CRIPTOGRAFIA: ESTUDO COMPARATIVO ENTRE SOFTWARES SOBRE A CRIPTOGRAFIA AES

Mauricio Frederico
Henrique Pachioni Martins
Kelton Augusto Pontara da Costa
André Luiz Ferraz Castro

Instituto de Informática – Universidade Sagrado Coração (USC)
Caixa Postal 17011-160 – Bauru – SP – Brasil

maufrederico@yahoo.com.br

Resumo

A criptografia é uma técnica milenar e a cada dia vem sendo mais utilizada por causa dos grandes avanços tecnológicos. No mundo atual há uma grande necessidade do uso de computadores para transferências de dados sigilosos, necessitando assim de ferramentas que garantem a sua confidencialidade, integridade e autenticação, sendo a criptografia importantíssima para que esses requisitos de segurança sejam preenchidos. Este trabalho faz uma explanação sobre as principais técnicas de criptografia simétrica e assimétrica. Por fim é realizada uma comparação entre softwares que utilizam a criptografia Advanced Encryption Standard mostrando as vantagens e desvantagens.

Abstract

The encryption is a millennial technique and each day has been most widely used because of technological advances. In current world has a big necessity to use computer for transfer secret data, thus needing tools to ensure it's confidentiality, integrity and authentication and encryption is important to fill this requirements. This article is an explanation of the main techniques of symmetric and asymmetric encryption. Finally a comparison among softwares that use a Advanced Encryption Standard encryption, is made to show the advantages and disadvantages.

1 Introdução

A criptografia vem sendo usada há vários séculos em contextos militares e diplomáticos para prover o sigilo das informações, pois ela torna ou tenta tornar os dados irreconhecíveis para qualquer pessoa que não seja o remetente ou receptor da mensagem.

Com os avanços tecnológicos e o uso do computador para transmissão e arquivamento de dados sigilosos foi preciso utilizar ferramentas automatizadas como: banco de dados, antivírus e firewall para prover a

segurança destes arquivos e outras informações, garantindo assim a confidencialidade, integridade e autenticação. A criptografia vem sendo de grande importância para que esses requisitos sejam atingidos.

Este trabalho tem o propósito de estudar, através de pesquisas bibliográficas, os vários tipos de criptografia existentes, mostrando as suas características. Posteriormente será realizada uma comparação de software utilizando a criptografia AES (Advanced Encryption Standard) que é a criptografia padrão dos EUA, aumentando assim o conhecimento de técnicas criptográficas utilizadas no mercado.

2 Desenvolvimento

2.1 Criptografia

O termo criptografia surgiu com a fusão de duas palavras de origem grega kryptós e gráphein que significam “escondido” e “escrita”, respectivamente. Essa técnica tem como objetivo de codificar a mensagem, sendo que apenas o emissor e o receptor, consigam acessá-las e obter corretamente a informação, evitando assim que pessoas não autorizadas obtenham conhecimento das informações sigilosas.(Mendes: 2007)

Tkotz (2005) afirma que a criptografia evolui e sofreu grandes transformações nos quatro mil anos de história, tendo como seu principal colaborador, os militares, os quais utilizavam estes métodos para obter segurança dos dados transmitidos.

Atualmente, com os avanços tecnológicos, a utilização do computador passou a ser indispensável, necessitando assim um vasto sistema de proteção, nas quais as informações estejam seguras e sejam confiáveis, este é o papel da criptografia.

2.2 Conceitos

Abaixo serão relacionados os principais conceitos de criptografia que serão de suma importância para o entendimento no decorrer deste trabalho.

O transmissor é aquele que transforma a mensagem original em uma mensagem criptografada. O receptor recebe a mensagem criptografada e transforma novamente na mensagem original.

É chamado de mensagem ou texto claro, o texto original, aquele que ainda não foi modificado. O processo de torná-la ilegível é chamado encriptação ou cifragem, já o processo inverso, ou seja, tornar a mensagem legível é chamado decriptação ou decifragem.

