Criptografia RSA Gaussiana

Luis Antonio Coêlho

Trabalho de Conclusão de Curso - parte I apresentado à
Faculdade de Tecnologia da
Universidade Estadual de Campinas

Orientador: **Profa. Dra. Juliana Bueno**

29 de novembro de 2016

Resumo

O presente projeto visa estudar a chamada criptografia de chave pública RAS, baseada em números primos, e investigar a possibilidade de se usar os chamados primos de Gauss obtendo assim o que chamaremos de *critografia RAS gaussiana*. O intuito do trabalho é fazer um comparativo entre as duas abordagens com relação à dificuldade de quebra de código.

Sumário

Introdução

Introduza o que você pretende fazer no decorrer do seu trabalho.

Capítulo 1

Justificativa

Faz parte da sobrevivência humana manter segredo acerca de alguns fatos e quando se trata de comunicação, seja escrita ou falada, essa prática se intensifica ainda mais à medida que se expandem os meios de comunicação. A necessidade de manter algumas informações em segredo levou o homem a se comunicar através de códigos e à medida em que tais códigos são descobertos há a necessidade de se criar novos códigos para que a comunicação seja antida em sigilo. Foi a partir desse tipo de necessidade que se inaugurou o que chamamos de *criptografia*, isto é, ao conjunto de técnicas usadas para se comunicar em códigos. O objetivo da comunicação em códigos é garantir que apenas as pessoas interessadas (ou envolvidas na comunicação) possam compreender a mensagem codificada (ou criptogtafada), garantindo que a mensagem seja lida apenas pelos interessados.

Para compreender como funciona o processo de codificação e decodificação fazemos uso de uma série de termos técnicos, com intuito pedagógico iremos introduzir tais conceitos apresentando um dos primeiros algorítmos criptográficos que se tem conhecimento, a criptografia de César, e suas sucessoras.

A chamada *criptografia de César*, criado pelo imperador romano César Augusto, consistia em substituir cada letra por outra que estivesse a três posições a frente, como, por exemplo, a letra **A** era substituída pela letra **D**.

Uma forma muito natural de se generalizar o algoritmo de César é fazer a troca da letra por outra em uma posição qualquer fixada. A chamada *criptografia de substituição monoalfabética* consite em substituir cada letra pela letra que ocupa n posições a sua frente, sendo que o número n é conhecido apenas pelo emissor e pelo receptor da mensagem. Chamamos este

número n de *chave criptográfica*.

O algoritmo monoalfabético tem a característica indesejada de ser de fácil decodificação, pois possui apenas 26 chaves, e isso faz com que no máximo 26 tentativas o código seja decifrado. Com o intuito de dificultar a quebra do código monoalfabético foram propostas as *cifras de substituição polialfabéticas* em que a chave criptográfica passa a ser uma *palavra* ao invés de um número. A ideia é usar as posições ocupadas pelas letras da chave para determinar o número de posições que devemos avançar para obter a posição da letra encriptada. Vejamos, por meio de um exemplo, como funciona esse sistema criptográfico.

Sejam "SENHA" a nossa chave criptográfica e "ABOBORA" a mensagem a ser encriptada. Abaixo colocamos as letras do alfabeto com suas respectivas posições. Observe que repetimos a primeira linha de letras para facilitar a localização da posição da letra encriptada e usamos a barra para indicar que estamos estamos no segundo ciclo.

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	**E**	F	G	**H**	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	**S**	T	U	V	X	Y	W	Z
27	28	29	30	31	32	33	34	35	36	37	38	39
$\overline{A}$	$\overline{B}$	$\overline{C}$	$\overline{D}$	$\overline{E}$	$\overline{F}$	$\overline{G}$	$\overline{H}$	$\overline{I}$	$\overline{J}$	$\overline{K}$	$\overline{L}$	$\overline{M}$

Vejamos como encriptar a palavra "ABOBORA". Iniciamos o processo escrevendo a mensgem. Ao lado de cada letra da mensagem aparece entre parênteses o número que indica a posição ocupada de cada letra. Abaixo da mensagem escrevemos as letras da chave criptográfica, repetindo de forma cíclica as letras da chave quando necessário. Analogamente, ao lado de cada letra da chave aparece entre parênteses o número da posição ocupada de cada letra, e o sinal de soma indica que devemos avançar o aquele número de posições. Ao final do processo aparecem as letras encriptadas. Entre parênteses está a posições resultante da combinação das posições da mensagem e da chave.

