**UNIVERSIDADE FEDERAL DE SÃO CARLOS – UFSCAR**

**PROFMAT – MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**DEPARTAMENTO DE MATEMÁTICA**

# CRIANDO MENSAGENS SECRETAS NA ESCOLA BÁSICA UTILIZANDO A CRIPTOGRAFIA – RSA

**WALDIR CLAUDIO DE CASTRO JUNIOR**

**SÃO CARLOS**

**2015**

**UNIVERSIDADE FEDERAL DE SÃO CARLOS – UFSCAR**

**PROFMAT – MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**DEPARTAMENTO DE MATEMÁTICA**

# CRIANDO MENSAGENS SECRETAS NA ESCOLA BÁSICA UTILIZANDO A CRIPTOGRAFIA – RSA

**WALDIR CLAUDIO DE CASTRO JUNIOR**

**Dissertação de mestrado profissional apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de Mestre em Matemática.**

**Orientador:** Prof. Dr. Pedro Luiz Aparecido Malagutti

**SÃO CARLOS**

**2015**

**Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária da UFSCar**

C355cm

Castro Junior, Waldir Claudio de.
Criando mensagens secretas na escola básica utilizando a criptografia – RSA / Waldir Claudio de Castro Junior. -- São Carlos : UFSCar, 2015.
85 f.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2015.

1. Matemática - estudo e ensino. 2. Criptografia. 3. Matemática aplicada. I. Título.

CDD: 510.7 (20ª)

**UNIVERSIDADE FEDERAL DE SÃO CARLOS**

Centro de Ciências Exatas e de Tecnologia
Programa de Mestrado Profissional em Matemática em Rede Nacional

## Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Waldir Claudio de Castro Júnior, realizada em 21/08/2015:

Prof. Dr. Pedro Luiz Aparecido Malagutti
UFSCar

Prof. Dr. Silvia Cristina Martini Rodrigues
UMC

Prof. Dr. Joao Carlos Vieira Sampaio
UFSCar

Dedico este trabalho aos meus familiares, minha esposa e amigos, os quais sempre me apoiaram nos momentos difíceis, dando a força necessária para seguir em frente.

# *Agradecimentos*

Agradeço em primeiro lugar a Deus, “Tudo posso naquele que me fortalece”.

Agradeço à minha esposa Flávia, sempre disposta a ajudar em momentos complicados e de cansaço por conta de trabalhos exaustivos.

Agradeço a meus familiares, meu pai Waldir e minha mãe Solange, sem eles nada seria possível e às minhas irmãs Fabiana e Sylmara que sempre acreditaram e se orgulharam de meu trabalho.

Agradeço a todos os professores e colegas que me ajudaram no Mestrado Profissional - PROFMAT - na UFSCar, sou grato à paciência e dedicação de todos vocês.

Agradeço em especial ao professor e orientador Pedro Malagutti; sem sua disposição e paciência, talvez o caminho não se tornasse tão gratificante.

Muito obrigado a todos, pela confiança.

# *RESUMO*

A criptografia é um assunto fascinante do ponto de vista prático; é útil para acessar contas bancárias, *e-mails* e redes sociais. Segundo esta perspectiva, esta dissertação baseou-se em mostrar o quão simples pode ser a utilização da criptografia. No trabalho realizado foi mostrado que é possível, para alunos do Ensino Fundamental e Médio, codificar e decifrar mensagens utilizando a criptografia - RSA, a qual envolve o conceito da criação de chaves públicas e chaves privadas para a codificação de mensagens. Uma atividade simples, porém importante do ponto de vista utilitário, foi aplicada para mostrar aos alunos do 9º ano do Ensino Fundamental, da 1ª e 2ª séries do Ensino Médio de uma escola particular do interior paulista para mostrar o quão interessante e prazerosa pode ser a utilização da Matemática. Tais atividades não constam usualmente nos materiais didáticos tradicionais. Nesta dissertação será apresentado o ferramental teórico, contendo teoremas e corolários, assim como suas demonstrações, os quais justificam, matematicamente, a validade das técnicas e do algoritmo utilizados na criptografia – RSA. As atividades não pressupõem pré-requisitos sofisticados, podendo ser aplicadas em sala de aula, em situações reais, para que os alunos apreciem a beleza da Matemática.

**Palavras-chave:** criptografia – RSA; chaves públicas; chaves privadas; aplicações da matemática no ensino.

# *ABSTRACT*

Cryptography is a fascinating topic, concerning the practical point of view, and it is useful to access bank accounts, e-mails and social networks. According to this perspective, this study aimed to show how simple it may be to make use of cryptography. It was proved, through the work performed, that it is possible for students from elementary and high school to encrypt and decrypt messages using R.S.A. Cryptography, which involves the concept of creating public keys and private keys for the encryption of messages. A simple but powerful activity on the utility view was assigned to show students from the 9$^{th}$ grade of elementary school and from the 1$^{st}$ and 2$^{nd}$ years of high school from a private school in São Paulo State how interesting and pleasurable the use of Mathematics can be. Such activities are not usually present in the traditional didactic materials. The theoretical tools, containing theorem and corollaries, as well as their demonstrations, which mathematically justify the validity of techniques and the algorithm used on R.S.A. Cryptography will be presented. The activities do not assume sophisticated prerequisites and can be applied in the classroom, in real situations, so that the students can appreciate the beauty of Mathematics.



**Key-words:** R.S.A. Cryptography; public keys; private keys, applications of Mathematics in teaching.

# LISTA DE FIGURAS

**SUMÁRIO**

# 1. INTRODUÇÃO

## 1.1 Breve relato da trajetória profissional

Desde muito pequeno me dou bem com os números. Não me lembro ao certo com qual idade comecei a gostar efetivamente da Matemática, mas me lembro que na antiga 8ª série (hoje 9º ano) do Ensino Fundamental comecei a perceber a lógica por detrás dos números. Comecei a notar que não se tratava apenas de fórmulas e regras prontas para serem usadas, mas que, em muitas situações, havia uma lógica extremamente bem elaborada e bem organizada que permitia construir o conhecimento dedutivo, desde as contas mais simples até os raciocínios mais complexos.

Naquela época, tive a oportunidade de fazer um trabalho com poliedros de Platão; foram feitas planificações por meio de dobraduras, com o cuidado de que, quando montadas, os sólidos fossem construídos com perfeição. Nesse entremeio, realizei também pesquisas sobre a validade da fórmula de Euller, a qual ainda não havia sido apresentada por completo no Ensino Fundamental. Além disso, trabalhei com as áreas das figuras criadas a partir das planificações. Essa atividade foi criada para uma oficina de geometria, realizada durante uma feira anual de ciências, desenvolvida pelo colégio onde estudava. Nessa feira de ciências, os alunos de cada sala eram separados em grupos e cada grupo era orientado por um professor. Geralmente, os alunos eram escolhidos de acordo com as afinidades que tinham para com as matérias que os professores lecionavam. Com isso, pude perceber também que já era visto como um bom aluno de matemática, já que fui selecionado junto com mais alguns colegas, pela professora de matemática. E, com a orientação da professora, desenvolvemos todo o trabalho sobre os poliedros de Platão, mostrando exemplos do manuseio da fórmula de Euller e da construção dos sólidos.

Quando atingimos certa idade, começam as especulações sobre qual curso devemos escolher na faculdade, e ainda, em qual faculdade devemos ingressar. Felizmente, a minha decisão já estava tomada. Entretanto, tantos outros amigos ainda se debruçavam sobre os livros buscando um caminho correto, que lhes proporcionasse uma vida digna. Optei pela graduação em Matemática, já que, como citado acima, tal

disciplina já havia me despertado interesse. Muitos diziam que, pela facilidade com os números, um curso de engenharia seria mais vantajoso, ou traria um retorno financeiro maior. Porém, a decisão já havia sido tomada. Não que eu já soubesse que me tornaria professor, mas havia um interesse maior em saber um pouco mais sobre aqueles números, os quais haviam me conquistado há alguns anos. Por meio do vestibular, tive o prazer de ser aprovado em duas Universidades públicas e a escolha pela Universidade Federal de São Carlos veio por certas comodidades, tais como a presença de outros amigos mudando para a mesma cidade, o que facilitava muito a adaptação à vida universitária, longe dos pais.

Contrastando com todas as opiniões, segui esse árduo caminho. Foram cinco anos de graduação, batalhando muito com disciplinas e trabalhos acadêmicos. Contudo, ao final do curso vi o quão gratificante a profissão de professor pode se tornar.

Comecei a lecionar aos 19 anos de idade, e não demorei muito tempo a me apaixonar pela profissão e perceber que ser professor não é algo que se faz por obrigação, mas é obrigatório que se faça com prazer. Preparar aulas, corrigir provas, trabalhar com alunos e lidar com a indisciplina não são situações que se possa resolver por obrigação pelo resto da vida. Após dez anos de caminhada, ainda não me cansei de aprender coisas novas e de tentar melhorar a cada dia, para que meus alunos possam aprender a matemática tão bonita que me chamou a atenção quando adolescente. Entender a lógica matemática é bem complicado, mas, assim como um dia pude ver a beleza dos números, quero transmitir essa beleza. Por isso escolhi a prática docente.

Todavia, há momentos na vida em que necessitamos de algo mais. Percebemos a rotina em que nos encontramos e, com isso, surge a necessidade de subir um degrau na escada da aprendizagem e de buscar um diferencial, tanto no currículo, quanto na prática docente. Nossos alunos precisam que estejamos sempre engajados no que estamos ensinando, para que possam sentir-se atraídos pela matéria que lecionamos.

Com esse desejo em mente, comecei a procurar por programas de pós-graduação. Cheguei a fazer um curso de especialização em gestão financeira, pois eu ministrava aulas no curso de administração e sentia a necessidade de estar inserido no universo administrativo, para que as aulas não ficassem apenas nas fórmulas e aplicações matemáticas. Eu precisava mostrar aos alunos que aquela matéria lhes seria útil em algum momento. Apesar de não ter concluído o curso, as aulas freqüentadas

puderam me dar uma base muito melhor para continuar ministrando as minhas disciplinas.

A mesma necessidade citada acima aparecia nas aulas do Ensino Fundamental e Médio. Foi então que me deparei com o programa de pós-graduação PROFMAT, que oferecia a oportunidade desejada com a idéia mais voltada para a sala de aula (exatamente o que supriria a minha necessidade). O único problema era vencer o obstáculo das vagas, já que não sou professor da rede pública, logo a concorrência seria mais árdua, já que a quantidade de vagas era menor.

A primeira tentativa foi para o PROFMAT na cidade de Uberaba, sediado pela Universidade Federal do Triângulo Mineiro, UFTM, em 2012. Porém, não obtive sucesso para a classificação em uma das quatro vagas destinadas a demanda social (para professores que não fossem da rede pública de ensino). Foi então, no final de 2012, que resolvi prestar o programa PROFMAT, dessa vez na Universidade Federal de São Carlos, UFSCar, pois já conhecia a qualidade do departamento de matemática e sabia da seriedade com que os professores sempre se dedicavam à instituição. Assim, em 2013 comecei o programa de pós-graduação PROFMAT, que representou uma grande ascensão profissional e me abriu um leque de possibilidades docentes, além de me abrir os olhos para uma matemática mais aprofundada.

## 1.2 Organização da dissertação

As primeiras técnicas utilizadas para o envio de mensagens secretas eram baseadas na troca de chaves entre os interessados em manter o sigilo de tais mensagens. Espiões, nos tempos modernos chamados de *hackers*, ameaçavam o segredo dessas mensagens, pois conseguiam, de alguma maneira, essas chaves, já que a mesma chave utilizada para cifrar a mensagem deveria ser usada para decifrá-la.

> O método de criptografia RSA baseia-se neste sistema de chaves duplas e na impossibilidade prática de se obter a chave secreta a partir da chave pública. Isto se deve ao fato de não se conhecer atualmente algoritmos para decompor números grandes em fatores primos em um tempo razoável – uma impossibilidade tecnológica. (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 108)

Ainda, segundo Bezerra, Malagutti e Rodrigues (2010), a chave pública consiste em um procedimento C utilizado por outras pessoas para que enviem as mensagens criptografadas. Este tipo de procedimento é publicado em uma lista ou estão disponíveis na internet. Cada recebedor deve guardar com muito sigilo um segundo procedimento D, sua senha secreta, para decifrar as mensagens recebidas. O que acontece, exatamente, é o que procedimento D reverte o procedimento C, trazendo de volta a mensagem original.

Pode-se notar que toda a ideia sobre a criptografia RSA é baseada na construção de uma função bijetora, sendo que, quanto mais difícil for inverter, ou encontrar a função inversa, mais seguro será o código.

> A idéia é transformar letras em números e construir uma função bijetora **C** definida no conjunto numérico obtido para usá-la na codificação de mensagens. A função inversa de **C** será denotada por **D** e usada para decifrar as mensagens criptografadas.
>
> Qualquer função bijetora serve para este processo funcionar; entretanto se for fácil obter **D** a partir de **C**, será também fácil "quebrar o código", tornando o sistema frágil. O método RSA nos fornece uma maneira de se obter as funções **C** e **D** com bastante segurança. (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 108)

Observando esta situação deparei-me com o tema desta dissertação: a criptografia RSA, a qual recebe esse nome por conta dos sobrenomes dos cientistas do MIT (Massachusetts Institute of Technology), responsáveis pela criação do método (Rivest, Shamir e Adleman). Trata-se de uma ferramenta de grande poder, utilizada o tempo todo, como por exemplo, na Internet, quando se realizam transferências bancárias, envios de *e-mails*, acessos às redes sociais, dentre outros.

Sempre busquei algo a mais para responder perguntas frequentemente formuladas pelos alunos: "Qual a utilidade da matemática?", ou então evitar comentários como: "Nunca vou usar isso na minha vida". Entretanto, na maioria das minhas buscas, me deparava com algum raciocínio muito complexo, difícil de ser explicado a um aluno típico da escola básica.

Esta dissertação foi feita com o intuito de mostrar aos alunos o quão simples e elegantes podem ser algumas teorias, com algumas aplicações que são utilizadas

diariamente sem que sequer tenhamos conhecimento de sua existência. Essa dissertação defende o ponto de vista de que os alunos podem entender muito bem o conceito da criptografia RSA sem nunca terem estudado álgebra superior ou teoria avançada dos números. É evidente que as demonstrações sofisticadas são deixadas de lado, por conta da maturidade dos alunos, assim como ocorre com várias teorias ensinadas regularmente no Ensino Fundamental ou Médio. Alguns ajustes foram feitos a fim de não tornar a ideia muito teórica, e sim, bem prática.

Ao longo desta dissertação serão mostrados os conceitos e teoremas de maneira mais aprofundada, que foram utilizadas de maneira adaptada para as aulas sobre a criptografia RSA. Serão mostrados também os raciocínios que os alunos tiveram durante o decorrer das atividades, assim como as dúvidas e os problemas que surgiram. Apesar de ser um estudo adaptado aos alunos, essa dissertação tenta deixar claro conceito da criptografia RSA. Tal adaptação será feita através do uso de números primos pequenos (dois dígitos, no máximo). Entretanto, para garantir a segurança do método, na realidade, a criptografia RSA é feita com números primos bem maiores (mais de 100 dígitos).

Esta dissertação mostrará primeiramente todo o embasamento teórico para oferecer uma compreensão sobre a criptografia RSA. O objetivo é deixar claras as validades das fórmulas e dos teoremas utilizados que permitem o entendimento da criptografia; pontuar seus princípios e, posteriormente, apresentá-la como uma atividade agradável e compatível com o conhecimento dos alunos dos ensinos fundamental e médio.

Em um segundo momento, esta dissertação deixará claro como o experimento/atividade foi desenvolvido pelos alunos. Será comentado como cada pergunta e cada passo da atividade foram elaborados para que os alunos se sentissem interessados e interados ao assunto proposto.

Em seguida, será mostrado como os alunos foram separados em três grupos e como conseguiram compreender o assunto proposto, resolvendo as atividades e se empenhando em debater as situações criadas pelos outros grupos. Serão relatadas ainda as dificuldades, facilidades e problemas encontrados durante o processo de criação e decodificação das mensagens criptografadas.

Por fim, buscar-se-á responder a seguinte pergunta:

É possível que os alunos jovens sejam capazes de aprender como a Matemática pode ser usada para fabricar um sistema seguro e atual de troca de mensagens secretas?

O mais importante é verificar que a matemática está em tudo o que vivemos, e que, ao criar situações didaticamente adaptadas, torna-se possível demonstrar o poder dos números, sem que os alunos, necessariamente, tenham que cursar graduação em Matemática ou áreas afins. Este era um sonho do matemático e educador alemão Felix Klein, do qual compartilhamos plenamente.

# 2. FERRAMENTAL TEÓRICO – O ALGORITMO RSA

Este capítulo terá a preocupação de deixar claro o algoritmo para a criação das chaves pública e privada, artifícios que norteiam a criptografia RSA, assim como mostrar a utilização das chaves no processo de criação das mensagens cifradas e de decodificação das mesmas.

Alguns teoremas serão necessários para garantir o rigor matemático por detrás da criptografia RSA, bem como alguns corolários, proposições e definições. A fim de garantir uma maior relevância matemática, os teoremas, corolários e proposições serão demonstrados neste capítulo, possibilitando a busca de uma melhor compreensão sobre as justificativas na utilização de algumas fórmulas no desenvolvimento do algoritmo RSA.

Será feita uma pequena introdução sobre o surgimento da criptografia e sobre a criação da criptografia RSA, assim como a utilidade do método do ponto de vista prático e seguro.

Será apresentado ainda o método em si, formalizando cada etapa do algoritmo. Para mostrar como o algoritmo funciona, um exemplo acompanhará cada etapa, para que haja maior clareza no funcionamento prático da criptografia RSA. É necessário lembrar que o método é feito de maneira adequada, utilizando números com uma quantidade de algarismos bem menor do que a quantidade considerada segura para a aplicação do método. Essa adequação garante o efeito didático da criptografia RSA, tornando-a acessível aos alunos.

Ao final deste capítulo, será apresentada uma aplicação da criptografia RSA utilizando os números e a data de validade de um cartão de crédito. Para que o banco possa assegurar os dados do cartão do cliente, no exemplo, utilizar-se-ão números bem maiores (ainda que não grandes o suficiente), mostrando a relevância do método.