A chave secreta é uma informação na qual é utilizada no método de cifragem e decifragem. Segundo Burnett e Paine (2002) “a chave secreta funciona da mesma maneira que uma chave convencional”, ela é utilizada em

uma fechadura (Algoritmo de Criptografia) e protegera as informações, que somente com a chave certa o usuário poderá proteger e ter acesso as mesmas (Floriano: 2007).

A técnica para manter a mensagem segura é chamada criptografia. A técnica utilizada para desvendar, quebrar, descobrir o conteúdo tem o nome de criptoanálise. Essas duas técnicas usadas juntas é denominado criptologia.

2.3 Criptografia Simétrica

A criptografia simétrica ou de chave privada é baseada na utilização de apenas uma chave tanto para emissor quanto para o receptor da mensagem. Benitz (2003) afirma que o grande problema deste tipo de criptografia é “o número de chaves cresce proporcionalmente ao quadrado do número de participantes, visto que entre cada par de usuários existe uma, e somente uma chave e essa não pode ser utilizada para comunicação com um terceiro usuário”, precisando assim de um grande numero de chaves caso a troca de informações ocorra com várias pessoas. Necessita assim de um gerenciamento nesta chave, pois se ela for interceptada por outra pessoa não autorizada, a mensagem criptografada poderá ser decifrada ou alterada facilmente. (Burnett; Paine: 2002)

Há grande vantagem da criptografia simétrica é que seu algoritmo são bem mais rápidos que algoritmos de chave pública e sua implementação pode ser alcançada mais facilmente. (GARFINKEL; SPAFFORD: 1999)

2.3.1 AES (Advanced Encryption Standard)

O órgão NIST encarregado para aprovar padrões para o Governo Federal dos Estados Unidos percebeu que a necessidade de um novo sistema criptográfico, pois o DES e o 3DES estavam com a vida útil no fim. Porém eles tinham o receio de com o anúncio desse novo padrão, as pessoas que soubessem algo sobre criptografia acabaram deduzindo automaticamente que National Security Agency (NSA) havia criado uma porta dos fundos no DES, conseguindo assim ler tudo o que foi criptografado por ele e o novo padrão criptográfico não fosse utilizado e provavelmente desaparecesse. (Tanenbaum: 2003)

Para solucionar este problema a NIST adotou uma estratégia diferente, patrocinando um concurso de criptografia chamado Advanced Encryption Standard (AES). Em 1997, pesquisadores do mundo inteiro foram convidados para participar deste concurso. (Tanenbaum: 2003)

Os principais critérios para a avaliação dos algoritmos estavam ligados a segurança (não possuir fraqueza algorítmica), desempenho (rapidez em várias plataformas) e tamanho (ocupar pouco espaço e memória). Para a escolha do vencedor foram realizadas conferencias públicas na qual os participantes eram encorajados a descobrir falhas. Na última conferência foi realizado uma

votação que teve como vencedor Rijndael dos autores Joan Daemen e Vicent Rijmen, com 84 votos. (Burnett; Paine: 2002)

2.4 Criptografia Assimétrica

A grande vantagem da criptografia assimétrica é que permite qualquer pessoa enviar uma mensagem, apenas utilizando a chave pública de quem vai recebê-la, não havendo a necessidade de um compartilhamento da mesma chave, aumentando assim a segurança (Schneier: 1996).

Burnett e Paine (2002) afirmam que é necessário ambas as chaves para criptografar e decriptografar, podendo uma se tornar pública, sem colocar a segurança em perigo. Para fazer a criptografia é utilizada a chave pública e para decriptografar é utilizado à chave privada.

Esta técnica permite que todos os participantes tenham acesso as chaves públicas, já as chaves privadas são geradas localmente para cada participante, não sendo preciso à distribuição das mesmas. A informação recebida estará protegida desde que a chave privada de um usuário permaneça protegida e secreta (Stallings: 2008).

