Criptografia de chave pública com primos de Gauss

Luis Antonio Coêlho

Novembro de 2016

Resumo

Projeto de pesquisa apresentado como requisito para aprovação da disciplina de Trabalho de Conclusão de Curso I na Faculdade de Tecnologia da Universidade Estadual de Campinas.

Sumário

1 Dados para identificação do projeto

O projeto será conduzido pelo aluno Luis Antonio Coêlho, sob a orientação da Profa. Dra. Juliana Bueno e será focado na comparação de algoritmos de criptografia de chave pública com relação a segurança dos dados.

2 Tema

Criptografia de chave pública com uso do conjunto numérico dos primos Gaussianos e sua eficiência para a área de segurança da informação.

3 Formulação do problema

O problema a ser resolvido com este projeto é se uma criptografia baseada no conjunto dos números primos de Gauss é viável?

4 Justificativa

A humanidade sempre quis manter algumas informações em segredo e para isso veio a inventar a criptografia, que em sua essência é um meio de garantir que apenas as pessoas certas venham a comprrender certa mensagem, mesmo que esta venha a cair nas mãos de pessoas que não deveriam recebê-la.

Para poder ter essa garantia que foram inventados os primeiros algoritmos criptográficos, como a criptografia de César, criado pelo imperador romano César Augusto. Nela toda a letra era substituída pela que viesse três posições a frente, como, por exemplo, a letra A era substituída pela letra D.

Baseado no algoritmo de César surgiu a criptografia de substituição monoalfabética, onde cada letra era substituída pela letra n posições a frente dela, sendo que n era conhecido apenas pelo emissor e pelo receptor da mensagem. A este número n deu-se o nome de chave criptográfica.

O algoritmo monoalfabético possuía um problema de possuir apenas 26 chaves, o que o tornava fácil de ser quebrado, por isso foi substituído pelas cifras de substituição polialfabéticas.

Em um sistema polialfabético normalmente é utilizada uma palavra como chave, e para a substituição usamos o monoalfabeto intercalando as chaves, ou seja, tomemos como chave a palavra SENHA, se a primeira letra de um texto for A, ela deverá ser substituída pelo S, se a segunda for B, ela deve ser substituída por F(pois aqui tomamos o E por A, logo usamos o monoalfabeto com a chave valendo 5). A partir da sexta letra repetimos a primeira chave.

Para exemplificar, assumindo que a palavra que queremos encriptar seja ABELHA e a chave seja SENHA a mensagem encriptada será SFRSHS. Repare que mesmo A e L sendo letras diferentes elas foram encriptadas com o mesmo valor(S).

Mesmo com a técnica polialfabética sendo mais avançada, ela ainda era muito suscetível a quebra, por possuírem a chave simétrica, ou seja igual para emissor e receptor, principalmente após o surgimento dos decifradores nas guerras mundiais, como o alemão Enigma, o inglês Typex e o norte-americano SIGABA CCM(Máquina de cifra combinada).

Baseado no resultado destas máquinas, principalmente do SIGABA, foi publicado em 1949 o artigo Communication Theory of Secrecy Systems (Shannon, 1949), onde se abordam os resultados das máquinas criptográficas de guerra. Este artigo é tomado como início da criptografia moderna.

Em 1995, com o objetivo de se criar um padrão de criptografia único, foi criado em parceria entre IBM e governo dos Estados Unidos que culminou na 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 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 2^{512} 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 extremament 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). Este números compõem o conjunto de números complexos $a+bi$ 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 hoje existentes, para que em um futuro, caso ele seja necessário ele possa ser imediatamente e amplamente utilizado.

5 Objetivos

5.1 Objetivo geral

Analisar se a substituição do algoritmo de criptografia RSA por um algoritmo derivado do RSA com a substituição do conjunto gerador de chaves de primos naturais para primos de gauss(Gauss, 1815) pode ser considerada eficiente para a segurança da informação.

5.2 Objetivos específicos

- Implementar o algoritmo de criptografia RSA em linguagem Python
- Implementar algoritmo derivado da criptografia RSA, baseado no conjunto dos primos de gauss, em linguagem Python
- Criar e aplicar uma metodologia de comparação de segurança para os dois sistemas

6 Metodologia

6.1 Método de abordagem

O projeto buscará checar a eficiência do algoritmo a ser desenvolvido, por meio de uma metodologia a ser desenvolvida.

6.2 Técnicas de pesquisa

Na primeira fase do projeto será feita uma revisão bibliográfica na área de criptografias, focada nas de chave pública. Em uma segunda fase serão executados testes de comparação de segurança entre algoritmos de criptografia de chave pública, buscando descobri qual dos pesquisados e/ou produzidos é mais seguro.

7 Referências

Diffie e Hellman, "New directions in cryptography" Gauss, *Methodus nova integralium valores per approximationem inveniendi* Riemann, "Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse" Rivest, Shamir e Adleman, "A method for obtaining digital signatures and public-key cryptosystems" Shannon, "Communication theory of secrecy systems" Sinkov e Feil, *Elementary cryptanalysis Millennium Problems — Clay Mathematics Institute*

Referências

Diffie, Whitfield e Martin Hellman. "New directions in cryptography". Em: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

Gauss, Carl Friedrich. *Methodus nova integralium valores per approximationem inveniendi*. apvd Henricvm Dieterich, 1815.

Millennium Problems — Clay Mathematics Institute. Acessado em 15/11/2016.

Riemann, Bernhard. "Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse". Em: *Ges. Math. Werke und Wissenschaftlicher Nachlaß* 2 (1859), pp. 145–155.

Rivest, Ronald L, Adi Shamir e Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Em: *Communications of the ACM* 21.2 (1978), pp. 120–126.

Shannon, Claude E. "Communication theory of secrecy systems". Em: *Bell system technical journal* 28.4 (1949), pp. 656–715.

Sinkov, Abraham e Todd Feil. *Elementary cryptanalysis*. Vol. 22. MAA, 2009.