Revista F@pciência, Apucarana-PR, ISSN 1984-2333, v.5, n. 4, p. 22 – 25, 2009.

A CRIPTOGRAFIA RSA E DES

SILVEIRA, A. de S.[1]

[1] Athânio de Souza Silveira. Formado em Licenciatura Ciências da Computação, UESPI. Especialista em Docência do Ensino Superior em Análise de Sistema FAP.

RESUMO

Em todo o momento da História, a criptografia está presente; deste o império romano, quando o imperador deveria criar uma criptografia para enviar uma mensagem e não ser lido por outra pessoa, criando-se, assim, a criptografia de César. Atualmente quase todo sistema que trabalho com envio e recebimento de informações utiliza algum método de criptografia. Por isso, o estudo e aperfeiçoamento da criptografia vêm se tornando cada vez mais complexo e essencial. Nesse artigo, são descritos alguns aspectos básicos sobre a criptografia DES e RSA, em que, com esse algoritmo, a quebra dessa criptografia, chamado encriptografia, torna-se cada vez mais difícil de acontecer.

Palavras-chave: Criptografia RSA. Algoritmo. Encriptografia.

ABSTRACT

In all the moment of the History the cryptography is present, of this the Roman empire, where the emperor to send a message he should create a cryptography for not could be read by other person without being the addressee, then in that time Caesar's cryptography was created. Now almost whole system that uses sending and reception of information uses some cryptography method. Therefore the study and improvement of the cryptography come if turning more and more complex and essential. In that article some basic aspects are described on the cryptography GIVE and RSA, where with that algorithm the break of that cryptography, called encriptografia becomes more and more difficult to happen.

Key-words: Cryptography RSA. Algorithm. Encriptografia.

INTRODUÇÃO

A criptografia, com o advento da Internet e a utilização de computadores em rede, acabou tornando-se uma necessidade. Ela é usada, dentre outras finalidades, para: proteger documentos secretos; autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade

de transações comerciais por meio eletrônico; e proteger o sigilo de comunicações pessoais.

A criptografia RSA é um sistema de criptografia em que a chave de codificação é pública, permitindo então que qualquer pessoa codifique mensagens, e a chave de decodificação é privada. Este tipo de criptografia é extremamente adequado para, por exemplo, comércio eletrônico na Internet. O DES é um ciframento composto que cifra blocos de 64 bits (8 caracteres) em blocos de 64 bits; para isso ele se utiliza de uma chave composta por 56 bits mais 8 bits de paridade (no total são 64 bits também). Neste artigo, iremos abordar essas duas técnicas de criptografia, as quais se transformaram nas principais criptografias e mais difundido algoritmo de chave única.

A CRIPTOGRAFIA RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA. As letras RSA correspondem às iniciais dos inventores do código.

Para implementar o RSA precisamos de dois números primos *p* e *q*. Para codificar a mensagem basta utilizar o produto destes dois números que chamaremos de *n*, que é a *chave pública de codificação.* Cada usuário do RSA possui sua própria chave. Esta chave é dita pública, pois todos podem codificar uma mensagem. A *chave de decodificação* é constituída pelos primos e deve ser mantida em segredo visto que a segurança do RSA depende disto. Vamos utilizar o código ASCII para converter cada caractere da mensagem em seu respectivo valor numérico na tabela ASCII transformando o texto então em um número gigantesco. Este número é quebrado em blocos de números menores do que o valor da *chave pública n*.

CODIFICAÇÃO E DECODIFICAÇÃO

Para codificar a mensagem, precisamos de *n* e de um inteiro positivo que seja inversível módulo *ø (n)*, onde *ø (n) = (p-1)(q-1).* Vamos chamar de *C(b)* o bloco codificado.

A CRIPTOGRAFIA DES

O algoritmo Data Encryption Standart (DES) é um algoritmo criptográfico simétrico que cifra blocos de 64 bits de texto claro e utiliza uma chave secreta de 64 bits.

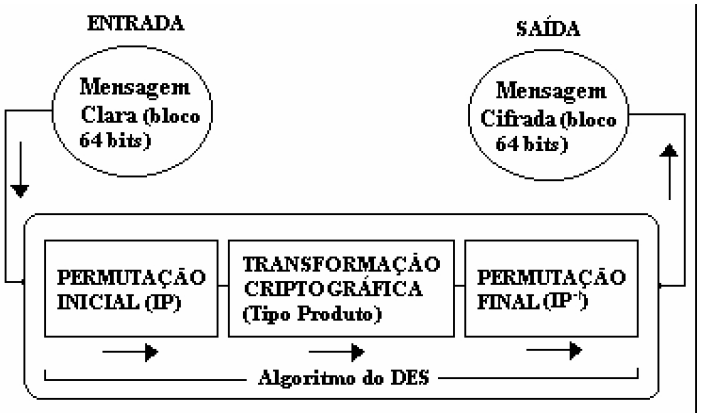

Figura 1 – Processo de criptografia do algoritmo DES

A primeira etapa do processo de cifragem acontece na Permutação Inicial. Nesta etapa, é realizada uma operação de transposição de bits. Essa transposição é feita no bloco de 64 bits da mensagem clara. Nesta etapa, serão realizadas inúmeras operações lógicas de substituição e de transposição, que serão executadas em 16 rodadas. Em seguida, é realizada uma operação de transposição que é o inverso da realizada na Permutação Inicial. Existem alguns sucessores do DES, como por exemplo: DES triplo, G-DES, DES-X, LOKI89, GELO.

ANÁLISE DO TEMPO

A análise do tempo é realizada utilizando mensagens de diferentes tamanhos usando o sistema RSA e o sistema DES com o uso do algoritmo. Verificamos que, de acordo com algoritmo RSA com números primos altos, fica quase impossível quebrar a chave; já no DES de chave única utilizando 64 bits torna um algoritmo seguro com sua permutação.

ANÁLISE DOS RESULTADOS

Observamos que aumentando linearmente o número de caracteres da mensagem, o tempo gasto pelo sistema RSA aumenta linearmente enquanto o

sistema que utiliza o algoritmo DES mantém um tempo quase constante. É importante salientar que isso ocorre com uso de números com poucos algarismos, visto que se aumentarmos muito tais números, o sistema RSA torna-se totalmente inviável de implementação.

CONSIDERAÇÕES FINAIS

Observamos que a implementação do sistema RSA ainda hoje é utilizado devido sua eficaz criptografia de dados, e a segurança na quebra da chave, em termos práticos. A segurança do RSA depende de uma chave com muitos dígitos. Já o sistema DES com o uso do algoritmo viável para chave única, em que não se utiliza codificação com número primos, apenas chaves de 64 bits, pode ser quebrado por tentativas de combinações contínuas, mas aumentando o número de caracteres da mensagem como o número de dígitos da chave, este demonstrou grande eficácia.

REFERÊNCIAS

COUTINHO, S. C. Números inteiros e criptografia RSA, **Série de Computação e Matemática**, Rio de Janeiro, IMPA, 1997.

DES - Data Encrypt Standard. Disponível em: http://penta.ufrgs.br/gere96/segur2/des.htm. Acesso em: ?

LEMOS, M. Criptografia, números primos e algoritmos, 17. **Colóquio Brasileiro de Matemática**, IMPA\CNPq, 1989.

VOLOCH, J. F. A distribuição dos números primos. **Matemática Universitária**, n. 06, 71-82, 1987.