3 Metodologia

Como proposta para o presente estudo, inicialmente foi realizada uma pesquisa bibliográfica que segundo DOMINGUES; HEUBEL; ABEL (2003) as pesquisas devem conter assuntos gerais e particulares podendo ser localizadas em diversas fontes de pesquisas como periódicos livros e materiais digitais nos quais tende a ter a facilidade em encontrar assuntos sobre criptografia.

Com o término desta pesquisa foi realizada uma procura por software de maneira aleatória, priorizando os que apresentavam uma interface amigável e utilizava a criptografia AES. Foram escolhidos: Chiave File Encryption, Sfx Creator e S.L Encrypt File, todos freeware. Também foi utilizado o software auxiliar Gerador de Chaves para Criptografia assimétrica, responsável por gerar as chaves usadas para realizar a criptografia.

Após o entendimento do funcionamento dos softwares foram realizados testes para coletar as vantagens e desvantagens, podendo assim ter um comparativo de cada software utilizando a criptografia AES.

Para realizar a criptografia foram escolhidos quatro tipos de arquivos de maneira aleatória, visando os arquivos mais comuns utilizados no computador. Foram criados arquivos de: música, imagem, documentos e filme com aproximadamente 300 MB cada. Por fim estes arquivos foram unidos criando um único arquivo de 1,20 GB que recebeu o nome de “todos”. Estes arquivos

com exceção do de vídeo foram zipados utilizando o programa Winrar.

Para a medição do tempo foi utilizado um cronometro de relógio, podendo assim ocorrer uma variação do tempo obtido. Na verificação da utilização da CPU e da memoria foi utilizado o gerenciador de tarefas do Windows, deixando o visível enquanto os testes eram realizados.

Os testes foram realizados utilizando um notebook HP Pavilion dv5-1260br com processador AMD TurionTM X2 ultra, com 4 GB de memória DDR2 e um disco rígido de 250 GB. O sistema utilizado foi Windows 7 Professional de 64 bits.

4 Resultados e Discussões

Neste capítulo será apresentado as características de cada software e os resultados obtidos nos testes realizados. Posteriormente será mostrado o desempenho obtido entre os softwares avaliados.

O primeiro software Chiave File Encryption apresenta uma interface intuitiva, além de proporcionar ao usuário o poder de adicionar vários arquivos para criptografar sem a necessidade de compactá-lo.

A grande diferença do SFX Creator é oferecer ao usuário a opção de escolher os algoritmos de criptografia finalistas do concurso AES e o blowfish. O software apresenta também um gerador de chaves que não foi utilizado nos testes.

Após serem criptografados o programa proporciona a escolha de três extensões: exe, zip e cab. Nos testes foi desprezado a extensão zip por necessitar um período de tempo muitas vezes maior do que os outros, cerca de 3 horas(10800 segundos).

Já o software S.L Encrypt file possui a vantagem de não precisar ser instalado para realizar a criptografia e a decriptografia, mas tem a desvantagem de não suportar o tamanho da chave de 256 bits, por isso os testes realizados que tinham como base a chave de 256 bits foram realizados utilizando a maior chave suportada pelo software.

O primeiro arquivo a ser analisado será o de Música. Observando o gráfico 1 é verificado que o software SFX Creator obteve o melhor desempenho em ambas as extensões exe e cab no processo de criptografia. Vale ressaltar o desempenho alcançado pela criptografia de 256 bits que embora utilize uma chave duas vezes maior conseguiu um tempo menor de execução, chegando no software Chiave File Encryption uma diferença de 150 segundos.

