos e até mesmo na Arte, mostrando com isso as várias aplicações dessa disciplina e o desenvolvimento que os números trouxeram as nossas vidas.

2.7 Breve Histórico da Criptografia

Na obtenção dos dados, os primeiros relatos sobre a arte de ocultar informações dói datada no quinto século antes de Cristo. A criptografia é a arte e ou ciência capaz de esconder informações e deixá-las ocultas.

De acordo com Sing (2011, p. 20):

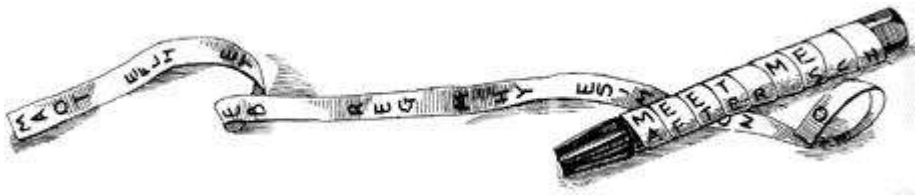
> Alguns dos primeiros relatos sobre escritas seretas datam de Heródoto " o pai da história", de acordo com o filósofo e estadista romano Cícero.Heródoto, escreveu As histórias, narrou os conflitos entre Grécia e a Pérsia, ocorrida no quinto século antes de Cristo

Em Sidnei(2016, p. 15) temos que:

> Embora o termo "criptografia" tenha sido cunhado apenas em 1920, um de seus métodos clássicos foi definido mais de mil anos antes.. No século IX por volta de 850, o matemático árabe Al-Kindi(Iraque, 801-853), conhecido no Ocidente como Alkindus, publicou um manuscrito sobre a decifração de mensagens criptográficas. O manuscrito incluía uma descrição de método de freqüência para a decifração de mensagens criptográficas simples.

Na Grécia antiga a criptografia foi utilizada para esconder segredos de guerras, por exemplo. Foi utilizado por espartanos para esconder informações. Quando o citale (bastão de madeira) era desenrolado a tira continha uma variação de letras aleatórias, porém quando enrolada novamente no citale correto a mensagem original poderia ser lida corretamente.

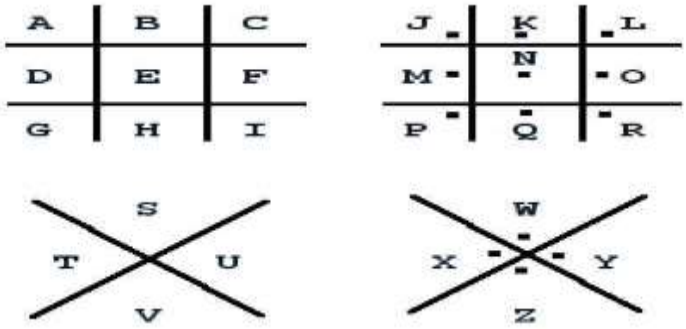
Figura 5: bastão de Licurgo



Fonte: Google imagens.

A cifra do chiqueiro como é conhecida à cifra abaixo e também conhecida como cifra maçônica, troca letras por símbolos da grade, como podemos verificar na figura abaixo. Além dos maçons é também utilizada por estudantes.

Figura 6: Cifra do Chiqueiro



Fonte: Google imagens

Um código muito conhecido em todo o mundo desenvolvido por Samuel Morse (criador do telégrafos elétrico) é, justamente, o código Morse.Esse código substitui cada letra do alfabeto por uma série de pontos e traços.Mais tarde o código foi aperfeiçoado pela introdução de letras acentuadas.

Porém, o código Morse não é um sistema criptográfico, pois o objetivo da mensagem nesse caso não é de oculta-lá, pelo contrário, o código Morse é um alfabeto alternativo que não é usado para esconder informações.Ele serve para a transmissão de mensagens á distância que são transmitidos a pulsos de longa e pequena duração e pausas entre a mensagem.