Este capítulo é baseado no material escrito por C. Rousseau e Y. Saint-Aubin, Mathematics and Technology, 2008, fazendo referências a algumas de suas passagens e utilizando alguns de seus exemplos.

## 2.1. Introdução à criptografia RSA

A criptografia é um assunto tão velho quando a própria civilização. O ser humano sempre tentou inventar códigos para transmitir mensagens que não poderiam ser entendidas por indivíduos indesejados. Todavia, construir esses códigos sempre fora uma tarefa árdua, já que estudiosos poderiam quebrá-los, eventualmente. Além disso, a pessoa que desejava enviar o código e a pessoa que o receberia deveriam saber como decifrá-lo, o que deixava o código suscetível às interceptações.

A criptografia RSA recebeu este nome devido a seus inventores (Rivest, Shamir e Adleman) e descreve um tipo de criptografia de chave pública. O que chama a atenção nesse algoritmo é o fato de ele ainda não ter sido quebrado, mesmo após mais de 30 anos de tentativas dos melhores cientistas na área. O mais impressionante é saber que todos os detalhes do sistema de criptografia RSA são completamente abertos ao público, havendo a necessidade de saber "apenas" a decomposição de um número grande em fatores primos para quebrar o sistema utilizado na criptografia RSA. A impossibilidade prática de se obter tal decomposição é justamente o que não permite que super computadores e mentes brilhantes consigam quebrar o código.

O algoritmo utilizado na criptografia RSA é baseado na teoria dos números, envolvendo a aritmética de congruência módulo $n$, e o pequeno teorema de Fermat, generalizado por Euler. Todo o sistema gira em torno de três propriedades:

- A dificuldade de um computador em fatorar números grandes.
- A facilidade de um computador em criar números primos grandes.
- A facilidade de um computador em reconhecer se um número primo é grande.

Existem muitos benefícios na utilização do sistema de criptografia de chave pública. Na troca de mensagens secretas, tanto quem envia quanto quem recebe deve conhecer os detalhes do sistema utilizado para criptografar a mensagem. E, justamente no compartilhamento desses detalhes, o perigo aparece. Entretanto, esse perigo não existe com a criptografia RSA, dado que todo o sistema é divulgado a todos, é público.

## 2.2. Algumas Ferramentas da Teoria dos Números

Esta seção é destinada a desenvolver algumas ferramentas de extrema necessidade para o desenvolvimento do algoritmo utilizado para a criação e utilização das chaves pública e privada. Ainda são demonstradas algumas proposições e alguns corolários fundamentais para garantir a validade das etapas que serão desenvolvidas no estudo da criptografia RSA.

***Definição 1***

***i)*** Sejam $a$ e $b$ dois inteiros. Dizemos que $a$ divide $b$ se existir um inteiro $q$ tal que $b = aq$. Escrevemos $a \mid b$.

***ii)*** O máximo divisor comum (mdc) de $a$ e $b$, denotado por $(a,b)$, é definido pelas seguintes duas propriedades:

- $(a,b) \mid a$ e $(a,b) \mid b$
- Se $d \mid a$ e $d \mid b$ então $d \mid (a,b)$

***iii)*** Dizemos que $a$ é congruente a $b$ módulo $n$ se $n \mid (a-b)$, em outras palavras, se existe $x \in \mathbf{Z}$, tal que $(a-b) = n.x$. Escrevemos $a \equiv b \pmod{n}$.

***Proposição 1***

Considere $a,b,c,d,x,y \in \mathbf{Z}$, então segue que:

- Se $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$, então $a+b \equiv c+d \pmod{n}$;
- Se $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$, então $ab \equiv cd \pmod{n}$;
- Se $a \equiv c \pmod{n}$ e $b \equiv d \pmod{n}$, então $ax+by \equiv cx+dy \pmod{n}$.

(em outras palavras, a congruência módulo $n$ é compatível com as operações de adição e multiplicação de inteiros).

***Demonstração***

Como $a \equiv c \pmod{n}$, temos que $n \mid a-c$, então há a existência de algum $x \in$ **Z** tal que $a-c=nx$. Do mesmo modo, como $b \equiv d \pmod{n}$, temos que $n \mid b-d$, então existe $y \in$ **Z** tal quem $b-d=ny$.

Mostrar que $a+b \equiv c+d \pmod{n}$ é equivalente a mostrar que $n \mid (a+b)-(c+d)$, assim:

$$\begin{aligned}(a+b)-(c+d) &= a+b-c-d = \\ &= a-c+b-d = \\ &= nx+ny = \\ &= n(x+y)\end{aligned}$$

Portanto, $n \mid (a+b)-(c+d)$.

Mostrar que $ab \equiv cd \pmod{n}$ é equivalente a mostrar que $n \mid ab-cd$, assim:

$$\begin{aligned}ab-cd &= (ab-ad)+(ad-cd) = \\ &= a(b-d)+d(a-c) = \\ &= any+dnx = \\ &= n(ay+dx)\end{aligned}$$

Portanto, $n \mid ab-cd$.

Mostrar que $ax+by \equiv cx+dy \pmod{n}$ é equivalente a mostrar que $n \mid (ax+by)-(cx+dy)$, assim:

$$\begin{aligned}(ax+by)-(cx+dy) &= ax-cx+by-dy = \\ &= x(a-c)+y(b-d) = \\ &= xnx+yny = \\ &= n(x^2+y^2)\end{aligned}$$

Portanto, $n \mid (ax+by)-(cx+dy)$.

O algoritmo de Euclides nos permite calcular o máximo divisor comum, $(a,b)$, de dois inteiros *a* e *b*, usando-se o algoritmo da divisão. A proposição abaixo mostra os detalhes do algoritmo; a noção de divisão dos inteiros com resto é de suma importância.

***Proposição 2 (Algoritmo de Euclides)***

Sejam *a* e *b* dois inteiros positivos com $a \geq b$, e seja $\{r_i\}$ uma sequência de inteiros construída da seguinte forma: divida *a* por *b*, chamemos $q_1$ o quociente da divisão e $r_1$ o resto, tal que $a = b.q_1 + r_1$, com $0 \leq r_1 < b$.

Do mesmo modo, dividamos *b* por $r_1$, tendo $b = r_1.q_2 + r_2$, com $0 \leq r_2 \leq r_1$.

Repetindo o processo, teremos $r_{i-1} = r_i.q_{i+1} + r_{i+1}$, com $0 \leq r_{i+1} \leq r_i$.

A sequência $\{r_i\}$ é estritamente decrescente. Assim, deve existir um inteiro *n* tal que $r_{n+1} = 0$. Então, $r_n = (a,b)$.

***Demonstração***

Comecemos mostrando que $r_n \mid a$ e $r_n \mid b$. Como $r_{n+1} = 0$, a última equação pode ser escrita $r_{n-1} = r_n.q_{n+1}$, então $r_n \mid r_{n-1}$. A penúltima equação é dada por $r_{n-2} = r_{n-1.}q_n + r_n$, e como $r_n \mid r_{n-1}$, então $r_n \mid r_{n-1.}q_n + r_n = r_{n-2}$. Então podemos repetir o processo, vendo que $r_n \mid r_i$, para todo *i*.

Então, $r_n \mid q_2.r_1 + r_2 = b$, e como $r_n \mid b$ e $r_n \mid r_1$, temos que $r_n \mid b.q_1 + r_1 = a$.

Logo $r_n \mid a$ e $r_n \mid b$.

Por fim, devemos mostrar que sendo um *d* divisor de *a* e *b*, *d* divide $r_n$.

Façamos o caminho inverso, como $d \mid a$ e $d \mid b$, então $d \mid r_1 = a - b.q_1$. Na segunda equação verificamos que, como $d \mid b$ e $d \mid r_1$, então $d \mid r_2 = b - r_1.q_2$. Sendo assim, repetindo o processo, vemos que $d \mid r_i$ para todo *i*, e em particular *d* divide $r_n$.

Portanto, como $r_n$ divide *a* e *b*, e ainda, escolhendo um divisor qualquer de *a* e *b*, ele também divide $r_n$, então $r_n = (a,b)$.

Para exemplificar esta proposição pode-se observar a seguinte questão, bem como sua resolução, publicada na RPM 29, por Zelci Clasen de Oliveira:

Um terreno retangular de 221 *m* por 117 *m* será cercado. Em toda a volta desse cercado, serão plantadas árvores igualmente espaçadas. Qual o maior espaço possível?

O pensamento geométrico para tal resolução pode ser descrito como abaixo:

O valor 117 não divide 221. Fazendo a diferença 221 menos 117, encontramos 104. Porém, 104 não divide 117. Fazendo a diferença 117 menos 104, encontramos 13, que divide 104 e é a resposta do problema.

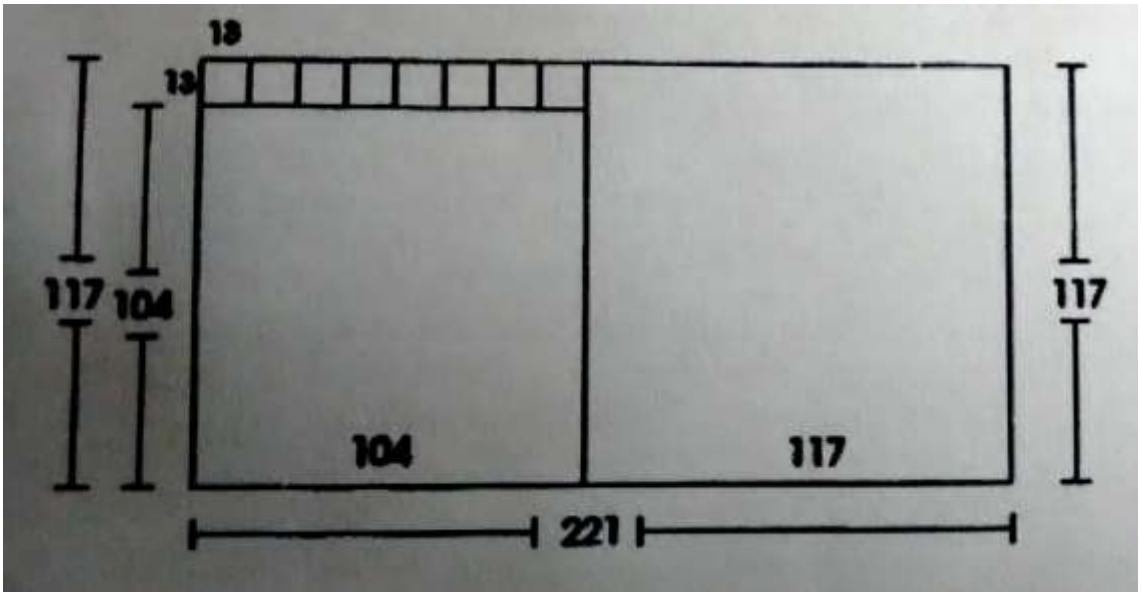



*Figura 1 – Exemplo de mdc*

A figura acima mostra como a resolução foi feita e representa uma resolução geométrica utilizando o princípio das divisões sucessivas.

### *Corolário 1*

Sejam $a$ e $b$ dois inteiros e seja $c=(a,b)$, então existe $x,y\in \mathbf{Z}$ tal que $c=ax+by$.

***Demonstração***

Como $c=(a,b)$, sabemos que $c=r_n$, isso é garantido pela proposição 2, acima.

Temos que $r_{n-2}=r_{n-1}.q_n+r_n$, então podemos isolar $r_n$, conseguindo a equação

$$r_n=r_{n-2}-r_{n-1}.q_n. \qquad (1)$$

Observando a equação $r_{n-3} = r_{n-2}.q_{n-1} + r_{n-1}$ e isolando $r_{n-1}$, conseguimos a equação:

$$r_{n-1} = r_{n-3} - r_{n-2}.q_{n-1}. \qquad (2)$$

Substituindo a equação (2) na equação (1), teremos:

$$\begin{aligned} r_n = r_{n-2} - r_{n-1}.q_n &\Rightarrow r_n = r_{n-2} - (r_{n-3} - r_{n-2}.q_{n-1}).q_n \\ &\Rightarrow r_n = r_{n-2} - r_{n-3}.q_n + r_{n-2}.q_{n-1}.q_n \\ &\Rightarrow r_n = r_{n-2}(1 + q_{n-1}.q_n) - r_{n-3}.q_n \qquad (3) \end{aligned}$$

Observando a equação $r_{n-4} = r_{n-3}.q_{n-2} + r_{n-2}$ e isolando $r_{n-2}$, conseguimos a equação:

$$r_{n-2} = r_{n-4} - r_{n-3}.q_{n-2}.$$

Agora, substituindo a equação (4) na equação (3), teremos:

$$\begin{aligned} & r_n = r_{n-2}(1 + q_{n-1}.q_n) - r_{n-3}.q_n \Rightarrow r_n = (r_{n-4} - r_{n-3}.q_{n-2})(1 + q_{n-1}.q_n) - r_{n-3}.q_n \\ & \Rightarrow r_n = r_{n-4} + r_{n-4}.q_{n-1}.q_n - r_{n-3}.q_{n-2} - r_{n-3}.q_{n-2}.q_{n-1}.q_n - r_{n-3}.q_n \\ & \Rightarrow r_n = r_{n-4}(1 + q_{n-1}.q_n) - r_{n-3}(q_{n-2} + q_{n-2}.q_{n-1}.q_n + q_n) \end{aligned}$$

Continuando o processo de iteração, chegaremos à equação $r_n = r_1 x_1 + r_2 y_1$ (5), onde $x_1, y_1 \in \mathbf{Z}$.

Ainda vimos na proposição anterior que $b = r_1 q_2 + r_2$, e isolando $r_2$ temos a equação $r_2 = b - r_1 q_2$ (6), a qual substituindo em (5), teremos:

$$\begin{aligned} r_n = r_1 x_1 + r_2 y_1 &\Rightarrow r_n = r_1 x_1 + (b - r_1.q_2).y_1 \\ &\Rightarrow r_n = r_1 x_1 + b y_1 - r_1.q_2.y_1 \\ &\Rightarrow r_n = r_1(x_1 - q_2.y_1) + b y_1 \qquad (7) \end{aligned}$$

Finalmente, na proposição anterior tínhamos que $a = bq_1 + r_1$ e também isolando $r_1$ temos a equação $r_1 = a - bq_1$ (8). O que nos leva ao resultado final, substituindo (8) em (7):

$$r_n = r_1(x_1 - q_2.y_1) + by_1 \Rightarrow r_n = (a - bq_1)(x_1 - q_2.y_1) + by_1$$
$$\Rightarrow r_n = ax_1 - a.q_2.y_1 - b.q_1.x_1 - b.q_1.q_2.y_1 + b.y_1$$
$$\Rightarrow r_n = a(x_1 - q_2.y_1) + b(-q_1.x_1 - q_1.q_2.y_1 + y_1)$$
$$\Rightarrow r_n = a\,x + b\,y$$

sendo $x = x_1 - q_2 y_1$ e $y = -q_1.x_1 - q_1.q_2.y_1 + y_1$.

Observação; Esta demonstração, além de mostrar que *(a,b)* é uma combinação linear com coeficientes inteiros de *a* e *b*, também fornece um método construtivo de se obter tal combinação.

***Proposição 3***

***i)*** Seja $c = (a,b)$. Então *c* é caracterizado pela seguinte propriedade:
$c = \min\{ax + by \mid x, y \in \mathbf{Z}, ax + by > 0\}$.

***ii)*** Considere $a, b, m \in \mathbf{N}$, então $(ma, mb) = m(a,b)$

***iii)*** Considere $a, b, m \in \mathbf{N}$. Se $c \mid ab$ e $(c,b) = 1$, então $c \mid a$.

***iv)*** Se *p* é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

***<u>Demonstração</u>***

***i)*** Definimos $E = \{ax + by; x, y \in \mathbf{Z}, ax + by > 0\}$ e seja $c = (a,b)$. Pelo corolário 1, temos que $c \in E$. Vamos supor que exista $d = ax' + by' \in E$, com $d > 0$ e $d < c$. Como $c \mid a$ e $c \mid b$, então $c \mid ax' + by'$, assim $c \mid d$. Entretanto, $0 < d < c$, o que nos leva a uma contradição. Logo $c = \min\{ax + by \mid x, y \in \mathbf{Z}, ax + by > 0\}$.

***ii)*** Por ***i)***, como $m \in \mathbf{N}$, temos que:

$$(ma.mb) = \min\{m.a.x + m.b.y \;;\; x, y \in Z,\; m.a.x + m.b.y > 0\}$$
$$= m.\min\{ax + by \;;\; x, y \in Z,\; ax + by > 0\}$$
$$= m(a,b)$$

***iii)*** Como $(c,b) = 1$, pelo corolário 1, existem $x, y \in \mathbf{Z}$ tal que $cx + by = 1$. Multiplicando os dois lados por *a*, obtemos $acx + aby = a$. Então, temos que $c \mid acx$ e $c \mid aby$, pois $c \mid ab$. Assim, $c \mid (acx + aby)$. Logo, $c \mid a$.

***iv)*** Utilizando ***iii)***, com $c = p$, Se $(p,b)=1$, então $p \mid a$. Por outro lado, podemos ter $(p,b)=d>1$. Como os únicos divisores de um número primo são 1 e *p*, então teremos $d = p = (p.b)$, ou seja, $p \mid b$.

***Corolário 2***

Sejam *a* e *n* dois inteiros, com $a \leq n$. Se $mdc(a,n)=1$, então existe um único $x \in \{1,2,...,n-1\}$ tal que $ax \equiv 1(\text{mod}\, n)$.

***Demonstração***

Comecemos pela existência. Como $mdc(a,n)=1$, então existem $x, y \in \mathbf{Z}$, tal que $ax+ny = mdc(a,n)=1$. Assim, $ax = 1-ny$, ou seja, $ax \equiv 1(\text{mod}\, n)$.

Agora, provemos a unicidade. Vamos supor que exista outra solução $x' \in \{1,2,...,n-1\}$, com $ax' \equiv 1(\text{mod}\, n)$. Assim $a(x-x') \equiv 0(\text{mod}\, n)$ e então, verificamos que $n \mid a(x-x')$. Como $mdc(a,n)=1$, então $n \mid x-x'$. Mas, $x-x' \in \{-(n-1),...,n-1\}$, logo, $x-x'=0 \Rightarrow x = x'$ e daí segue a unicidade.