$A(1)$	$B(2)$	$O(15)$	$B(2)$	$O(15)$	$R(18)$	$A(1)$	Mensagem
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
$S(+19)$	$E(+5)$	$N(+14)$	$H(+8)$	$A(+1)$	$S(+19)$	$E(+5)$	Chave
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
$T(20)$	$G(7)$	$C(29)$	$J(10)$	$P(16)$	$K(37)$	$F(6)$	Mensagem encriptada

Observe que a encriptação polialfabética é mais difícil de ser quebrada do que a monoalfabética uma vez que letras iguais não têm, necessariamente, a mesma encriptação. Observe que nesse tipo de criptografia o emissor precisa passar a chave para o receptor da mensagem de forma segura para que o receptor possa decifra a mensagem, isto é, a chave usada para encriptar a mensagem é mesma que deve ser usada para decifrar a mensagem. Veremos que esse é justamente o ponto fraco nesse tipo de encriptação pois usa a chamada *chave simétrica*, ou seja, a chave usada pelo emissor para codificar a mensagem é a mesma usada pelo receptor para decodificar a mensagem. Nesse processo, a chave deve ser mantida em segredo e bem guardada para garantir que o código não seja quebrado e isso requer algum tipo de contato físico entre emissor e receptor.

Durante a Primeira Guerra Mundial muitos foram os investimentos em máquinas para fazer encriptação de mensagens de maneira automática. *Enigma* é o nome da famosa máquina utilizada pelos alemães tanto para criptografar como para descriptografar códigos de guerra. Era uma máquina semelhante a uma máquina de escrever, os primeiros modelos foram patenteados por Arthur Scherbius em 1918. Essas máquinas ganharam popularidade entre as forças militares alemãs devido a facilidade de uso e sua suposta indecifrabilidade do código.

O matemático Alan Turing foi o responsável por quebrar o código dos alemães durante a Segunda Guerra Mundial. A descoberta de Turing mostrou a fragilidade da criptografia baseada em chave simétrica e colocou novos desafios à criptografia. O grande problema passou a ser a questão dos protocolos, isto é, como transmitir a chave para o receptor de forma segura sem que haja contato físico entre as partes? Em 1949, com a publicação do artigo *Communication Theory of Secrecy Systems* de Shannon, novos desafios marcam o início da criptografia moderna.

MELHORAR O TEXTO DAQUI PARA FRENTE.

1. O QUE ACONTECEU ENTRE 1949 E 1995? A CRIPTOGRAFIA ESTEVE PARADA NESSE MEIO TEMPO?

2. COMENTE O ARTIGO DO SHANNON.

3. PONTO IMPORTANTE: A CRIPTOGRAFIA RSA TIRA PARTIDO DO TEMPO GASTO PARA FATORAR NÚMEROS. ISSO SERÁ DIFERENTE COM OS PRIMOS DE GAUSS? ESSE É UM DOS PONTOS A SER INVESTIGADO.

4. FALAR SOBRE O PROBLEMA P=NP.

5. FALAR SOBRE AS SEMELHANÇAS E AS DIFERENÇAS ENTRE OS PRIMOS E O PRIMOS DE GAUSS.

6. COLOCAR AS REFERÊNCIAS AO LONGO DO TEXTO.

Em 1995, com o objetivo de se criar um padrão de criptografia único, foi criado em parceria entre IBM e governo dos Estados Unidos a criptografia DES, que foi substituída pela AES em 2001.

Antes disso houve a publicação de um artigo que revolucionou a área, em *New Directions in Cryptography* (Diffie e Hellman, 1976) houve a introdução do conceito de chave assimétrica, onde há chaves diferentes entre o emissor da mensagens e o receptor.

Um dos algoritmos deste modelo de chave assimétrica é o RSA(RIVEST et al, 1983), algoritmo desenvolvido por Rivest, Shamir e Adleman. Este algoritmo está presente em muitas aplicações de alta segurança, como bancos, sistemas militares e servidores de internet, e ele utiliza para a geração de chaves os números primos naturais de grandeza superior a 2512 multiplicados entre si.

O grande problema no uso de primos naturais consiste na Hipótese de Riemann (Riemann,1859), um dos sete desafios matemáticos do milênio. A hipótese diz que informando um número teto, podemos saber quantos e quais são os primos presentes naquele conjunto, este tipo de dado é desastroso para modelos criptográficos centrados nos primos naturais, como o RSA, pois tornaria extremamente mais fácil a realização da descoberta das chaves.

Uma forma para se evitar este problema seria uma substituição dos primos naturais por um conjunto de primos não-naturais, como os primos de Gauss (Gauss, 1815). Estes números compõem o conjunto de números complexos da forma $a+bi$, onde a e b são diferentes de 0, com a^2+b^2 resultando em um primo natural.

Por isso venho a propor esta pesquisa, para que possa testar a capacidade de um algoritmo criptográfico centrado nos primos de gauss de ser tão efetivos quanto os algoritmos criptográficos centrados em primos naturais, para que em um futuro, caso ele seja necessário ele possa ser imediatamente e amplamente utilizado.

Referências Bibliográficas