2.7.1 Criptografia RSA

A criptografia com chave pública foi proposto inicialmente pela dupla Diffie e Hellman em 1976. Em Sing “Diffie tinha bolado um novo tipo de cifra, que incorporava a chamada chave assimétrica.”

Entende-se por assimétrica duas chaves a chave publica e a chave privada, ou seja a ideia de criptografar e descriptografar. Até então os modelos de criptografar que eram utilizados eram simétricos, ou seja, usa uma única chave para o processo de criptografar e descriptografar.

Tempos depois um professor chamado Ron Rivest decidiu criar um algoritmo com as idéias da dupla Diffie e Hellman. Para isso o professor “recrutou” dois colegas Adi Shamir e Len Adleman para trabalharem juntos.

Segundo Sing (2011, p. 297)

> Rivest, Shamir e Adleman formavam uma equipe perfeita.Rivest um cientista da computação com tremenda capacidade para absorver idéias novas e aplicá-las nos locais mais improváveis. Ele sempre se mantinha a par dos mais recentes trabalhos de pesquisa, que o inspirava a apresentar toda uma série de candidatas estranhas e e maravilhosas para a função de mão única que estaria no coração da cifra assimétrica.

Adleman era o matemático que trabalhava com a dupla de cientistas da computação no qual passarm quase um ano trabalhando juntos. Em 1977 Rivest fez uma descoberta importante. Ele descobriu uma maneira de criar uma função de mão única, com base em funções modulares. O trio originalmente era Adleman, Rivest e Shamir (ARS) e, após uma discussão do trio eles resolveram mudar o nome para RSA, hoje conhecida como criptografia RSA.

O trio do MIT (*Massachusetts Institute of Technology*) propôs um sistema com base na

matemática da teoria dos números com base nos estudos, fatoração e do teorema de Fermat e do pequeno teorema de Fermat.

Para começar são escolhidos, secretamente, dois Números Primos (P e Q), de modo que N=P·Q, onde N é conhecido como Módulo Codificador (O número N é o único de conhecimento de todos). Os números P e Q, escolhidos secretamente, consituem as chaves para decifrar o código RSA.

Em seguida um número público F é dado a todos para que possam dele usufruir. O número F é chamado de número de codificação e é igual para todos os usuários. É usado para codificar um número de cartão de crédito, por exemplo, de uma determinada página da Internet.

No final da década de 70 a Criptografia começa a se fazer presente na computação com o trio do MIT utilizando técnicas da matemática pura.

Em Sing (2011, p. 420), temos que:

> Rivest, Shamir e Adleman criaram uma função de mão única especial, que pode ser revestida somente por alguém com acesso a informação privilegiada, ou seja, os valores P e Q. Cada função pode ser uma personalização de P e Q, que, multiplicados um pelo outro, darão o valor de N. A função permite que qualquer um cifre mensagens para uma pessoa em especial usando o valor de N que aquela pessoa escolheu, mas somente o destinatário poderá decifrar a mensagem, pois o destinatário é a única pessoa que conhece p e q, e, portanto, é a única pessoa que conhece a chave de decifragem, d.

No caso, só é possível descobrir **D** conhecendo-se os primos P e Q. O número **d** é também chamado à chave de decifragem, conhecida como chave particular.

2.8 A Inter-relação da Matemática com a Criptografia

E bem verdade que o processo descrito acima parece ser fácil, porém quando lidamos com números estritamente grandes, mesmo com a ajuda de computadores o processo se torna lento demais.

De acordo com Sautoy (2013, p.250)

> A matemática usada por Rivest para criar esse truque criptográfico é bastante simples. As cartas são embaralhadas por meio de cálculo matemático. Quando o cliente faz um pedido na página da internet o computador utiliza o número de seu cartão de crédito para realizar um cálculo. O cálculo é fácil de ser fazer, mas quase impossível de ser desfazer sem que se conheça a chave secreta. Isso ocorre porque o cálculo não e feito numa calculadora convencional, em sim em uma calculadora- relógio de Gauss.