Muitos dos corolários e proposições dados acima garantem o cálculo envolvendo a congruência modulo *n* sem a utilização de algum artifício computacional elaborado. Porém, vale a ressalva de que na aplicação das atividades com os alunos, as contas foram feitas com o auxílio de uma calculadora contendo a função "mod *n*", a qual faz o cálculo da congruência módulo *n* sem maiores problemas, inclusive para números relativamente grandes.

Alguns outros teoremas e proposições ainda estarão presentes na próxima seção, a fim de fortalecer e esclarecer melhor as passagens que compõem o algoritmo RSA.

## 2.3. Como Criar Chaves Públicas e Privadas

Nesta parte do trabalho será apresentado o algoritmo para a criação e utilização das chaves pública e privada envolvidas na criptografia RSA. Todos os passos serão exemplificados com a utilização de números pequenos para uma melhor compreensão. Algumas outras ferramentas também serão enunciadas e demonstradas durante este processo, sendo, sempre que possível, serão acompanhadas pelo exemplo geral que ajudará a elucidar os estudos presentes nesta unidade.

A chave pública é criada pela pessoa que deseja receber as mensagens de maneira segura, tal pessoa é responsável pelas escolhas na montagem da chave. Por praticidade, as passagens serão separadas por etapas.

Os resultados serão apresentados seguindo de perto o tratamento dado por Rousseau e Saint-Aubin (Mathmetics and Technology, 2008, p.214).

- **1ª Etapa**

Faz-se a escolha de dois números primos grandes (com mais de cem dígitos), nomeando-os $p$ e $q$. E em seguida calcula-se $n = p.q$. Este número $n$ é a chave pública e, caso a escolha dos números primos seja como requerida, terá mais de duzentos dígitos. Dado $n$, os computadores atuais não conseguem encontrar os valores de $p$ e $q$ em um tempo razoável.

Exemplo:

Tome $p = 13$ e $q = 17$, dois números primos. Calculando $n = p \,.\, q$, obtém-se $n = 13 \,.\, 17 = 221$. Este número será a chave pública utilizada em todo o processo de criação de um sistema RSA simples.

- **2ª Etapa**

Calcula-se $\phi(n)$, sendo $\phi$ a função de Euler. A função de Euler, $\phi(n)$, dá a quantidade de números inteiros no conjunto $\{1,2,...,n-1\}$ que são primos entre si com $n>1$. Por convenção, $\phi(1)=1$. A proposição demonstrada abaixo mostrará que $\phi(n)=(p-1)(q-1)$. Note que a fórmula depende dos valores de *p* e *q*, o que apresenta mais uma dificuldade na quebra do código.

***Proposição 4***

Sejam *p* e *q* dois números primos distintos. Então $\phi(pq)=(p-1)(q-1)$.

***Demonstração***

Queremos contar quantos inteiros temos no conjunto $E=\{1,2,3,...,pq-1\}$ que são primos com *pq*. Os únicos inteiros que não são primos com *pq* são os múltiplos de *p*, ou seja, são os elementos do conjunto $P=\{p,2p,3p,...,(q-1)p\}$, o qual tem $(q-1)$ elementos, e os múltiplos de *q*, são os elementos do conjunto $Q=\{q,2q,3q,...,(p-1)q\}$, o qual tem $(p-1)$ elementos. Lembremos que $P\cap Q=\emptyset$, já que *p* e *q* são primos, segundo hipótese.

Assim, dos $(pq-1)$ elementos de E, somente os $(q-1)$ elementos de *P* e os $(p-1)$ elementos de *Q* não são primos entre si com *n*, deixando assim:

$$pq-1-(p-1)-(q-1)\Rightarrow$$
$$\Rightarrow pq-p-q+1\Rightarrow$$
$$\Rightarrow p(q-1)-1(q-1)\Rightarrow$$
$$\Rightarrow (p-1)(q-1)$$

Portanto, $\phi(n)=(p-1)(q-1)$ é a quantidade de números primos com *n*, que são positivos e menores do que *n*.

Exemplo:

Calculando $\phi(221) = (13-1)(17-1) = 12 \,.\, 16 = 192$, tem-se 192 números inteiros primos com 221, sendo eles todos os elementos do conjunto $\{1,2,...,220\}$, exceto os múltiplos de 13 e 17, que são os seguintes 28 números: 13, 17, 26, 34, 39, 51, 52, 65, 68, 78, 85, 91, 102, 104, 117, 119, 130, 136, 143, 153, 156, 169, 170, 182, 187, 195, 204 e 208, ou seja, $\varphi(221) = 220 - 28 = 192$.

- **3ª Etapa**

Escolhe-se um número $e \in \{1,2,...,n-1\}$ relativamente primo com $\phi(n)$. Este número *e* é a chave, juntamente com *n*, utilizada para criptografar a mensagem e será parte da chave pública.

Exemplo:

Como $\phi(221) = 192$, dentre estes 192 números deve-se escolher um número *e* relativamente primo com 192, por exemplo, 5. Pode-se verificar rapidamente que $(e, \phi(n)) = (5,192) = 1$, pois 5 é um número primo e $192 = 2^6 .3$. Logo, tem-se a chave pública para codificar a mensagem, $e = 5$ e $n = 221$.

- **4ª Etapa**

Existe um inteiro $d \in \{1,2,...,n-1\}$, tal que $e.d \equiv 1 \bmod \phi(n)$. Sua existência foi garantida pelo corolário 2, enunciado e demonstrado acima. A maneira de calcular este número *d* está contida na demonstração do corolário 2, e deve fazer uso do Algoritmo de Euclides (proposição 2). Este número *d* é a chave, juntamente com *n*, utilizada para

decodificar a mensagem e é privada, já que para calculá-la é necessário o conhecimento dos números *p* e *q* (ao menos com a teoria até agora existente).

Para o cálculo do número *d* efetua-se a divisão de $\phi(n)$ por *e*, obtendo um quociente $q_1$ e um resto $r_1$. Efetua-se a divisão de *e* pelo $r_1$, obtendo um novo quociente $q_2$ e um novo resto $r_2$. Efetua-se a divisão de $r_1$ por $r_2$, e assim sucessivamente até que o resto obtido seja numericamente igual a 1.

Então, isolando os restos $r_1$, $r_2$ até 1, e substituindo $r_1$ em $r_2$, $r_2$ em $r_3$, até $r_i$ em 1, ter-se-á uma equação da forma $1 = d.e - r.\phi(n)$ e, com os valores de *e* e $\phi(n)$ já conhecidos, pode-se encontrar o valor de *d*.

Exemplo:

Utilizando o Algoritmo de Euclides para calcular *d*, pode-se verificar:

$192 = 38.5 + 2 \Rightarrow 2 = 192 - 38.5 \quad (I)$
$5 = 2.2 + 1 \quad \Rightarrow 1 = 5 - 2.2 \quad (II)$

Substituindo ( *I* ) em ( *II* ), tem-se:

$1 = 5 - 2.(192 - 38.5) = 77.5 - 2.192$, sendo $e = 5$, $\phi(n) = 192$ e comparando com a fórmula $1 = d.e - r.\phi(n)$, pode-se extrair o valor de *d*. Logo, tem-se a chave para decodificar a mensagem, $d = 77$.

- **5ª Etapa**

Para enviar uma mensagem escrita é necessário transformar cada letra em um número correspondente, sendo a letra *a* correspondente ao número 1; *b* correspondente ao número 2 e assim sucessivamente até a letra *z* correspondente ao número 26. Seja *m* um desses números. Enviar a mensagem criptografada consiste em calcular o resto da divisão de $m^e$ por *n*, ou seja, calculamos $c \equiv m^e \mod(n)$, $0 < c < n$. Nesta dissertação

esse cálculo será efetuado com o auxílio de uma calculadora, presente em qualquer computador.

Exemplo:

Suponhamos que mensagem a ser criptografada seja a palavra WALDIR. Assim, primeiramente faz-se a correspondência das letras para transformá-las em números, então WALDIR é correspondente ao conjunto de números: 23 – 1 – 12 – 4 – 9 – 18. Cada um desses valores será colocado no lugar de *m* para calcular $c \equiv m^e \mod(n)$, com $e = 5$ e $n = 221$.

$$c_1 \equiv 23^5 \mod(221) \Rightarrow c_1 = 160$$
$$c_2 \equiv 1^5 \mod(221) \Rightarrow c_2 = 1$$
$$c_3 \equiv 12^5 \mod(221) \Rightarrow c_3 = 207$$
$$c_4 \equiv 4^5 \mod(221) \Rightarrow c_4 = 140$$
$$c_5 \equiv 9^5 \mod(221) \Rightarrow c_5 = 42$$
$$c_6 \equiv 18^5 \mod(221) \Rightarrow c_6 = 18$$

Logo a mensagem criptografada fica representada pelo conjunto de números: 160 – 1 – 207 – 140 – 42 – 18.

- **6ª Etapa**

Com a mensagem criptografada em mãos, basta calcular $m \equiv c^d \mod(n)$, para obter o valor inicial *m* e então voltar à letra correspondente ao número calculado para decodificar a mensagem. As proposições abaixo mostram que o calculo de $c^d \mod(n)$ chega exatamente no valor inicial *m*.

***Pequeno Teorema de Fermat***

Seja $m < n$, sendo m relativamente primo com n, então é válida a equivalência $m^{n-1} \equiv 1 \pmod{n}$, sendo *m* primo.

***Demonstração***

Tome $m \in \{1,2,...,n-1\}$ e considere os produtos $1.m$, $2.m$, ..., $(n-1).m \quad (I)$.

Mostraremos que quando divididos por *n*, os restos $r_k$ desses produtos

$k.m \equiv r_k \pmod{n}$, criam uma permutação da sequencia 1, 2, ..., $n - 1$. Inicialmente, o resto $r_k$ da divisão de $k.m$ por *n* nunca será zero se *n* é primo e $k, m < n$, sendo $r_k$ pertencente a E.

Resta, então, mostrar que os restos são distintos. Suponha que $k_1.m$ e $k_2.m$ tenham o mesmo resto na divisão por *n*. Sem perda de generalidade assuma que $k_1 \geq k_2$. Então, vemos que:

$k_1.m = q_1.n + r$, $k_2.m = q_2.n + r$, e então subtraindo as duas equações obtemos:

$$(k_1 - k_2).m = (q_1 - q_2).n.$$

Então *n* divide $(k_1 - k_2).m$. Como *n* é primo, $0 \leq k_1 - k_2 < n$ e $m < n$, a única possibilidade é que $k_1 = k_2$.

Tomando o produto dos restos $r_i$ módulo *n* da sequencia ( *I* ), vemos que:

$$\begin{aligned}(n-1)! &= 1.2.3...(n-1) = r_1.r_2...r_{n-1} \equiv \\ &\equiv (m.1).(m.2)...(m.(n-1)) \pmod{n} = \\ &= m^{n-1}.(n-1)!\end{aligned}$$

Reescrevendo, temos:

$$n \mid (m^{n-1} - 1).(n-1)!$$

Como *n* é primo, sabemos que $(n,(n-1)!) = 1$. Então $n \mid m^{n-1} - 1$, que é equivalente ao resultado $m^{n-1} \equiv 1 \pmod{n}$.

***Proposição 5***

O codificador "*e*" e decodificador "*d*" são inversos na congruência módulo *n*. Ao se criptografar uma mensagem *m* como *c*, em que $c \equiv m^e \mod(n)$, tem-se sempre a decodificação que leva *c* em *m*, ou seja, $m \equiv c^d \mod(n)$.

***Demonstração***

Sendo $c \equiv m^e \mod(n)$, então:

$$c^d \equiv \left(m^e\right)^d = m^{ed} = m^{k\phi(n)+1} = m^{k\phi(n)}.m = \left(m^{\phi(n)}\right)^k.m$$

Pelo pequeno teorema de Fermat, enunciado e demonstrado acima, temos que:

sendo $\phi(n) = (p-1).(q-1)$, então $m^{\phi(n)} = m^{(p-1).(q-1)} = \left(m^{p-1}\right)^{q-1}$, e como $p$ é primo, temos $m^{p-1} \equiv 1$.

Logo, $c^d \equiv \left(m^{\phi(n)}\right)^k.m \equiv 1^k.m \equiv 1.m \equiv m \pmod{n}$

Portanto $m \equiv c^d \pmod{n}$.

Exemplo:

Com a mensagem criptografada representada pelo conjunto de números 160 – 1 – 207 – 140 – 42 – 18, sendo $d = 77$ e calculando $m \equiv c^d \mod(n)$, chega-se a mensagem original.

$m_1 \equiv 160^{77} \mod(221) \Rightarrow m_1 = 23$
$m_2 \equiv 1^{77} \mod(221) \Rightarrow m_2 = 1$
$m_3 \equiv 207^{77} \mod(221) \Rightarrow m_3 = 12$
$m_4 \equiv 140^{77} \mod(221) \Rightarrow m_4 = 4$
$m_5 \equiv 42^{77} \mod(221) \Rightarrow m_5 = 9$
$m_6 \equiv 18^{77} \mod(221) \Rightarrow m_6 = 18$

Logo, a mensagem decodificada é representada pelo conjunto de números: 23 – 1 – 12 – 4 – 9 – 18, cuja correspondência com relação às letras do alfabeto revela a mensagem secreta WALDIR, como desejado.

## 2.4. Exemplo Complementar

Este exemplo foi adaptado do livro de Rousseau e Saint-Aubin (Mathmetics and Technology, 2008, p. 217 e 218). Uma companhia quer construir um sistema de compras *online*. Para assegurar a transmissão das informações do cartão de crédito do cliente, eles utilizam a criptografia RSA. O cartão de crédito possui dezesseis dígitos com mais quatro dígitos informando a data de validade, totalizando vinte dígitos. A companhia escolhe dois números primos grandes $p$ e $q$. Este exemplo consta de primos com vinte e cinco dígitos, deixando $n = p.q$ com mais de cinquenta dígitos. Então, sendo

$p = 12345679801994567990089459$ e $q = 83695679777773687123430 87$.

Como $n = p.q$, então

$n = 1033280063346665821884785640073336248556226302199 33$.

Calculando $\phi(n) = (p-1)(q-1)$, tem-se

$\phi(n) = 1033280063346665821884785432920858450836859277873 88$.

A companhia escolhe $e = 115670849$ de maneira que $(e, \phi(n)) = 1$ e utiliza o corolário 2 para calcular

$d = 341139317439109257844835610654421839775167312021 77$.

É fácil perceber que esses números não podem ser obtidos por tentativa e erro, necessitando de auxílio computacional.

Considerando um cliente com o cartão de crédito com número 4540 3204 4567 8231 e data de validade 10/02. O cliente quer enviar de maneira segura a mensagem $m = 45403204456782311002$, então o computador calcula

$$c \equiv m^e \equiv 4932908522179127579301751139739556684799888618330 8 \bmod(n)$$

e envia para a companhia. Recebendo a mensagem a companhia calcula

$$m \equiv c^d \equiv 45403204456782311002 = m \bmod(n).$$

Vale lembrar que, apesar de este exemplo conter números primos com uma quantidade grande de dígitos, estes números ainda não são grandes o suficiente para garantir que um computador não consiga fatorar rapidamente o número *n*.

Este exemplo serve para mostrar algo mais próximo da realidade, deixando claro que ao trabalhar com números com muitos dígitos a quebra do código acaba por se tornar algo extremamente complicado até mesmo para computadores, uma falha intransponível para a atual tecnologia.

# 3. DESCRIÇÃO DA ATIVIDADE E DO MATERIAL USADOS EM SALA DE AULA

## 3.1. Metodologia Empregada – A Engenharia Didática

A noção de engenharia didática clássica surgiu no início dos anos 1980. Os primeiros pesquisadores a estudar as diretrizes da engenharia didática foram Yves Chevallard e Guy Brousseau, seguidos por Michèle Artigue, mais ao final dos anos 1980. Essa metodologia apresenta capacidade de mostrar os fenômenos didáticos em condições que se aproximam da funcionalidade de uma sala de aula regular.

A metodologia de engenharia didática baseia-se na concepção, realização, observação e análise de sequências de ensino, confrontando análise *a priori* e análises *a posteriori*. Uma pesquisa, seguindo os princípios de uma Engenharia Didática, deve seguir algumas fases, as quais serão observadas nas etapas dessa dissertação. Essas etapas são, segundo Revemat, R. Eletr. De Edu. Matem., 2008, p. 26 e 27:

- Análises preliminares: considerações sobre o quadro teórico didático geral e os conhecimentos já adquiridos sobre o assunto em questão.

Ao observar as idades dos alunos selecionados para o estudo da criptografia RSA, pode-se notar que os requisitos necessários, tais como fatoração, divisão euclidiana e resolução de equações por meio de substituições, são aprendidos a partir do 8º ano do Ensino Fundamental. Logo, ao realizar o estudo com alunos do 9º ano do Ensino Fundamental até a 2ª série do Ensino Médio, ficou garantida a compreensão do assunto em questão.

- Concepção e análise *a priori* das situações didáticas: o pesquisador, orientado pelas análises preliminares, delimita certo número de variáveis pertinentes ao sistema sobre os quais o ensino pode atuar, chamadas de variáveis de comando.

Com as idades e níveis de aprendizado adequados, a análise *a priori* assegurou aos alunos que o aprendizado ficasse dentro do esperado. Além disso, os alunos foram,

até certo ponto, guiados durante o processo de criação das chaves pública e privada pela folha atividade disponibilizada para cada grupo.

- Experimentação: consiste na aplicação da sequência didática, tendo como pressupostos apresentar os objetivos e condições da realização da pesquisa, estabelecer o contrato didático e registrar as observações feitas durante a experimentação.

Todos os objetivos foram colocados aos alunos de maneira clara, dando, assim, condições para que eles fossem capazes de criar suas próprias chaves públicas e privadas para então, ao final da atividade, conseguir criptografar e decifrar mensagens.