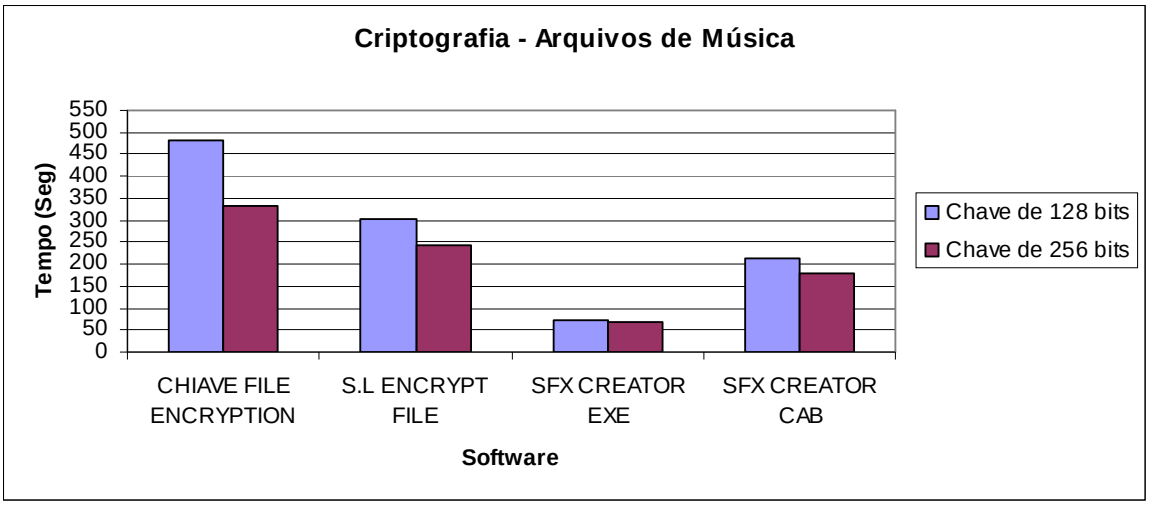

Gráfico 1- Desempenho dos softwares na criptografia do arquivo de música

O próximo tipo de arquivo a ser analisado é o de imagem como no teste anterior o SFX Creator atingiu o melhor desempenho na utilização das duas chaves, seguido pelo S.L Encrypt File na chave de 128 bits ou pelo Chiave File Encryption na chave de 256 bits como mostra o Gráfico 2. A utilização da chave de 256 bits acarretou o aumento no tempo em todos os softwares, exceto no Chiave File Encryption que teve seu tempo três vezes menor.

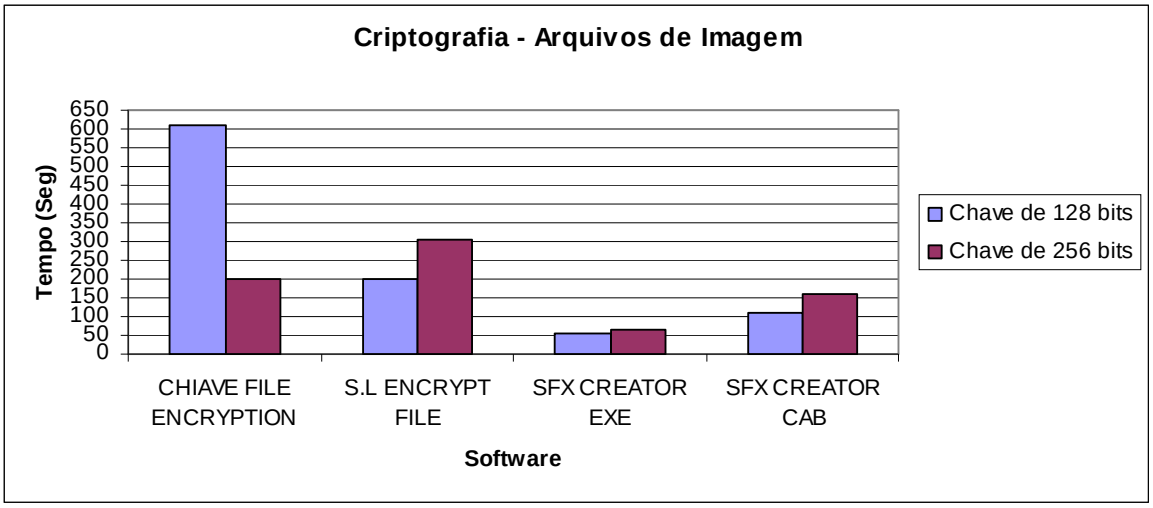

Gráfico 2 - Desempenho dos softwares na criptografia do arquivo de imagem

Analisando o gráfico 3 observa-se que os resultados obtidos pelos softwares Chiave File Encryption e S.L Encrypt File, utilizando o arquivo documentos, ficaram mais próximos do SFX Creator, embora este último continua com o melhor desempenho na extensão exe.