E o que torna esse processo, fascinante, tão importante? A reposta para isso é o modo como as potencias são computadas.

Vejamos o que relata Sautoy (2013, p.251)

> E se o hacher tentasse verificar todas as horas possíveis na calculadora-relógio? Sem chance. Atualmente, os criptógrafos utilizam relógios nos

> quais o N, o número de horas tem mais de cem algarismos - em outras palavras há mais horas no relógio do que o número de átomos no universo.

De acordo com Lemos (2010, p. 77) “A tendência, com o passar dos anos para garantir segurança, é o aumento no tamanho das chaves, isto é, a escolha de primos p e q maiores, já que novos e melhores algoritmos de fatoração surgem”.

O que é preciso na escolha dos números primos para a segurança do RSA é que eles sejam grandes e longe um do outro, pois se estivessem perto demais um do outro o algoritmo de Fermat seria colocado em prática e os números primos descobertos.

Não se pode negar que o desenvolvimento da interação entre criptografia e matemática tornou-se mais importante porque promoveu a união da matemática com as ciências experimentais.

2.9. O Futuro da Criptografia

Com novas formas de acessar a internet (celulares, palmtop e outros aparelhos) possibilitou também um aumento nas vendas de produtos comprados via internet. O grande problema, é que esses aparelhos possuem menos memória do que um computador e seus processadores também são mais lentos o que não é ideal para codificar um cartão de crédito para uma compra online, por exemplo. Sendo assim foi desenvolvido uma nova forma de criptografia, a criptografia por curvas elípticas.

Em Lemos (2010, p. 113) temos que:

> Curvas elípticas são objetos matemáticos fascinantes e altamente sofisticados. Tem inúmeras aplicações nos tópicos considerados nestas notas. São utilizadas nos melhores algoritmos para fatoração de inteiros, em algoritmos randomizados para decidir primalidade em alguns sistemas de criptografia pública.

Até hoje a criptografia esta sendo adotada por grandes agências governamentais. De acordo com Sautoy (2012, p. 43), “O número do cartão de crédito é movimentado ao redor das curvas elípticas , escondendo suas pegadas no processo.”

O estudo de algumas áreas da matemática como curvas elípticas se tornou tão sério que é preciso autorização para publicação de certos trabalhos sobre teoria dos números.

Em Sautoy (2012, p. 45) contata-se que:

> Em questões mais domesticas, Kloblitz se ressente das restrições que a NSA, agência de Segurança Nacional dos Estados Unidos, mantém sobre essa área da matemática. Atualmente, é necessário obter autorização da NSA para poder publicar certos trabalhos sobre teoria dos números, mesmo em jornais matemáticos mais desconhecidos. Graças às novas ideias de Kloblitz, as curvas elípticas se juntaram aos primos na “lista restrita” de pesquisas que o governo deseja monitorar.

Hoje a RSA faz estudos próprios sobre curvas elípticas conjuntamente com seu sistema.

2.10. A Criptografia é o Futuro.

È inegável a importância da Internet nos dias atuais. Através do celulares e computadores ela faz parte de nossas vidas e dependemos dela em quase tudo que fazemos. Ir a um lugar novo com o GPS (em inglês *global positioning system* traduzindo para nosso idioma sistema de posicionamento global) jogar um jogo online, fazer uma transação bancária, fazer compras e até mesmo entrar em sites de relacionamento são ações mais do que comuns e a tendência é que dependeremos ainda mais da Internet para vivermos.