O contrato didático também foi negociado com os alunos para o desenvolvimento eficaz das atividades, tanto teóricas, feitas no primeiro dia, quanto práticas, feitas no segundo dia. Além disso, a experimentação foi registrada em uma folha atividade as quais serão descritas no próximo capítulo desta dissertação (a imagem da folha completa está nos Anexos).

- Análise *a posteriori* e validação: a análise *a posteriori* consiste em uma análise de um conjunto de dados colhidos ao longo da experimentação, como por exemplo, produção dos alunos, registros de observadores e registro em vídeo. Nessa análise, se faz necessário sua confrontação com a análise *a priori* para que seja feita a validação ou não das hipóteses formuladas na investigação.

Essa análise *a posteriori* será apresentada em grande parte na conclusão desta dissertação, mostrando o confronto entre a análise feita *a priori* e a conclusão das atividades, onde será respondida a pergunta central deste trabalho:

É possível que os alunos jovens sejam capazes de aprender como a Matemática pode ser usada para fabricar um sistema seguro e atual de troca de mensagens secretas?

## 3.2. Material Teórico para os Alunos

Primeiramente, um material teórico foi elaborado para que os alunos ficassem realmente inseridos no mundo da criptografia e para que eles vissem a evolução da mesma, devido a necessidade de manter-se segura; sem a possibilidade de quebra em tempo hábil.

O início da parte teórica consistia em apresentar aos alunos um pouco sobre a criptografia primitiva, que foi, basicamente, o primeiro tipo de criptografia que se utilizou, deixando claro seu valor para os demais tipos de criptografia, porém, mostrando também seus problemas e fragilidades. Os exemplos utilizados foram:

- Cifrário de César

  Criptografia baseada na posição das letras do alfabeto, apenas deslocando as letras três posições à frente.

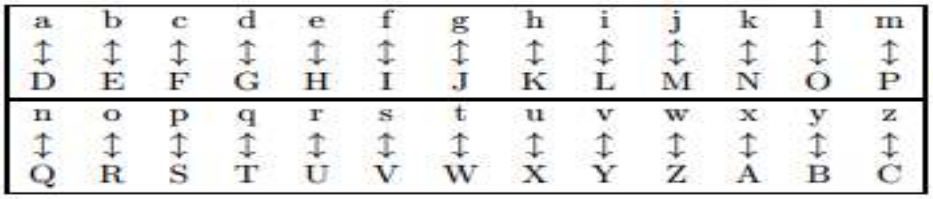



*Figura 2 – Cifrário de César*

Assim, a palavra “matemática” seria transformada em “pdwhpdwlfd” (o acento no segundo a foi omitido).

- Atbash Hebraico

  Criptografia baseada, também, na posição das letras, associando a primeira letra com a última, a segunda com a penúltima e assim por diante.

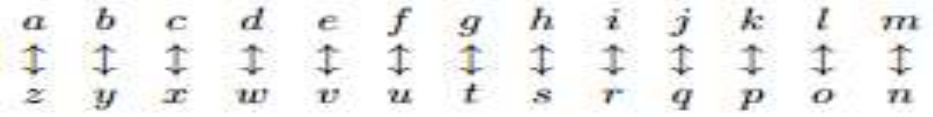



*Figura 3 – Atbash Hebraico*

Assim, a palavra “matemática” seria transformada em “nzgvnzgrxz”.

A partir daí, a ideia lógica de criptografia já estava criada. Então, foi introduzido um breve contexto histórico sobre a criptografia RSA, deixando claro que a prática de mensagens secretas sempre foi utilizada e segue sendo utilizada até os dias atuais. Mas, um método seguro, para deixar essas mensagens em segredo, até então não havia sido criado, uma vez que os métodos de criptografia primitivos poderiam ser quebrados, mesmo que com alguma dificuldade, por intermédio de tentativas e, mais atualmente, com o auxílio de computadores.

Ainda dentro do contexto histórico, foi exposto que em 1977, três cientistas do MIT: Ronald Rivest, Adi Shamir e Leonard Adleman patentearam, utilizando as iniciais de seus sobrenomes, a conhecida criptografia RSA. A partir desse contexto histórico se deu início à problemática da criação de um código seguro.

Os primeiros métodos criptográficos eram chamados de sistemas criptográficos de chave simétrica, os quais consistiam em enviar uma mensagem à outra pessoa, utilizando um código (chave) para tornar essa mensagem secreta. Assim, essa mensagem poderia ser enviada e, a outra pessoa, assim que a recebesse, poderia decodificá-la utilizando o mesmo código (chave) que foi utilizado para criptografá-la. O fato de a chave utilizada pelas duas pessoas ser a mesma dá o nome de chave simétrica, já que, sem a chave correta usada para “trancar” a mensagem, não seria possível “abri-la”.

Verificou-se então que havia problemas com o método, como por exemplo, assegurar o recebimento da chave sem que mais pessoas tivessem acesso a ela.

Então, foi apresentada aos alunos a criptografia de chave assimétrica, a qual consistia em enviar uma mensagem criptografada com uma chave de tipo 1. Quando o destinatário recebesse a mensagem, colocaria uma segunda chave para criptografar a mensagem. Assim, a mensagem seria enviada de volta para a primeira pessoa que decodificaria a mensagem com a sua chave do tipo 1 e reenviaria a mensagem (que estaria “trancada” com a segunda chave). O destinatário receberia a mensagem, agora criptografada apenas com a sua chave, a qual seria decodificada.

Contudo, alguns problemas também poderiam aparecer, tais como a quantidade de processos necessários para criptografar e decodificar uma única mensagem. Sendo

assim, o tempo tornou-se um grande empecilho para a praticidade desse método; apesar de ser um método bem mais seguro do que o método empregado nas chaves simétricas.

Foi então que os três cientistas começaram a pensar na possibilidade de criar um código no qual uma das chaves pudesse ser conhecida (chave pública) ou utilizada por todos que quisessem mandar uma mensagem. Porém, somente a pessoa que recebesse a mensagem poderia decodificá-la, utilizando a sua própria chave (chave privada). Método esse, que possui vários exemplos nos dias atuais, tais como as criptografias utilizadas em bancos, já que todos podem enviar dinheiro para uma conta qualquer, basta possuir o número (chave pública), mas somente a pessoa que possui a senha bancária (chave privada) pode sacar o dinheiro.

Os alunos puderam perceber que, para enviar uma mensagem para outra pessoa, bastava conhecer a chave pública criada por essa pessoa, para que a mensagem pudesse ser criptografada. Depois da mensagem enviada, a pessoa que recebesse poderia decodificar utilizando sua própria chave privada. Um conceito simples de entender, mas não tão simples de ser executado.

Neste momento, os alunos haviam entendido por completo no conceito básico de criptografia RSA. Faltava mostrar que criar tal código era possível e que, para números pequenos, o entendimento era bem acessível.

Foi apresentado a eles, então, que a criptografia RSA baseia-se na escolha de dois números primos grandes e a chave pública é construída como o resultado da multiplicação desses números primos. Como não existem fórmulas para procurar a decomposição de números e fatores primos, mesmo grandes computadores demorariam um tempo considerável para encontrar esses dois números primos a partir do seu produto, já que esse processo só pode ser feito por meio de iterações.

## 3.3. Como Criptografar

Para codificar uma mensagem utilizando a algoritmo da criptografia RSA, bastava que os alunos seguissem alguns passos para criar suas chaves públicas e privadas. Para tanto, desde o início da criação, foi utilizado um exemplo.

Primeiramente, estipulou-se uma tabela para correspondência entre as letras da mensagem e o conjunto de números que representariam a mensagem:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | L | M | N | O | P | Q | R | S | T | U | V | X | Z |

*Figura 4 – Tabela de Conversão*

Assim, era possível começar a criar as chaves necessárias.

O primeiro passo foi escolher dois números primos quaisquer. Para essa atividade os números escolhidos foram 17 e 41.

Após a escolha, efetuou-se a multiplicação dos dois números, definindo assim o número "*n*", o primeiro número da chave pública:

$$n = 17.41 = 697$$

Fez-se, então, uso da função de Euler: $\phi(n) = (p-1).(q-1)$, que no exemplo seguido é igual a:

$$\phi(n) = (17-1).(41-1) = 16.40 = 640$$

Para calcular a segunda parte da chave pública escolheu-se um número "*e*" sendo $mdc(\phi(n), e) = 1$, no caso do exemplo seguido a opção foi o número 13, já que 640 e 13 são números primos entre si.

Assim, a chave pública foi criada com os números 697 e 13.

Neste ponto, já era possível utilizar a correspondência entre letras e números dada pela tabela acima para criptografar a mensagem desejada.

Fazendo uso da congruência módulo *n*, utilizou-se a fórmula:

$$c = m^e \bmod n,$$

sendo *c* o número criptografado, *m* o valor numérico da letra atribuído fazendo uso da tabela acima e "*n"* e "*e"* os números da chave pública.

Para o exemplo utilizado, a fórmula geral para criptografar passou a ser: $c = m^{13} \bmod 697$

Fazendo uso do computador, criptografamos a palavra VERDAO, que possui sequência numérica: 21 – 5 – 17 – 4 – 1 – 14.

| Letra | Fórmula | Valor de c |
|---|---|---|
| V | 21^13 mod 697 | 497 |
| E | 5^13 mod 697 | 326 |
| R | 17^13 mod 697 | 391 |
| D | 4^13 mod 697 | 310 |
| A | 1^13 mod 697 | 1 |
| O | 14^13 mod 697 | 396 |

Assim, a palavra VERDAO criptografada passou a ser a sequência numérica: 497 - 326 - 391 - 310 - 1 - 396.

Para decifrar a mensagem é necessário que se tenha também a chave privada correspondente. Ela é definida, também, por dois números: um desses números é o próprio "*n"* e o outro é representado por um número "*d"*, inverso multiplicativo modular que vem da implicação abaixo:

$mdc(\phi(n), e) = 1 \Rightarrow 1 = d.e - r.\phi(n)$, sendo *d* o inverso modular de *e*.

Para calcular o inverso multiplicativo modular, foi feito o uso do algoritmo de Euclides. Portanto, efetuou-se a divisão euclidiana de $\phi(n)$ por *e*, dividindo, então, o

divisor pelo resto da divisão anterior, até que o resto seja numericamente igual a 1. No exemplo, pode-se verificar:

$640 : 13 = 49$, com resto 3, isolando o resto: $3 = 1.640 - 49.13$ (1)

$13 : 3 = 4$, com resto 1, isolando o resto: $1 = 1.13 - 4.3$ (2)

Substituindo (1) em (2), tem-se:

$1 = 197.13 - 4.640$, que ao ser comparado com a fórmula do inverso modular $1 = d.e - r.\phi(n)$, permite extrair o valor numérico de *n*. Então o número *d* é igual a 197.

Logo, a chave privada é determinada por *n* = 697 e *d* = 197. Então, para decodificar a mensagem, utilizou-se a fórmula $m \equiv c^d \mod(n)$. De maneira geral, a fórmula, já utilizando os valores calculados para *n* e *d*, é dada por $m \equiv c^{197} \mod(697)$; sendo *m* o valor numérico da letra na tabela inicial e *c* o valor criptografado da letra.

No exemplo que seguimos:

| **Valor de *c*** | **Fórmula** | **Valor de *m*** |
|---|---|---|
| 497 | 497^197 mod 697 | 21 |
| 326 | 326^197 mod 697 | 5 |
| 391 | 391^197 mod 697 | 17 |
| 310 | 310^197 mod 697 | 4 |
| 1 | 1^197 mod 697 | 1 |
| 396 | 396^197 mod 697 | 14 |

Assim, os valores 497 - 326 - 391 - 310 - 1 - 396, foram decodificados para o código numérico 21 - 5 - 17 - 4 - 1 – 14; e, ao buscar cada valor correspondente na tabela de conversão letra-número, foi possível determinar, novamente, a palavra VERDAO.

# 4. ATIVIDADES REALIZADAS PELOS ALUNOS

A aplicação do material foi feita em duas etapas, cada uma em um dia, e, em cada dia contendo uma aula dupla, com duração de uma hora e trinta minutos, totalizando três horas de curso nos dois dias. A primeira etapa, no primeiro dia, focou apenas na parte teórica, mostrando aos alunos o significado da criptografia, assim como, alguns métodos simples para que houvesse um entendimento geral sobre o tema proposto. Ainda nessa primeira etapa, os alunos tiveram contato com um exemplo completo sobre como criptografar e decodificar uma palavra simples.

A segunda etapa, no segundo dia, foi inteiramente prática, os alunos foram divididos em três grupos para que pudessem calcular suas próprias chaves públicas e privadas. Cada grupo criptografou uma palavra usando a chave pública do outro grupo, sendo que o grupo 1 utilizou  a chave pública do grupo 2, o grupo 2 utilizou a chave pública do grupo 3 e o grupo 3 utilizou a chave pública do grupo 1.

## 4.1. Aplicação da Teoria

Ao iniciar a aplicação da parte teórica, já foi possível perceber o interesse dos alunos. A apresentação de teorias simples, como a criptografia primitiva, já evidenciou a necessidade de interação para que os alunos começassem a se sentir mais à vontade com a aula e pudessem perceber um dos objetivos da atividade – tentar transmitir efetivamente uma mensagem com algum tipo de código.

Utilizando-se criptografias primitivas foi possível criptografar e decodificar algumas palavras para compreensão do conceito. Prontamente, alguns alunos perceberam a existência de certa dificuldade em descobrir qual o critério utilizado para posicionar as letras e então, criptografar. Mas, ao mesmo tempo, perceberam que, após algumas tentativas, seria possível descobrir como funcionavam códigos mais simples.

Como esses códigos poderiam ser quebrados, iniciou-se um questionamento sobre como fazer um código seguro, sem pensar em números, apenas especulando-se

como tal procedimento poderia ser feito e como o código poderia ser transmitido em segurança.

Com o conceito de chave simétrica, verificou-se a possibilidade de criar algo mais elaborado para que uma mensagem chegasse de maneira segura ao destinatário, uma vez que esse tinha fácil decodificação. Foi dito que os dois lados (emissor – receptor) deveriam saber a chave para poderem trocar as informações. Caso o destinatário não soubesse a chave correta, a mesma deveria ser enviada também. Logo, os alunos questionaram como fazer para que essa chave chegasse de maneira segura ao outro lado.

Com as dificuldades que a chave simétrica impunha, foi introduzido o conceito de chave assimétrica, que por sua vez, possuía uma idéia mais segura, mas ainda apresentava alguns problemas, como por exemplo, a demora para o envio e reenvio das mensagens para decodificação de cada uma das chaves. Entretanto, os alunos já pareciam mais convencidos de que o processo assimétrico era bem mais seguro, mesmo com os problemas citados.

Com a aparição da criptografia RSA e a utilização das chaves públicas e privadas, a ideia da segurança da criptografia sofreu um avanço. Nesse ponto, os alunos já estavam curiosos para ver e testar o funcionamento do método e começar a fazer alguns cálculos.

A “demonstração" da veracidade do algoritmo RSA foi feita com o uso de um exemplo; as demonstrações rigorosas foram deixadas de lado para dar um efeito mais prático à aula, visto que, um dos objetivos da aula era mostrar o algoritmo em si e não atentar aos detalhes que o cercam.

Ao final do exemplo e da parte teórica, ficou fácil notar o interesse dos alunos e eles puderam perceber que o método não era nem um pouco difícil de aplicar. Toda a complexidade se dava pela parte das demonstrações e das validades das fórmulas, mas as aplicações não davam trabalho.

## 4.2. Aplicação de Parte Prática

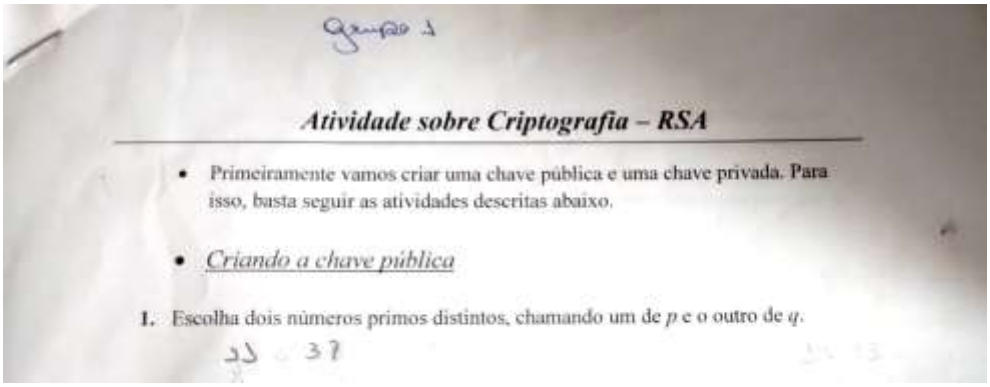
Neste momento, ao fim da teoria, era hora de colocar os alunos para trabalhar e construir os códigos. A partir de então, eles foram separados em três grupos, sendo cada grupo composto pelos alunos de um mesmo ano, sendo assim o grupo 1 foi formado pelos alunos do 9º ano do Ensino Fundamental (G1), o grupo 2 foi formado pelos alunos da 1ª série do Ensino Médio (G2) e o grupo 3 foi formado pelos alunos da 2ª série do Ensino Médio (G3).

Para maior clareza de como foi realizada a aplicação, em cada etapa serão apresentados, a seguir, os dados feitos por cada um dos três grupos.

Partindo para a aplicação da criptografia, a primeira parte era fazer com que cada grupo criasse sua própria chave pública a partir de escolhas feitas por eles mesmos:

**1.** Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.

**G1**: 11 e 37


Grupo 1

***Atividade sobre Criptografia – RSA***

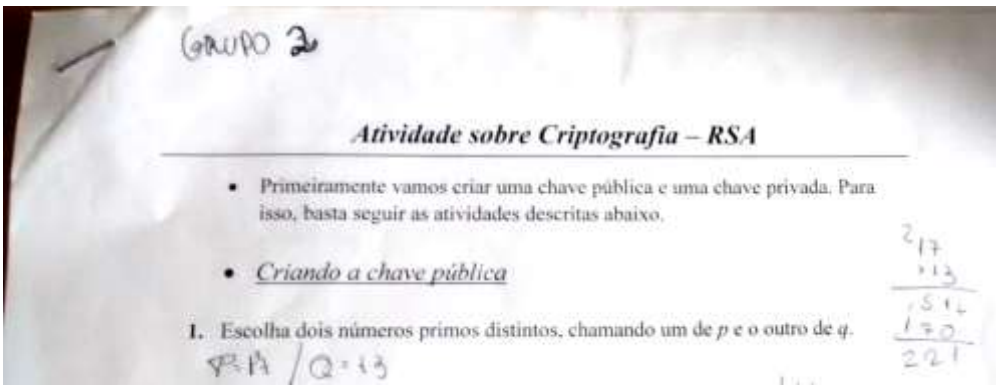
- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.
- *Criando a chave pública*

1. Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.