Na criptografia usando a chave de 128 bits, o software S.L Encrypt File

se destaca por conseguir o segundo tempo superando o SFX CAB na extensão cab em 32 segundos.

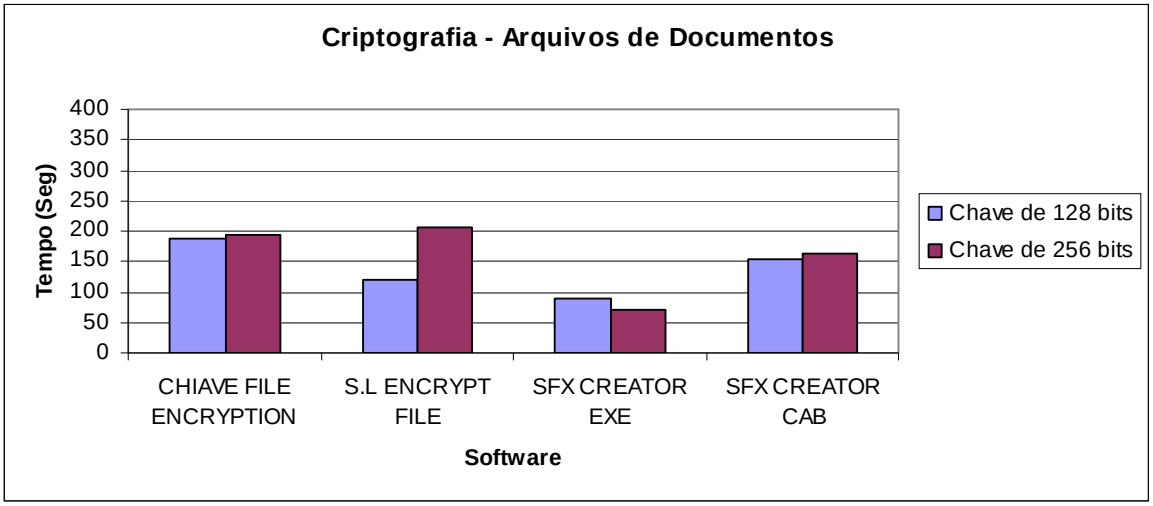

Gráfico 3 - Desempenho dos softwares na criptografia do arquivo de documentos

No Gráfico 4 é avaliado o desempenho obtido pelos softwares quando testados com arquivos de filmes. Novamente o SFX Creator atingiu o melhor resultado, seguido pelo S.L Encrypt e o Chiave File Encryption.

Nota-se que a variação de tempo entre a utilização da chave de 128 e a chave de 256 bits foi baixa, sendo a maior variação encontrada pertencente ao software SFX Creator, cerca de 50 segundos.