Em Michael (2016, p. 13) podemos perceber que:

> Inúmeros tipos de aparelhos inteligentes já foram criados ou estão sendo projetados, para o uso em uma infinidade de diferentes ambientes. Como exemplo só para nossas residências, já existem termostatos inteligentes, lâmpadas e fechaduras automáticas, conectadas por Wi-Fi, câmeras de seguranças, babás eletrônicas online e até geladeiras conectadas a Internet. Infelizmente, muitos deles demonstram ser dotados de sérias vulnerabilidades de segurança, pois foram projetados priorizando apenas questões de funcionalidades.

Educar as pessoas para o futuro ou mesmo criar oportunidades para se ter acesso a informação será de suma importância as futuras gerações.

Ainda em Michael (2016, p. 15) temos que:

> Felizmente, está-se criando cada vez mais consciência sobre a necessidade de educar corretamente os futuros profissionais, a necessidade de criamos cursos de engenharia criptográfica, de técnico em criptografia, de tecnólogo criptográfico, de validador ou testador de sistemas seguros, de projetista de hardware seguro, de projetista e analista de software seguro, de uma gama de profissões e especializações profissionais que precisaremos no futuro próximo.

Fica claro que muitas outras profissões estão e poderão surgir com o desenvolvimento da Internet, porém os desafios também serão imensos. Problemas como: autenticação de usuários, quebra de sigilo, segurança nacional, necessidade de interceptar informações e prevenção de crimes são só alguns problemas que surgirão com o tempo e o futuro estará no desenvolvimento da criptografia.

3 METODOLOGIA

A metodologia utilizada nesse trabalho foi a pesquisa bibliográfica, tendo como fonte de pesquisa artigos, livros, sites e revistas da temática. Com o levantamento de dados podemos trabalhar o que foi lido e fazer uma interpretação dos dados.

De acordo com Célia (2009, p. 13):

> Através desses princípios, a realidade passa a ser percebida pelos olhos da ciência não de uma forma desordenada e fragmentada, como ocorre na visão subjetiva do senso comum, mas sob enfoque de um princípio explicativo que esclarece e proporciona a compreensão do tipo de relação que se estabelece sobre os fatos, coisas e fenômenos unificando a visão de mundo. Nesse sentido, o conhecimento científico é expresso sob forma de enunciados que explicam as condições que determinam a ocorrência dos fatos e dos fenômenos relacionados a um problema.

Dentre os principais autores que mais fundamentaram esta pesquisa, pode-se destacar Sautoy (2012; 2013) e Sing (2011).

Ainda em Célia (2009, p. 14):

> O conhecimento científico é um produto resultante da investigação científica. Surge não apenas da necessidade de encontrar soluções para problemas de ordem prática da vida diária, características do conhecimento do senso comum, mas do desejo e da necessidade de fornecer explicações sistemáticas que possam ser testadas e criticadas através de provas empíricas. É um produto da necessidade de se alcançar um conhecimento "seguro"

Sobre o conhecimento "seguro" teve-se como base a pesquisa de livros, revistas, artigos, e teses de outros pesquisadores devidamente registrados para o desenvolvimento do presente trabalho.

4 CONSIDERAÇÕES FINAIS

A ideia de que todo número maior que um não primo, pode ser escrito como um produto de números primos é um dos teoremas mais importantes da matemática e é conhecido como teorema fundamental da aritmética. Muitos estudiosos se dedicaram aos estudos sobre números primos e desenvolveram uma área importante da matemática a teoria dos números.

Ao longo dos anos muitas descobertas foram feitas e outras até os dias de hoje continuam em aberto fazendo com que muitos estudiosos do mundo todo continuem seus estudos e façam novas descobertas.

Aproximadamente, na década 70 os números primos passaram a ter uma maior importância não só na matemática pura, mas também na computação. O estudo dos números primos serviu de base para os algoritmos de criptografia de chaves públicas. Muitos prêmios foram oferecidos a pessoas ou empresas que tentassem gerar números primos grandiosos como 10 bilhões de dígitos 100bilhões de dígitos entre outros. O que comoveu os grandes estudiosos e pessoas da área.