11 . 37

*Figura 5 – Fragmento 1, grupo 1*

**G2**: 17 e 13


GRUPO 2

***Atividade sobre Criptografia – RSA***

- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.
- *Criando a chave pública*

1. Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.

P=17 / Q=13

17 × 13 = 51 + 170 = 221

*Figura 6 – Fragmento 1, grupo 2*

**G3**: 23 e 13

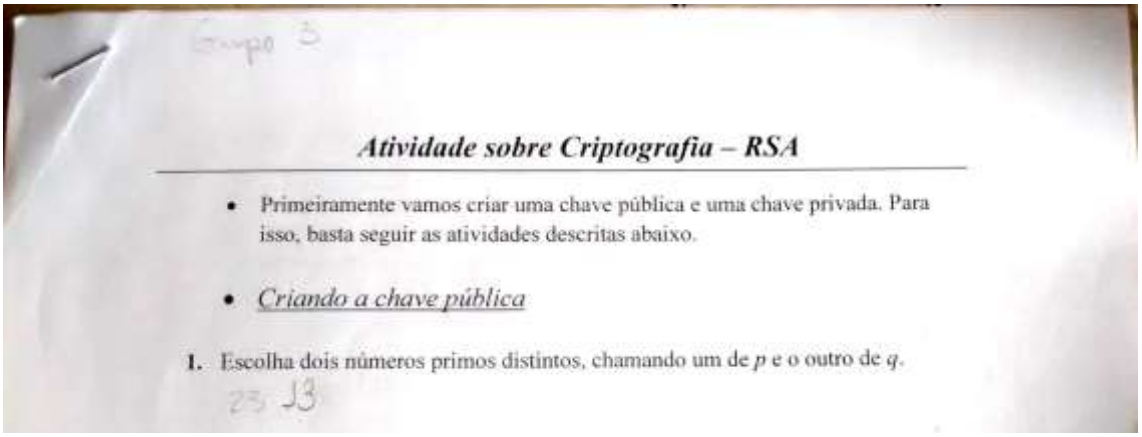



*Figura 7 – Fragmento 1, grupo 3*

**2.** Calcule o valor de $n$, $n = p.q$.

**G1**: $n = 11.37 = 407$


*Figura 8 – Fragmento 2, grupo 1*

**G2**: $n = 17.13 = 221$


*Figura 9 – Fragmento 2, grupo 2*

**G3**: $n = 23.13 = 299$

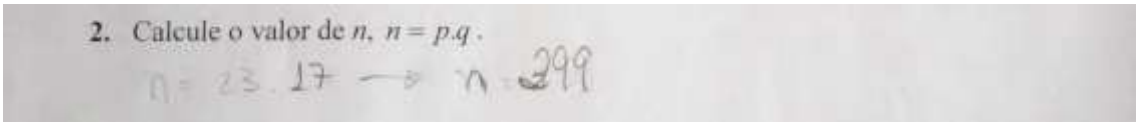



*Figura 10 – Fragmento 2, grupo 3*

**3.** Encontre o valor de $\phi(n) = (p-1).(q-1)$.

**G1**: $(11-1).(37-1) = 10.36 = 360$

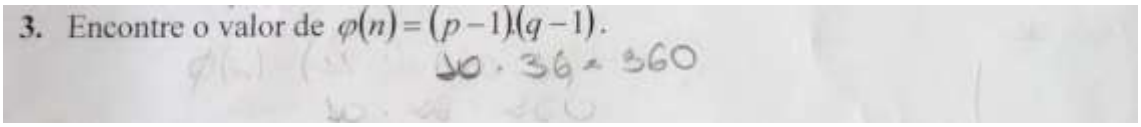



*Figura 11 – Fragmento 3, grupo 1*

**G2**: $(17-1).(13-1)=16.12=192$

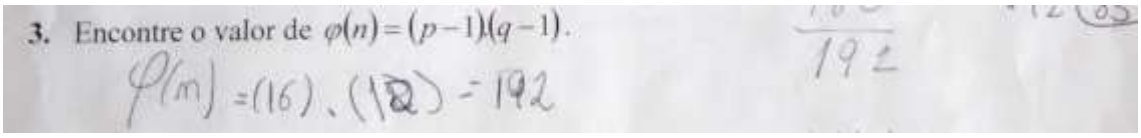



*Figura 12 – Fragmento 3, grupo 2*

**G3**: $(23-1).(13-1)=22.12=264$

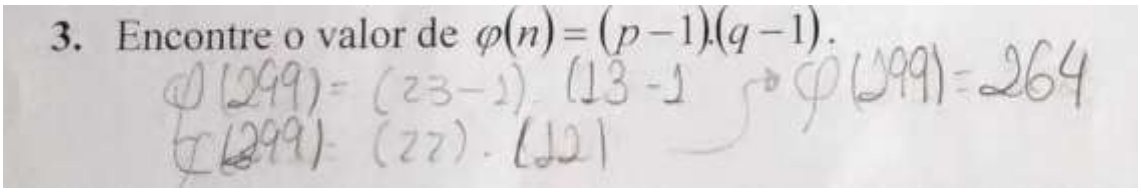



*Figura 13 – Fragmento 3, grupo 3*

**4.** Escolha um número *e* primo entre si com $\phi(n)$, ou seja, $mdc(\phi(n),e)=1$.

**G1**: $e=7$

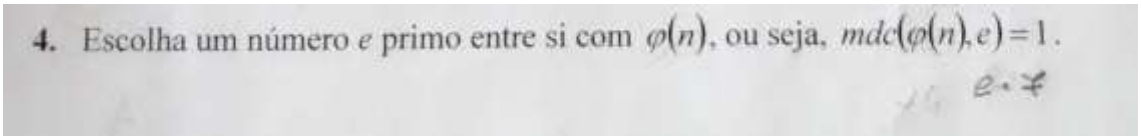



*Figura 14 – Fragmento 4, grupo 1*

**G2**: $e=5$

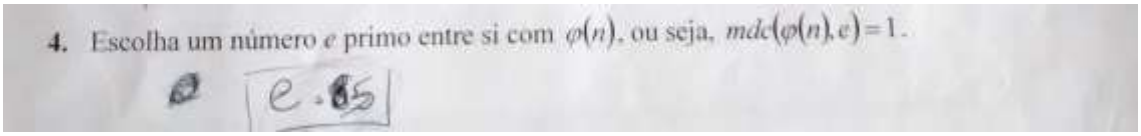



*Figura 15 – Fragmento 4, grupo 2*

**G3**: $e = 5$

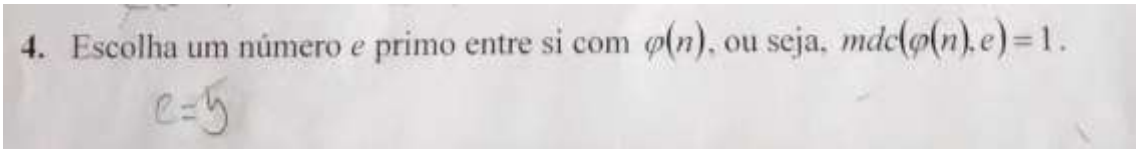



*Figura 16 – Fragmento 4, grupo 3*

Em seguida, cada grupo divulgou suas chaves públicas na lousa, no espaço reservado, para que, posteriormente os outros alunos pudessem utilizá-las para codificar a mensagem e enviar de volta para cada grupo.

Após as chaves públicas calculadas, era hora de os alunos calcularem as chaves privadas, as quais seriam utilizadas para decifrar a mensagem enviada pelo outro grupo.

**1.** Faça a divisão de $\phi(n)$ por $e$, depois divida o (~~quociente~~) divisor da divisão pelo (~~divisor~~) resto, sucessivamente até que o resto da divisão seja 1.

**G1**: Na divisão de 360 ($\phi(n)$) por 7 ($e$) a equação encontrada foi $3 = 1.360 - 51.7$

Na divisão de 7 (divisor) por 3 (resto) a equação encontrada foi $1 = 1.7 - 2.3$

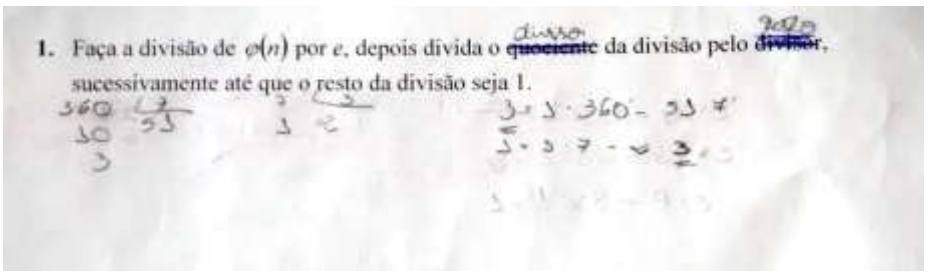



*Figura 17 – Fragmento 5, grupo 1*

**G2**: Na divisão de 192 ($\phi(n)$) por 5 ($e$) a equação encontrada foi $2 = 1.192 - 38.5$

Na divisão de 5 (divisor) por 2 (resto) a equação encontrada foi $1 = 1.5 - 2.2$

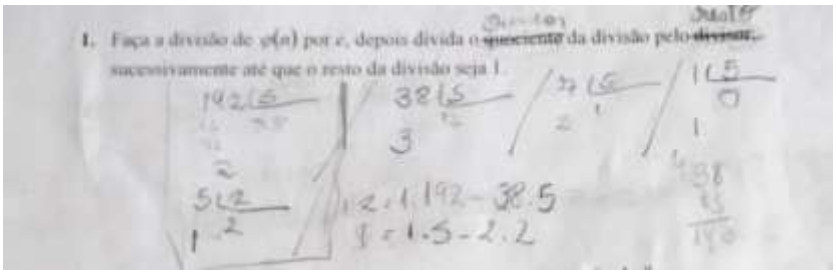


*Figura 18 – Fragmento 5, grupo 2*

**G3**: Na divisão de 264 ($\phi(n)$) por 5 ($e$) a equação encontrada foi $4 = 1.264 - 52.5$

Na divisão de 5 (divisor) por 4 (resto) a equação encontrada foi $1 = 1.5 - 1.4$

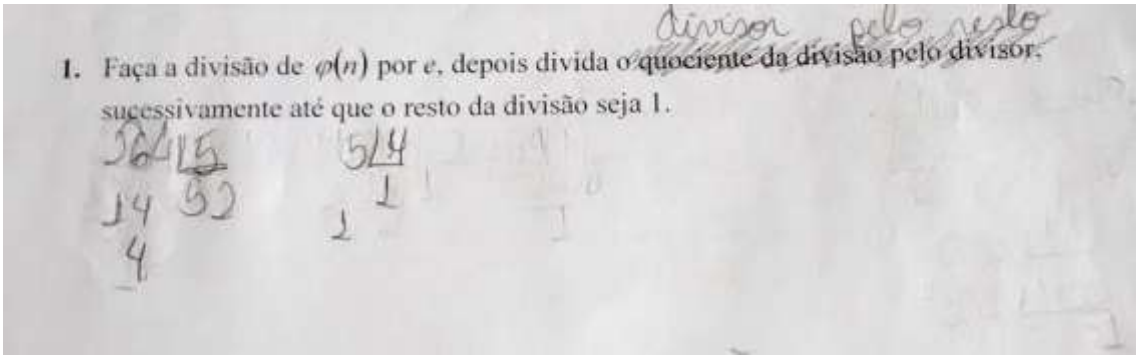


*Figura 19 – Fragmento 5, grupo 3*

**2.** Isole os restos das divisões euclidianas para ter uma equação da forma $1 = d.e - r.\phi(n)$, e extraia o valor de $d$.

**G1**: $1 = 1.7 - 2.3 = 1.7 - 2.(1.360 - 51.7) = 103.7 - 2.360 \Rightarrow d = 103$

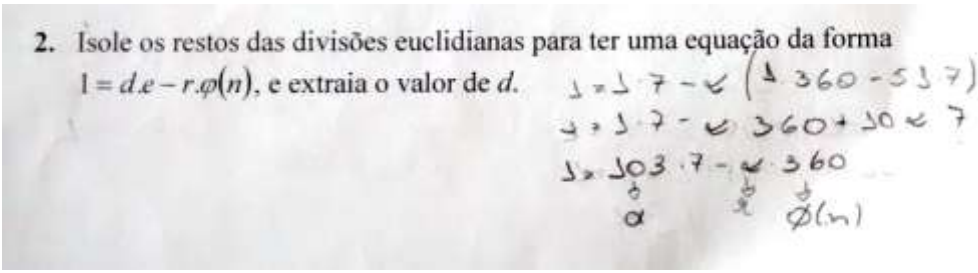


*Figura 20 – Fragmento 6, grupo 1*

**G2**: $1 = 1.5 - 2.2 = 1.5 - 2.(1.192 - 38.5) = 77.5 - 2.192 \Rightarrow d = 77$

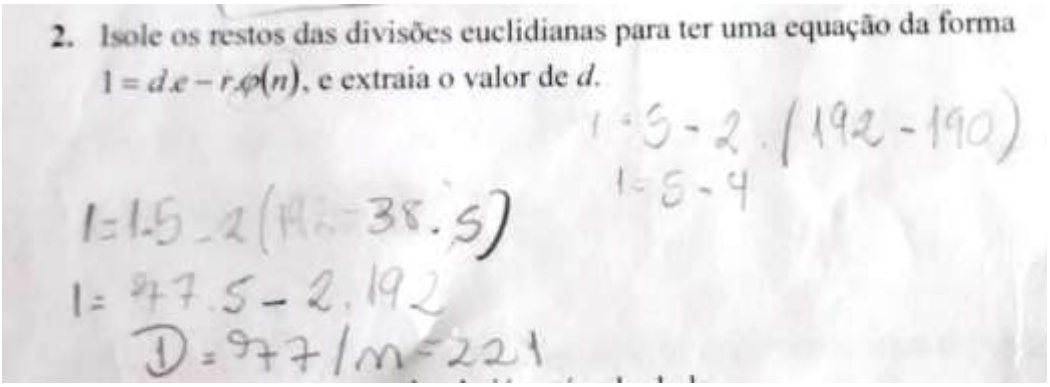



*Figura 21 – Fragmento 6, grupo 2*

**G3**: $1 = 1.5 - 1.4 = 1.5 - 1.(1.264 - 52.5) = 53.5 - 1.264 \Rightarrow d = 53$

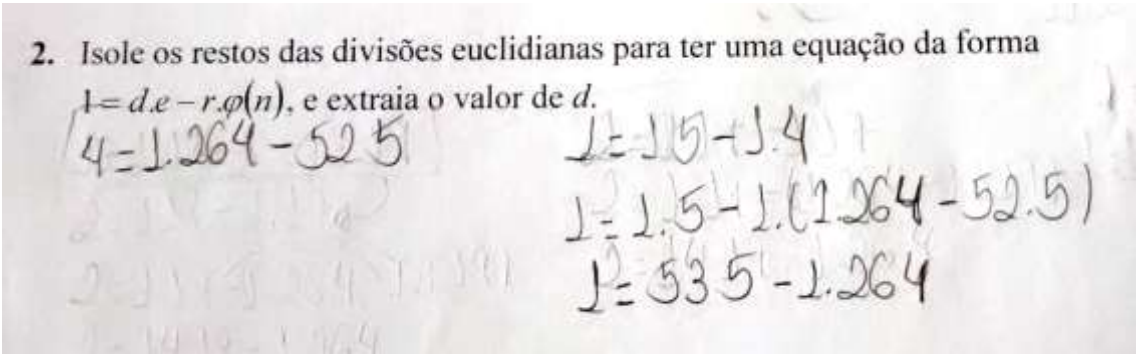



*Figura 22 – Fragmento 6, grupo 3*

Nessas duas últimas passagens, os alunos tiveram um pouco mais de dificuldade, recebendo um auxílio maior na execução das divisões, já que esse tipo de divisão euclidiana, com o resto sendo isolado para substituir em outra equação não é de costume dos alunos. Apesar de os alunos da segunda série do ensino médio já terem mais contato com as divisões polinomiais; semelhantes à escrita acima utilizada, os alunos do 9º ano do ensino fundamental e 1ª série do ensino médio não estavam habituados a isolar os restos para deixar a equação no formato necessário. Contudo, mesmo com as dificuldades, os alunos executaram essa parte da atividade de maneira razoável e puderam criar suas chaves privadas para utilizar na decodificação das palavras.

Com as chaves públicas e privadas na mão, os alunos passaram para a última parte da atividade, que consistia em escolher uma palavra de seis letras para codificar, usando as chaves públicas calculadas pelo grupo seguinte.

Sendo assim, o grupo 1 utilizou as chaves públicas do grupo 2 ($n = 221; e = 5$), o grupo 2 utilizou as chaves públicas do grupo 3 ($n = 299; e = 5$) e o grupo 3 utilizou as chaves públicas do grupo 1 ($n = 407; e = 7$) para criptografar a palavra criada e enviar de volta, para que o grupo decodificasse utilizando sua própria chave privada.

O grupo 1 criptografou a palavra ZEUGMA, que foi trocada pelos valores da tabela inicial ficando 23 – 5 – 20 – 7 – 12 – 1, utilizando as chaves públicas do grupo 2 ($n = 221; e = 5$), tendo a fórmula padrão: $c = m^5 \bmod 221$, como base para a montagem da tabela, utilizando a calculadora do computador.

| | | |
|---|---|---|
| Z | $23^5 \bmod 221$ | 160 |
| E | $5^5 \bmod 221$ | 31 |
| U | $20^5 \bmod 221$ | ~~14~~ 141 |
| G | $7^5 \bmod 221$ | 11 |
| M | $12^5 \bmod 221$ | 207 |
| A | $1^5 \bmod 221$ | 1 |

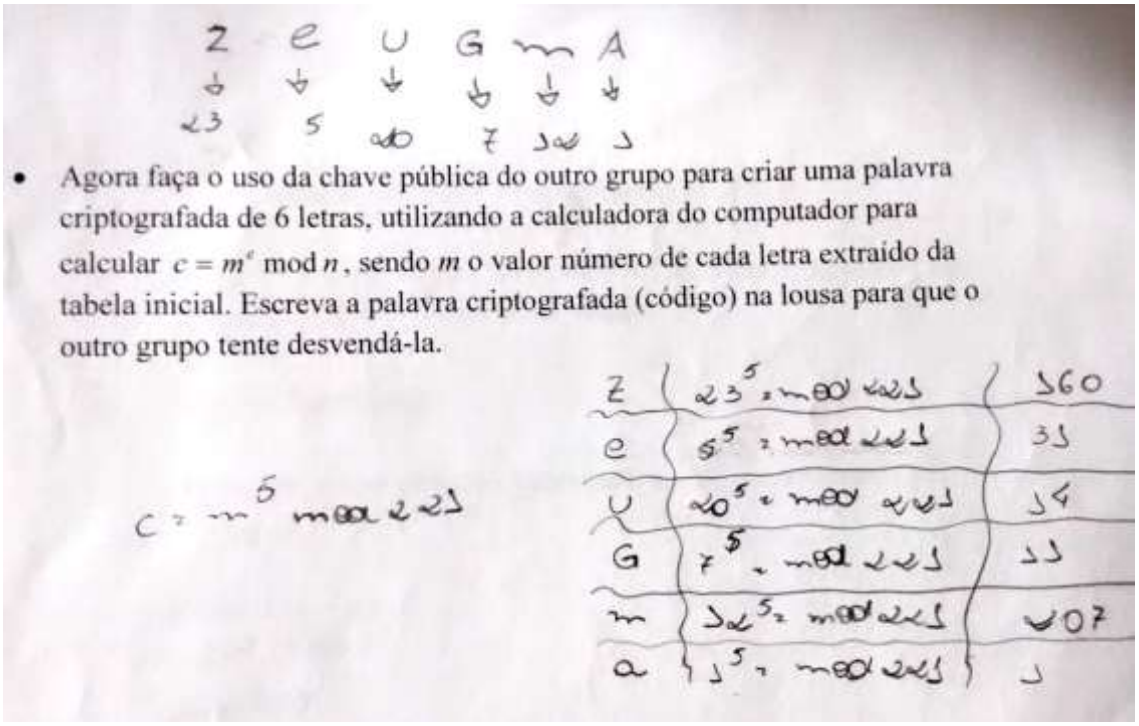



*Figura 23 – Fragmento 7, grupo 1*

O grupo 1 cometeu um erro na linha da letra U, a qual teria como resultado criptografado o valor 141. O erro de cálculo levou-os ao valor 14, mas esse fato não alterou o resultado da aplicação, já que as outras letras foram criptografadas de maneira correta e foi possível deduzir a palavra correta no final.

Então o grupo 1 entregou o código 160 – 31 – ~~14~~141 – 11 – 207 – 1 para que o grupo 2 decodificasse utilizando suas chaves privadas ($n = 221; d = 77$), tendo a fórmula padrão: $m = c^{77} \bmod 221$, como base para a montagem da tabela.

| | | |
|---|---|---|
| $160^{77} \bmod 221$ | 23 | Z |
| $31^{77} \bmod 221$ | 5 | E |
| ~~$14^{77}$~~ $141^{77} \bmod 221$ | ~~209~~20 | U |
| $11^{77} \bmod 221$ | 7 | G |
| $207^{77} \bmod 221$ | 12 | M |
| $1^{77} \bmod 221$ | 1 | A |

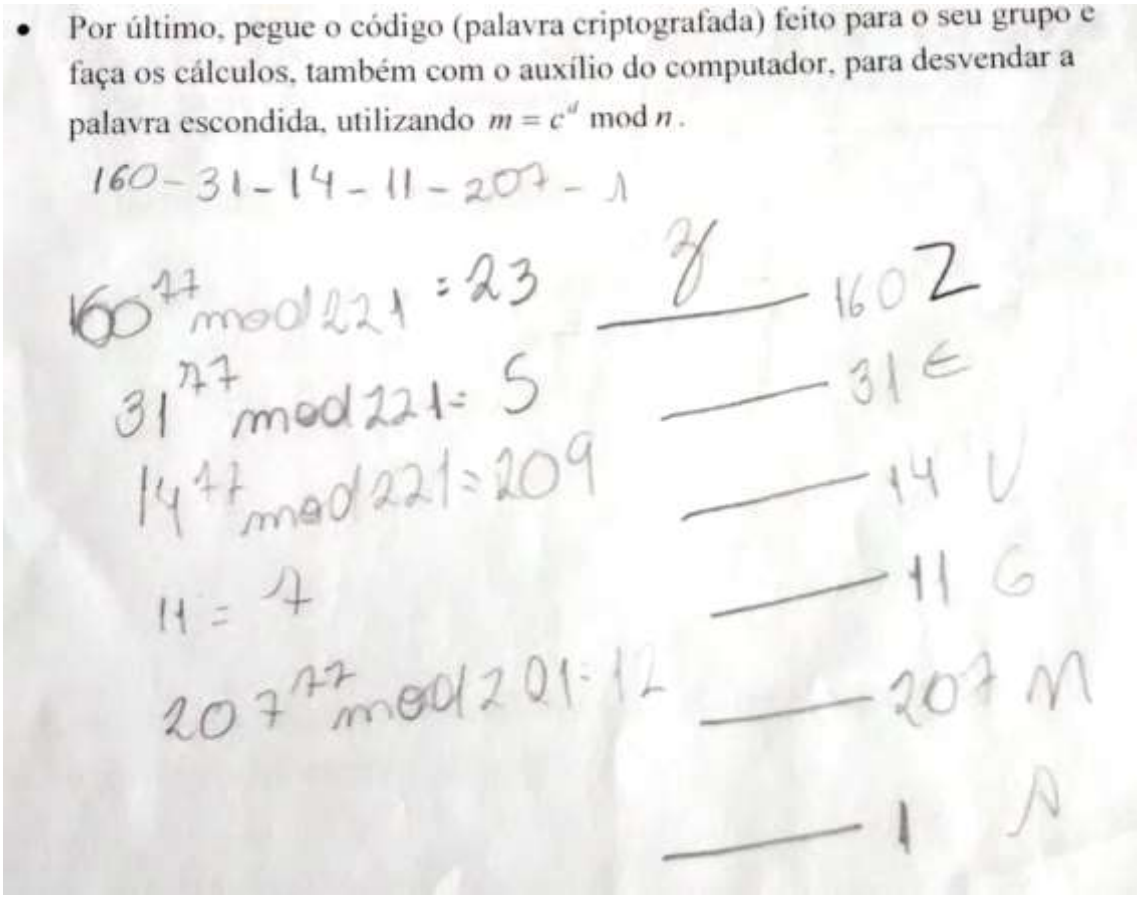



*Figura 24 – Fragmento 7, grupo 2*

O grupo 2 criptografou a palavra ROBSON que foi trocada pelos valores da tabela inicial ficando 17 – 14 – 2 – 18 – 14 – 13 , utilizando as chaves públicas do grupo 3 ($n = 299; e = 5$), tendo a fórmula padrão: $c = m^5 \bmod 299$, como base para a montagem da tabela, utilizando a calculadora do computador.

| | | |
|---|---|---|
| R | $17^5 \bmod 299$ | 205 |
| O | $14^5 \bmod 299$ | 222 |
| B | $2^5 \bmod 299$ | 32 |
| S | $18^5 \bmod 299$ | 187 |
| O | $14^5 \bmod 299$ | 222 |
| N | $13^5 \bmod 299$ | 234 |

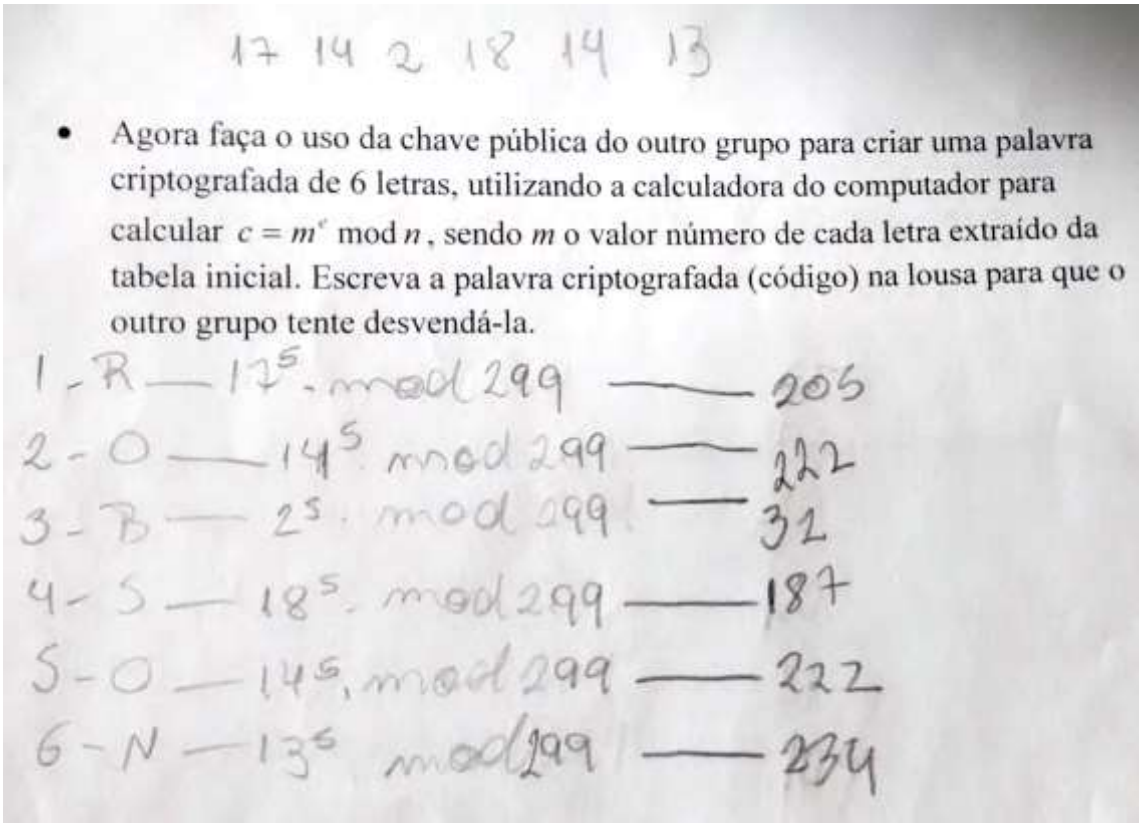



*Figura 25 – Fragmento 7, grupo 3*

Então o grupo 2 entregou o código 205 – 222 – 32 – 187 – 222 – 234 para que o grupo 3 decodificasse utilizando suas chaves privadas ($n = 299; d = 53$), tendo a fórmula padrão: $m = c^{53} \bmod 299$, como base para a montagem da tabela.

| | | |
|---|---|---|
| $205^{53} \bmod 299$ | 17 | R |
| $222^{53} \bmod 299$ | 14 | O |
| $32^{53} \bmod 299$ | 2 | B |
| $187^{53} \bmod 299$ | 18 | S |
| $222^{53} \bmod 299$ | 14 | O |
| $234^{53} \bmod 299$ | 13 | N |

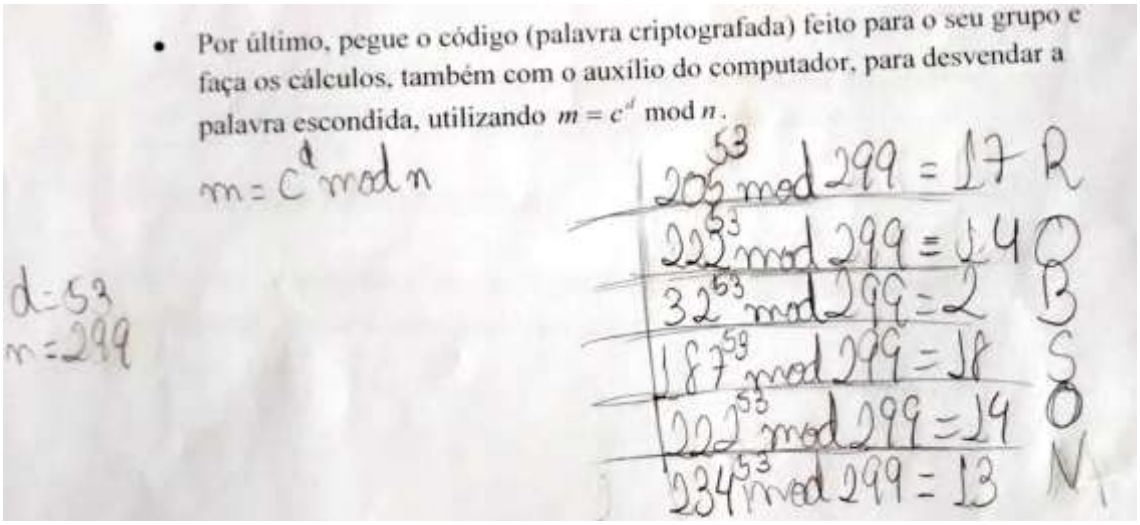



*Figura 26 – Fragmento 8, grupo 1*

O grupo 3 criptografou a palavra MONGOL que foi trocada pelos valores da tabela inicial ficando 12 – 14 – 13 – 7 – 14 – 11 , utilizando as chaves públicas do grupo 1 $(n = 407; e = 7)$, tendo a fórmula padrão: $c = m^7 \bmod 407$, como base para a montagem da tabela, utilizando a calculadora do computador.

| | | |
|---|---|---|
| M | $12^7 \bmod 407$ | 342 |
| O | $14^7 \bmod 407$ | 97 |
| N | $13^7 \bmod 407$ | 106 |
| G | $7^7 \bmod 407$ | 182 |
| O | $14^7 \bmod 407$ | 97 |
| L | $11^7 \bmod 407$ | 11 |

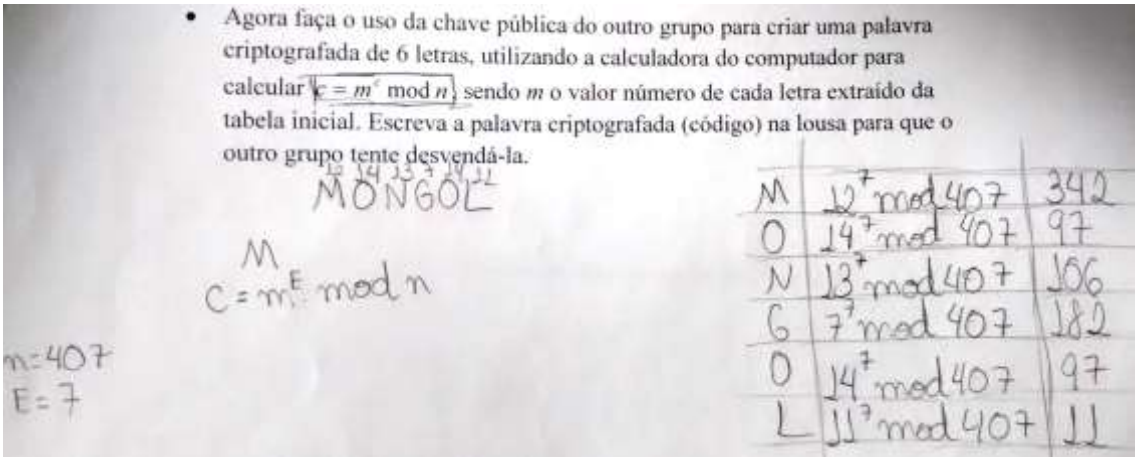



*Figura 27 – Fragmento 8, grupo 2*

Então o grupo 3 entregou o código 342 – 97 – 106 – 182 – 97 – 11 para que o grupo 3 decodificasse utilizando suas chaves privadas ($n = 407; d = 103$), tendo a fórmula padrão: $m = c^{53} \bmod 299$, como base para a montagem da tabela.

| | | |
|---|---|---|
| $342^{103} \bmod 407$ | 12 | M |
| $97^{103} \bmod 407$ | 14 | O |
| $106^{103} \bmod 407$ | 13 | N |
| $182^{103} \bmod 407$ | 7 | G |
| $97^{103} \bmod 407$ | 14 | O |
| $11^{103} \bmod 407$ | 11 | L |

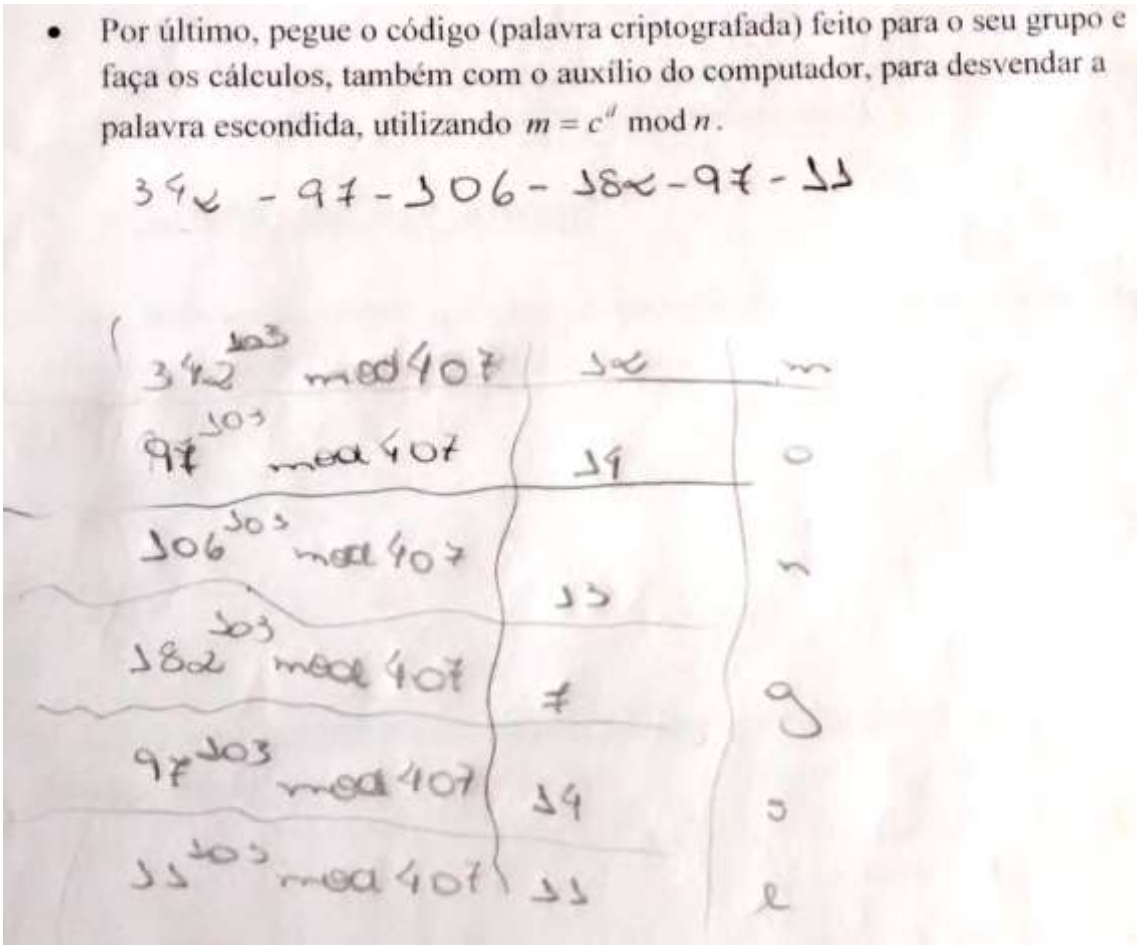



*Figura 28 – Fragmento 8, grupo 3*

E assim a atividade foi concluída com sucesso pelos alunos, que ainda baixaram emuladores de calculadoras científicas nos celulares. Dessa maneira, todos puderam fazer as contas, incluindo as contas envolvendo a congruência módulo *n*.