Importante ressaltar que as ciências não progridem sozinhas, mas em conjunto, e o estudo dos números primos na teoria dos números deu base à outra ciência,a ciência da computação, e com isso a criptografia ganhou um novo destaque na atualidade com o crescimento da internet. Vale destacar a importância da matemática nos modernos sistemas criptográficos. A matemática unida a criptografia é um exemplo magnífico de como a as ciências estão interligadas no nosso cotidiano.

E no final deste trabalho algumas considerações sobre o futuro envolvendo a criptografia merecem ser abordadas. Estamos educando as pessoas para o futuro ou criando oportunidades para se ter acesso a informação?

O que os governantes internacionais e ou nacionais tem a falar sobre interceptação de informações, prevenção de crimes e quebra de sigilo, atualmente? Estarão os profissionais capacitados para lidarem com todos esses problemas?

Muitos problemas surgirão com o tempo e o futuro estará no desenvolvimento da criptografia.

REFERÊNCIAS

Célia, Regina.(2009). *Metodologia do Trabalho Científico*. Curitiba: IESDE Brasil S.A

Coutinho, S. C. (2005). *Números Inteiros e Criptografia.* Rio de Janeiro: IMPA.

Derbyshire, Jonh. (2012). *Obesessão Prima.* Tradução de Jesus de Paula Assis. Rio de Janeiro: Editora Record.

Eves, Howard. (2005). *Introdução à História Da Matemática.* São Paulo: Editora Unicamp.

Lemos, Manoel. (2010). *Criptografia, Número Primos e Algoritmos.* Pernambuco.Universidade Federal de Pernambuco. Distribuição IMPA.

Marmo, Antônio. (n/d) *Curso de Matemática Moderna Lisa.* Barueri: Editora Lisa S.A.

Michael, Sean. (2016). *Criptografia Essencial:* A Jornada do Criptógrafo. Rio de Janeiro: Editora Elsevier.1º ed.

Nobuo, Daniel. (2017). *Princípios de Criptografia Quântica.* SP, São José. Disponível em <http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf> Acesso em 21 de maio de 2017.

Peruzzo, Jucimar. (2012). *O Fascínio dos Números Primos*.1º ed. Irani SC edição do autor.

Pimentel, Elaine Gouvêa. (2006). *Teoria de números e criptografia RSA.* Maio. Disponível em: <http://www.mat.ufmg.br/~elaine/OBMEP/criptografia.pdf >. Acesso em: 26 de março de 2018

Postal, Tannery. (2008). *Criptografia RSA.* Monografia (Graduação) – Curso de Licenciatura em Matemática, UFMT, Cuiabá.

Sautoy, Marcus du. (2012). *A Música dos números primos:* a história de um problema não resolvido na matemática. Tradução de Diego Alfaro. Rio de Janeiro: Jorge Zahar.

_____. (2013). *Os mistérios dos números.* Tradução George Schlesinger. Rio de Janeiro: Editora Zahar.

Stallings, William. (2008). *Criptografia e Segurança de Redes - Princípios e Práticas.* Editora: Prentice Hall do Brasil.

Sidnei, Raul. (2016). *A história da computação.* 1º edição Rio de Janeiro. Editora ElSEVIER

Sing, Simon. (2011). *O livro dos códigos.* Tradução de Jorge Calife. Rio de Janeiro, Record.

Viswanathan, Tim. (1979). *Instituto de Matemática pura e aplicada.* Rio de janeiro.

SITES INVESTIGADOS

http://www.uff.br/sintoniamatematica/curiosidadesmatematicas/curiosidadesmatematicas-html/audio-primos-br.html

http://www.dimap.ufrn.br/~bedregal/Tese-alunos/Monografia%20Ricardo.pdf

https://www.estudopratico.com.br/numeros-primos/

http://www.ebah.com.br/content/ABAAAAfvW4AE/criptografia-Instituto