Nas fotos anexadas, é possível acompanhar todo o desenvolvimento dos alunos; desde o começo até a colocação dos valores calculados na lousa. Uma das fotos ainda consta um valor colocado de forma incorreta, já que os alunos do grupo 3 colocaram o valor de $\phi(n)$ ao invés do valor de *n*, o que foi notado e depois corrigido, não prejudicando os cálculos feitos pelo outro grupo.

# 5. CONCLUSÕES

Por meio dessa dissertação, pode-se perceber o quanto a adequação de algumas teorias, até certo ponto complexas, pode deixar o estudo bem mais agradável e prático. Sendo possível mostrar aos alunos um pouco da praticidade da matemática, sem que os professores fiquem presos aos livros didáticos, que, em sua maioria, são repetitivos e cansativos; com poucas atividades práticas, deixando os alunos desinteressados e cada vez mais distantes do mundo dos números.

Essa dissertação não possui o intuito de criticar materiais didáticos tradicionais, e sim, acrescentar algo de valor, sabendo-se que não é possível desvincular a teoria da prática.

A teoria dos números é uma das mais belas áreas de estudo da Matemática; sempre preocupada em encontrar padrões e possibilitar um entendimento cada vez mais amplo no que diz respeito ao comportamento dos números. Esse comportamento dos números é o que mais assusta os alunos, deixando uma falsa ideia de que a matemática é somente retratada através de fórmulas e conceitos complicados.

Com uma pequena e, até certo ponto, simples atividade, como a descrita nesta dissertação, torna-se possível não só revisar e ensinar determinados conceitos, como também deixar claro para o aluno que a matemática aprendida nas escolas é utilizada no mundo que os cerca, e eles não se dão conta disso.

Com elementos poderosos, do ponto de vista matemático, a criptografia tornou-se uma ferramenta cada vez mais presente e cada vez mais desenvolvida, ainda mais com a socialização da *internet*, e a utilização de ferramentas informatizadas por praticamente toda a população.

A atividade foi proposta para os alunos do 9º ano do ensino fundamental à 2ª série do ensino médio, podendo ser notado que as três turmas terminaram as atividades basicamente ao mesmo tempo. Verifica-se que essa atividade pode ser aplicada até mesmo para alunos do 8º ano do ensino fundamental, já que os conceitos de fatoração em números primos, o conceito base da divisão euclidiana e resolução de equações utilizando o método de substituição já são ensinados nessa idade. Além disso, pode ser percebida uma maior organização na maneira de escrever dos alunos mais velhos; os

que formaram o grupo três, por conta da maturidade matemática já adquirida. Contudo, mesmo os mais novos conseguiram executar as atividades de maneira satisfatória, concluindo-as juntamente com os demais.

A priori, esta dissertação objetivava apenas a noção da força que a matemática pode apresentar em situações reais no mundo que cerca os alunos. Esse objetivo foi atingido, visto que os alunos puderam perceber onde a teoria de criptografia RSA está presente e, efetivamente, construir os códigos a partir do algoritmo criado para a execução da criptografia.

A motivação dos alunos quando souberam do que se tratava a atividade e que seriam capazes de criptografar ou codificar uma mensagem é algo que merece atenção especial. O fato de que os alunos disponibilizaram tempo e disposição para algo que não acrescentaria nota e que foi feito fora do horário regular de aula, realizado nas tardes de duas sextas-feiras, serve para reforçar ainda mais o interesse em atividades extracurriculares.

Sendo assim, pode-se responder à pergunta: É possível que os alunos jovens sejam capazes de aprender como a Matemática pode ser usada para fabricar um sistema seguro e atual de troca de mensagens secretas? A resposta afirmativa é justificada por cada passagem dessa dissertação, visto que os alunos submetidos às atividades a concluíram com sucesso e ainda saíram extremamente satisfeitos em saber uma aplicação nova da Matemática.

Pode-se concluir ainda, que alguns fundamentos da Matemática são utilizados sem que se tenha uma noção exata da utilidade. A teoria dos números, juntamente com o pequeno teorema de Fermat e a utilização dos números primos não foi estudada, no início, para que se pudessem criptografar mensagens. Entretanto, como a teoria havia sido bem desenvolvida pode-se tornar uma ferramenta de extrema valia no que diz respeito à arte de criar mensagens secretas. Criptografia, esta, tão utilizada nos tempos modernos em que vivemos.

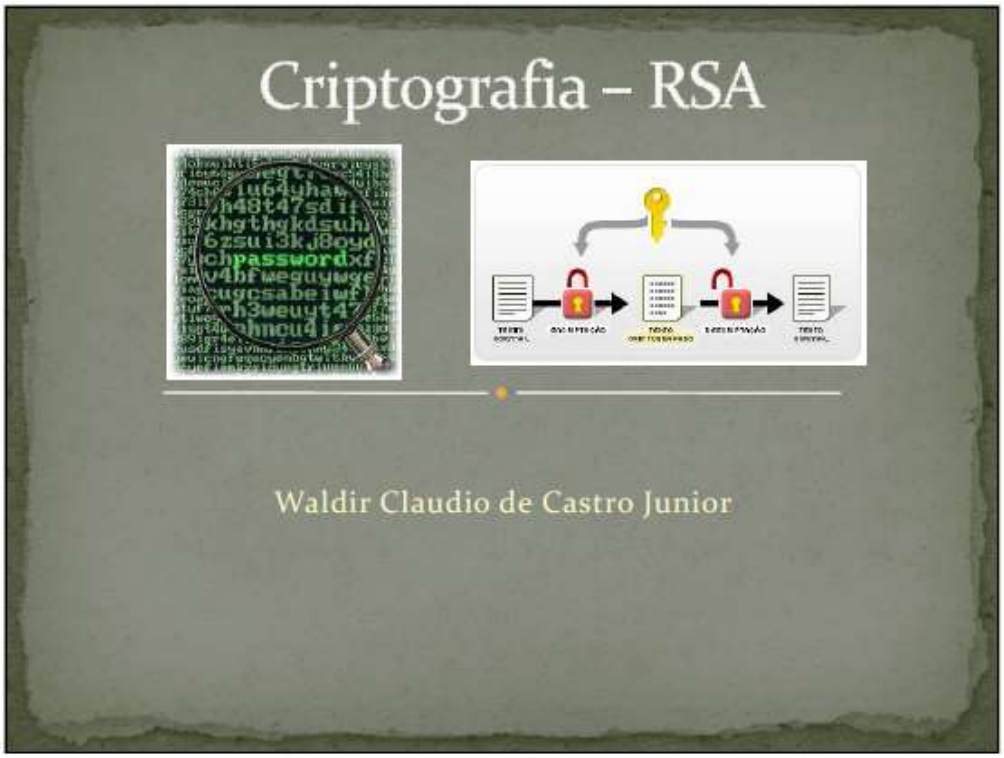
Vale ressaltar ainda, que esta atividade foi aplicada para alunos de graduação em Licenciatura em Matemática, matriculados em uma faculdade particular do interior do estado de São Paulo. Esses alunos cursavam o segundo ano e tiveram a oportunidade de assistir ao mini curso sobre criptografia RSA em uma semana de palestras e mini cursos

oferecido anualmente pela coordenação do curso em questão, juntamente com a coordenação do curso de Pedagogia e do curso de Letras. Assim como os alunos do ensino fundamental e médio, os alunos da graduação também gostaram bastante da experiência. Muitos deles tiveram contato com uma aplicação da matemática pela primeira vez, o que fez com que gostassem ainda mais do curso em que estavam.

Enfim, esta é apenas uma das atividades que pode ser desenvolvida com os alunos eventualmente, utilizando a desenvoltura dos mesmos em prol de algo mais criativo, desenvolvendo ainda mais o raciocínio lógico e a capacidade dedutiva para solucionar problemas. Tais atividades são de suma importância, pois além de acrescentar prática às aulas, elas despertam um interesse maior para a matemática e proporcionam uma maior autonomia aos alunos durante a execução dos exercícios.

# 6. ANEXOS

## 6.1. Slides Apresentados na Aula Teórica




# Criptografia Primitiva

- Atbash Hebraico

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ |
| z | y | x | w | v | u | t | s | r | q | p | o | n |

- Exemplo:
  - Decodificar que eh dificil.
  - Wvlwruxzi jfv vs wrurxro.

# História

- Acredita-se que a criptografia sempre foi utilizada para enviar mensagens secretas.
- Um método seguro para criptografar as mensagens era desconhecido.
- Em 1977, três cientistas do MIT: Ronald Rives, Adi Shamir e Leonard Adleman patentearam a criptografia RSA.




# História

- Na teoria, o conceito da criptografia de chave simétrica, era simples:
  - Eu quero enviar uma mensagem secreta para o alguém.
  - Eu uso uma chave para criptografar essa mensagem.
  - Envio a mensagem para essa pessoa.
  - Ela recebe a mensagem criptografada.
  - Ela faz uso da chave correta e deixa a mensagem legível.


# História

- Problemas:
  - As duas pessoas devem conhecer a chave.
  - Como assegurar o recebimento da chave.
  - Não deixar que a chave chegue a mais pessoas.

# História

- Criou-se então uma criptografia de chave assimétrica:
  - Eu criptografo a mensagem, com uma chave 1 e mando para alguém.
  - Essa pessoa recebe a mensagem e criptografa, com uma chave 2 e manda de volta.
  - Eu recebo e descriptografo usando a minha chave (1) e envio novamente.
  - A pessoa recebe e descriptografa usando a chave dela(2).


# História

- Problemas:
  - Quantidade de viagens.
  - Tempo.

## História

- Pensaram então em criar um código, onde uma das "chaves" pudesse ser conhecida por todos que quisessem enviar uma mensagem a uma determinada pessoa.
- E somente a pessoa que recebesse a mensagem conseguiria decodificar a mensagem recebida, fazendo uso de sua "chave".

## Funcionamento

- Possui duas chaves: uma pública e uma privada.
- Todos podem enviar uma mensagem criptografada com a chave pública.
- Apenas quem possui a chave privada poderá descriptografar a mensagem.
- Assim:
  - Para enviar uma mensagem criptografada a uma pessoa, basta utilizar a criptografia pública divulgada por ela.

## Funcionamento

- A RSA é baseada na teoria dos números:
  - Fatoração de um número em fatores primos.
- Números "pequenos" são facilmente fatorados e sua fatoração é única (Teorema Fundamental da Aritmética)
- Números "grandes" são trabalhosos e demorados para fatorar, não possuindo fórmula para isso.

## Criptografando...

- Utilizamos uma tabela para numerar as letras do alfabeto:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | L | M | N | O | P | Q | R | S | T | U | V | X | Z |

- Escolhemos dois números primos quaisquer:
  - Por exemplo: 17 e 41.
- Segundo a RSA, recomenda-se utilização de chaves públicas de pelo menos 617 dígitos, ou seja, quanto maior melhor.

## Criptografando...

- Multiplicando os números primos selecionados obtemos o número *n*.
  - Por exemplo: $n = 17 * 41 = 697$
- Utilizamos a função Totiente (criada por Euler), para ver a quantidade de números primos entre si com *n*, que são menores do que ele mesmo.
  - $\Phi(n) = (p - 1)*(q - 1)$, *formados por dois fatores primos.*
- Calculando a função Totiente de *n*, temos:
  - $\Phi(697) = (17 - 1)*(41 - 1) = 640$

## Criptografando...

- Para calcular a chave pública devemos escolher um número "*e*" em que $1<e<\Phi(n)$, sendo "*e*" e $\Phi(n)$ primos entre si.
- Podemos escolher qualquer número "*e*".
  - Por exemplo:
    - mdc(640,3) = 1
    - mdc(640,13) = 1
    - mdc(640,23) = 1
- Escolhendo o 13 temos a nossa chave pública representada pelos números 697 e 13.

# Criptografando...

- Fazendo uso de congruência módulo *n*, podemos aplicar a seguinte fórmula:

$$c = m^e \bmod n$$

  - *e* – chave pública
  - *m* – valor numérico da letra
- Para o nosso exemplo, teríamos:

$$c = m^{13} \bmod 697$$

# Criptografando...

- Vamos criptografar a palavra VERDAO:

| Letra | Fórmula | Valor de c |
|---|---|---|
| V | 21^13 mod 697 | 497 |
| E | 5^13 mod 697 | 326 |
| R | 17^13 mod 697 | 391 |
| D | 4^13 mod 697 | 310 |
| A | 1^13 mod 697 | 1 |
| O | 14^13 mod 697 | 396 |

- Assim criptografamos a palavra VERDAO e obtemos o código:
  - 497 326 391 310 1 396

## Decifrando...

- Para decifrar uma mensagem precisamos saber sua chave privada.
- Para isso precisamos utilizar o conceito de inverso multiplicativo modular:

$$mdc(\phi(n), n) = 1 \Rightarrow 1 = d.e - (r.\phi(n))$$

  - d – inverso modular de *e*
- Para calcular o inverso multiplicativo modular fazemos uso do algoritmo de Euclides estendido.

## Decifrando...

- No exemplo tínhamos a chave pública 13 e $\Phi(n)$=640.
- Efetuando a divisão euclidiana de $\Phi(n)$ *por e*, obtemos:
  - 3 = 1*640 – 49*13 (1)
- Dividimos o divisor anterior pelo resto, obtendo:
  - 1 = 1*13 – 4*3 (2)
- Substituindo (1) em (2), chegamos em:
  - 1 = 197*13 – 4*640
    - d = 197
    - r = 4

# Decifrando...

- A chave privada é determinada então por *n* e por *d:*

$$m = c^d \bmod n$$

- Para o nosso exemplo, teríamos:

$$m = c^{197} \bmod 697$$

# Decifrando...

- Relembrando, nosso código criptografado era:
  - 497 326 391 310 1 396

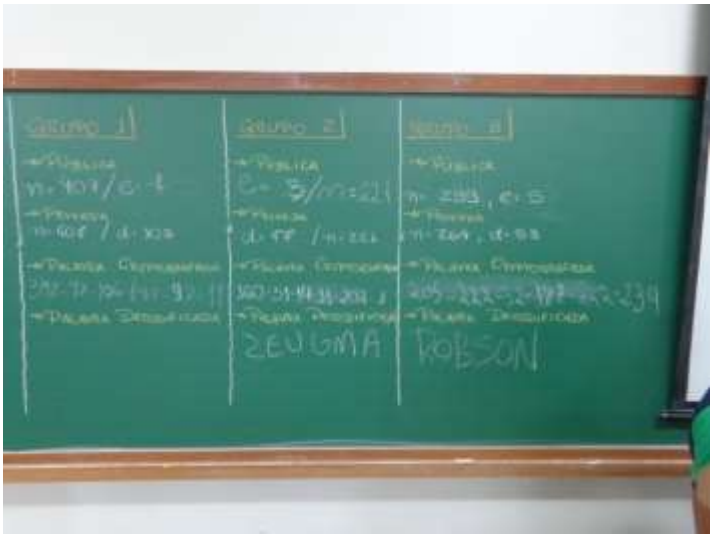
| Valor de *c* | Fórmula | Valor de *m* |
|---|---|---|
| 497 | 497^197 mod 697 | 21 |
| 326 | 326^197 mod 697 | 5 |
| 391 | 391^197 mod 697 | 17 |
| 310 | 310^197 mod 697 | 4 |
| 1 | 1^197 mod 697 | 1 |
| 396 | 396^197 mod 697 | 14 |

- Voltando os valores na tabela inicial, obtemos:
  - VERDAO

# Bibliografia


- Mathematics and Technology, Christiane Rousseau e Yvan Saint-Aubin, 2008
- Antonio Cândido Faleiros, Criptografia (Sociedade Brasileira de Matemática Aplicada e Computacional)
- blog.lambda3.com.br
- www.gta.ufrj.br

## 6.2. Fotos da Lousa

## 6.3. Folhas com Atividades dos Alunos

***Folha original corrigida***

# *Atividade sobre Criptografia – RSA*

---

- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.

- *Criando a chave pública*

**1.** Escolha dois números primos distintos, chamando um de *p* e o outro de *q*.

**2.** Calcule o valor de *n*, $n = p.q$.

**3.** Encontre o valor de $\varphi(n) = (p-1).(q-1)$.

**4.** Escolha um número *e* primo entre si com $\varphi(n)$, ou seja, $mdc(\varphi(n), e) = 1$.

- Pronto sua chave pública já está criada, divulgue-a na lousa para que o outro grupo possa enviar uma mensagem criptografada para vocês.

- Calculando sua chave privada

**1.** Faça a divisão de $\varphi(n)$ por *e*, depois divida o divisor da divisão anterior pelo resto, sucessivamente até que o resto da divisão seja 1.

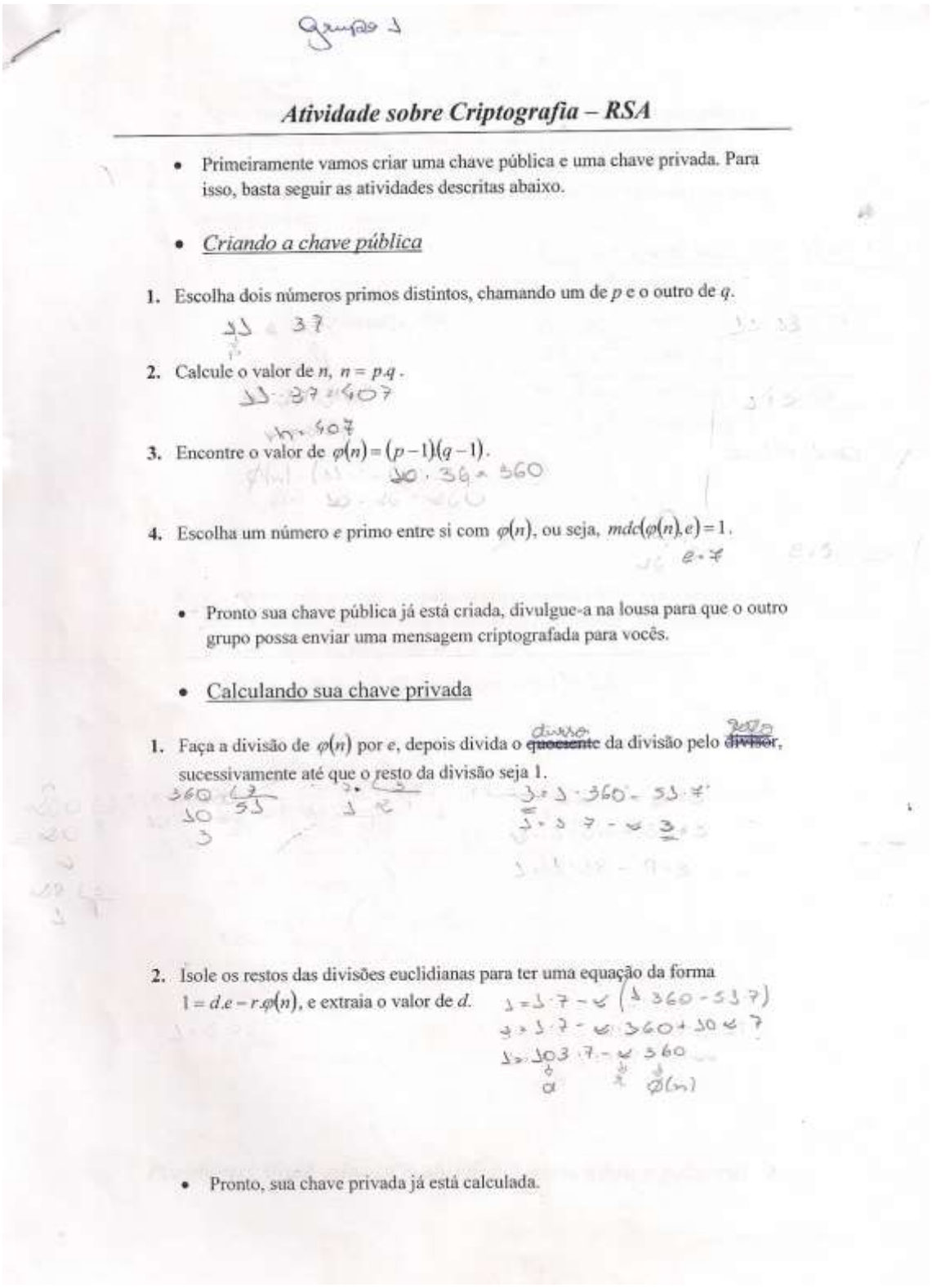
**2.** Isole os restos das divisões euclidianas para ter uma equação da forma $1 = d.e - r.\varphi(n)$, e extraia o valor de *d*.

- Pronto, sua chave privada já está calculada.
- Agora faça o uso da chave pública do outro grupo para criar uma palavra criptografada de 6 letras, utilizando a calculadora do computador para calcular $c = m^e \bmod n$, sendo $m$ o valor número de cada letra extraído da tabela inicial. Escreva a palavra criptografada (código) na lousa para que o outro grupo tente desvendá-la.

- Por último, pegue o código (palavra criptografada) feito para o seu grupo e faça os cálculos, também com o auxílio do computador, para desvendar a palavra escondida, utilizando $m = c^d \bmod n$.

***Parabéns! Você atingiu o objetivo e desvendou a palavra!***

Grupo 1



Grupo 1

## *Atividade sobre Criptografia – RSA*

- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.

- *Criando a chave pública*

1. Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.

2. Calcule o valor de $n$, $n = p.q$.

3. Encontre o valor de $\varphi(n) = (p-1)(q-1)$.

4. Escolha um número $e$ primo entre si com $\varphi(n)$, ou seja, $mdc(\varphi(n), e) = 1$.

- Pronto sua chave pública já está criada, divulgue-a na lousa para que o outro grupo possa enviar uma mensagem criptografada para vocês.

- Calculando sua chave privada

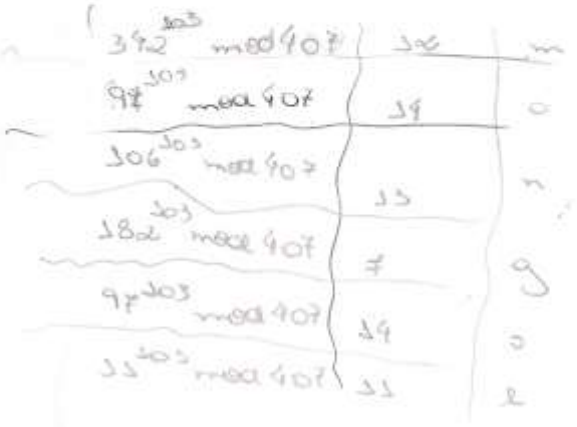
1. Faça a divisão de $\varphi(n)$ por $e$, depois divida o ~~quociente~~ divisor da divisão pelo ~~divisor~~ resto, sucessivamente até que o resto da divisão seja 1.

2. Isole os restos das divisões euclidianas para ter uma equação da forma $1 = d.e - r.\varphi(n)$, e extraia o valor de $d$.

- Pronto, sua chave privada já está calculada.

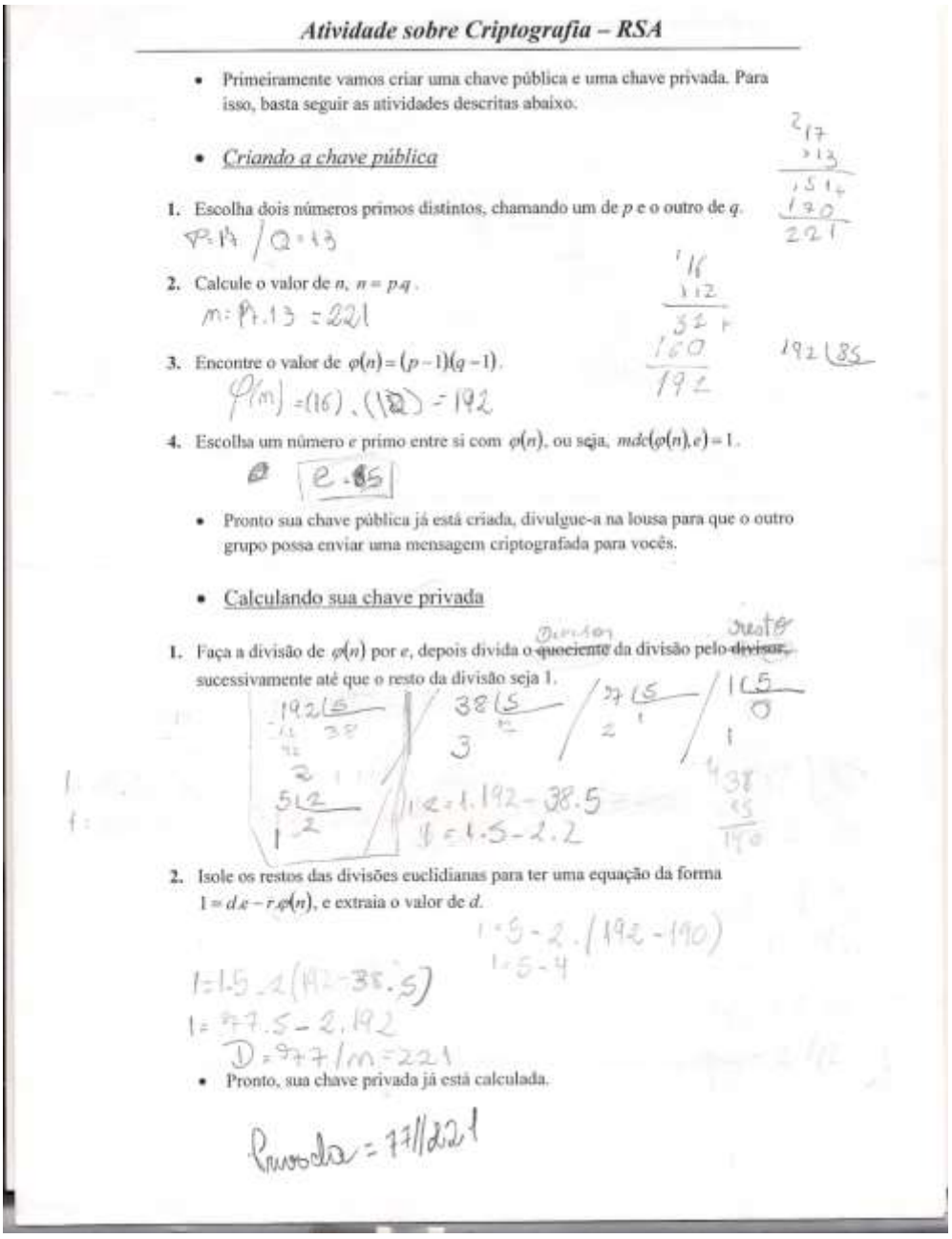
- Agora faça o uso da chave pública do outro grupo para criar uma palavra criptografada de 6 letras, utilizando a calculadora do computador para calcular $c = m^e \bmod n$, sendo $m$ o valor número de cada letra extraído da tabela inicial. Escreva a palavra criptografada (código) na lousa para que o outro grupo tente desvendá-la.

- Por último, pegue o código (palavra criptografada) feito para o seu grupo e faça os cálculos, também com o auxílio do computador, para desvendar a palavra escondida, utilizando $m = c^d \bmod n$.



***Parabéns! Você atingiu o objetivo e desvendou a palavra!***

Grupo 2



***Atividade sobre Criptografia – RSA***

- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.

- *Criando a chave pública*

1. Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.
   P=17 / Q=13
2. Calcule o valor de $n$, $n = pq$.
   n: P.13 = 221
3. Encontre o valor de $\varphi(n) = (p-1)(q-1)$.
   φ(n) = (16).(12) = 192
4. Escolha um número $e$ primo entre si com $\varphi(n)$, ou seja, $mdc(\varphi(n), e) = 1$.
   e = 5

- Pronto sua chave pública já está criada, divulgue-a na lousa para que o outro grupo possa enviar uma mensagem criptografada para vocês.

- Calculando sua chave privada

1. Faça a divisão de $\varphi(n)$ por $e$, depois divida o ~~quociente~~ da divisão pelo ~~divisor~~, sucessivamente até que o resto da divisão seja 1.
   192 | 5 → 38 | 5 → 7 | 5 → 1 | 5
   1 = 1.192 − 38.5
   1 = 1.5 − 2.2
2. Isole os restos das divisões euclidianas para ter uma equação da forma $1 = d.e - r.\varphi(n)$, e extraia o valor de $d$.
   1 = 5 − 2.(192 − 190)
   1 = 5 − 4
   1 = 1.5 − 2.(192 − 38.5)
   1 = 77.5 − 2.192
   d = 77 / n = 221

- Pronto, sua chave privada já está calculada.

Privada = 77/221

- Agora faça o uso da chave pública do outro grupo para criar uma palavra criptografada de 6 letras, utilizando a calculadora do computador para calcular $c = m^e \bmod n$, sendo $m$ o valor número de cada letra extraído da tabela inicial. Escreva a palavra criptografada (código) na lousa para que o outro grupo tente desvendá-la.

1 - R — $12^5 \cdot \text{mod } 299$ — 205
2 - O — $14^5 \cdot \text{mod } 299$ — 222
3 - B — $2^5 \cdot \text{mod } 299$ — 32
4 - S — $18^5 \cdot \text{mod } 299$ — 187
5 - O — $14^5 \cdot \text{mod } 299$ — 222
6 - N — $13^5 \cdot \text{mod } 299$ — 234

- Por último, pegue o código (palavra criptografada) feito para o seu grupo e faça os cálculos, também com o auxílio do computador, para desvendar a palavra escondida, utilizando $m = c^d \bmod n$.

160 - 31 - 14 - 11 - 207 - 1

$160^{77} \text{ mod } 221 = 23$ — 160 Z
$31^{77} \text{ mod } 221 = 5$ — 31 E
$14^{77} \text{ mod } 221 = 209$ — 14 V
$11 = 4$ — 11 G
$207^{77} \text{ mod } 221 = 12$ — 207 M
— 1 A

***Parabéns! Você atingiu o objetivo e desvendou a palavra!***

Grupo 3

Grupo 3

## *Atividade sobre Criptografia – RSA*

- Primeiramente vamos criar uma chave pública e uma chave privada. Para isso, basta seguir as atividades descritas abaixo.

- *Criando a chave pública*

1. Escolha dois números primos distintos, chamando um de $p$ e o outro de $q$.

23 . 13

2. Calcule o valor de $n$, $n = p.q$.

n = 23 . 17 → n = 299

3. Encontre o valor de $\varphi(n) = (p-1)(q-1)$.

φ(299) = (23-1) (13-1) → φ(299) = 264

φ(299) = (22) . (12)

4. Escolha um número $e$ primo entre si com $\varphi(n)$, ou seja, $mdc(\varphi(n), e) = 1$.

e = 5

- Pronto sua chave pública já está criada, divulgue-a na lousa para que o outro grupo possa enviar uma mensagem criptografada para vocês.

- Calculando sua chave privada

1. Faça a divisão de $\varphi(n)$ por $e$, depois divida o quociente da divisão pelo divisor, sucessivamente até que o resto da divisão seja 1.

divisor pelo resto

264 | 5 | 52
14
4

52 | 14 | 1
1

2. Isole os restos das divisões euclidianas para ter uma equação da forma $1 = d.e - r.\varphi(n)$, e extraia o valor de $d$.

4 = 1.264 - 5.25

1 = 14 - 1.4

1 = 1.5 - 1.(1.264 - 52.5)

1 = 53.5 - 1.264

- Pronto, sua chave privada já está calculada.

d = 53

- Agora faça o uso da chave pública do outro grupo para criar uma palavra criptografada de 6 letras, utilizando a calculadora do computador para calcular $c = m^e \bmod n$, sendo $m$ o valor número de cada letra extraído da tabela inicial. Escreva a palavra criptografada (código) na lousa para que o outro grupo tente desvendá-la.

12 14 13 7 14 11
MONGOL

M
$C = m^E \bmod n$

n=407
E=7

| | | |
|---|---|---|
| M | $12^7 \bmod 407$ | 342 |
| O | $14^7 \bmod 407$ | 97 |
| N | $13^7 \bmod 407$ | 106 |
| G | $7^7 \bmod 407$ | 182 |
| O | $14^7 \bmod 407$ | 97 |
| L | $11^7 \bmod 407$ | 11 |

- Por último, pegue o código (palavra criptografada) feito para o seu grupo e faça os cálculos, também com o auxílio do computador, para desvendar a palavra escondida, utilizando $m = c^d \bmod n$.

$m = C^d \bmod n$

d=53
n=299

| | |
|---|---|
| $205^{53} \bmod 299 = 17$ | R |
| $223^{53} \bmod 299 = 14$ | O |
| $32^{53} \bmod 299 = 2$ | B |
| $187^{53} \bmod 299 = 18$ | S |
| $225^{53} \bmod 299 = 14$ | O |
| $234^{53} \bmod 299 = 13$ | N |

***Parabéns! Você atingiu o objetivo e desvendou a palavra!***

# 7. REFERÊNCIAS

ALMOULOUD, Saddo Ag; SILVA, Maria José Ferreira. **Engenharia didática: evolução e diversidade**. Revemat: R. Eletr. de Edu. Matem. eISSN 1981-1322. Florianópolis, v. 07, n. 2, p. 22-52, 2012.

ALMOUOUD, Saddo, Ag; COUTINHO, Cileda de Queiroz e Silva. **Engenharia didática e seus usos em trabalhos apresentados no GT-19 / ANPEd**. REVEMAT - Revista Eletrônica de Educação Matemática. V3.6, p.62-77, UFSC: 2008.

BEZERRA, Débora de Jesus; MALAGUTTI, Pedro Luiz; RODRIGUES, Vânia Cristina da Silva. **Aprendendo criptologia de forma divertida**.

FALEIROS, Antonio Cândido. **Criptografia** - São Carlos, SP: SBMAC, 2011, 138 p., (Notas em Matemática Aplicada; v. 52).

ROUSSEAU, Christiane; SAINT-AUBIN, Yvan. **Mathmetics and Technology**. Springer, 2008.

OLIVEIRA, Zelci Clasen. **Uma interpretação geométrica do mdc**. RPM 29.