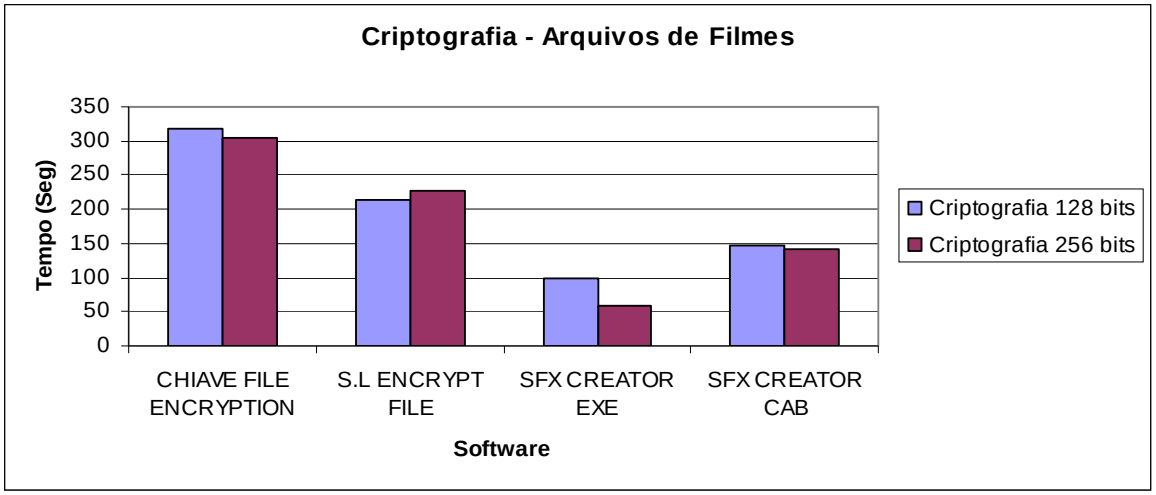

Gráfico 4 - Desempenho dos softwares na criptografia do arquivo de filmes

O ultimo arquivo a ser analisado é o todos que abrange os quatro tipos observados anteriormente: música, imagem, documentos e filmes. Observa-se no Gráfico 5 que SFX Creator como nos testes realizados em outros arquivos conseguiu o melhor desempenho.

O software Chiave File Encryption conseguiu superar o S.L Encrypt file quando criptografado com a chave de 128 bits, cerca de 300 segundos. Porem quando a chave foi aumentada seu tempo quase triplicou ficando em último lugar. Vale destacar que o arquivo todos foi o único arquivo onde o Chiave File Encryption perdeu rendimento significativo, alcançando a diferença de 1000 segundos.

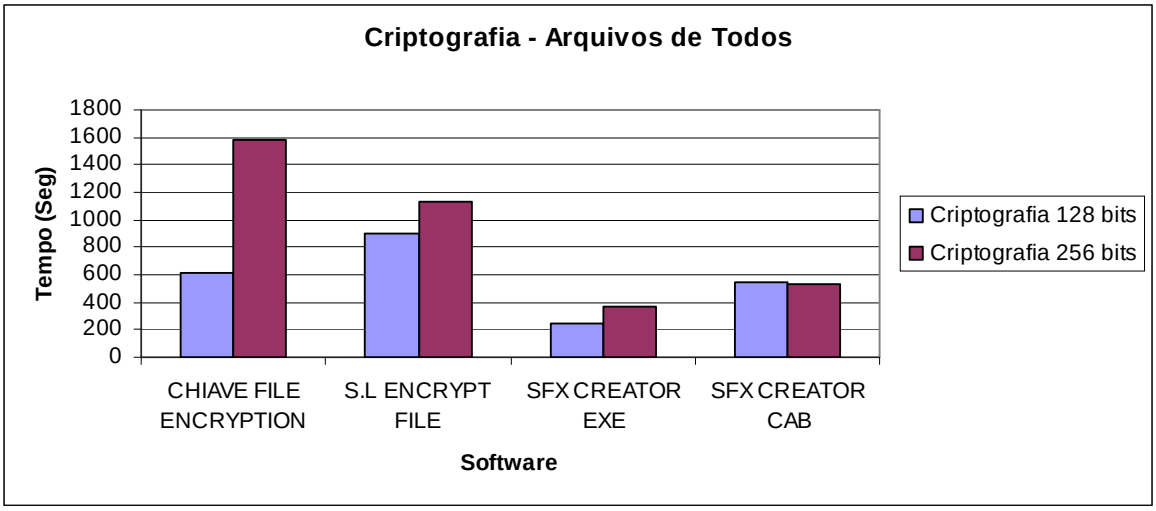

Gráfico 4 - Desempenho dos softwares na criptografia do arquivo de todos

Nos testes referentes ao desempenho da CPU obtiveram os resultados parecidos, havendo uma pequena variação de 2% entre o maior e menor valor como pode ser observado nos resultados obtidos no gráfico 6.

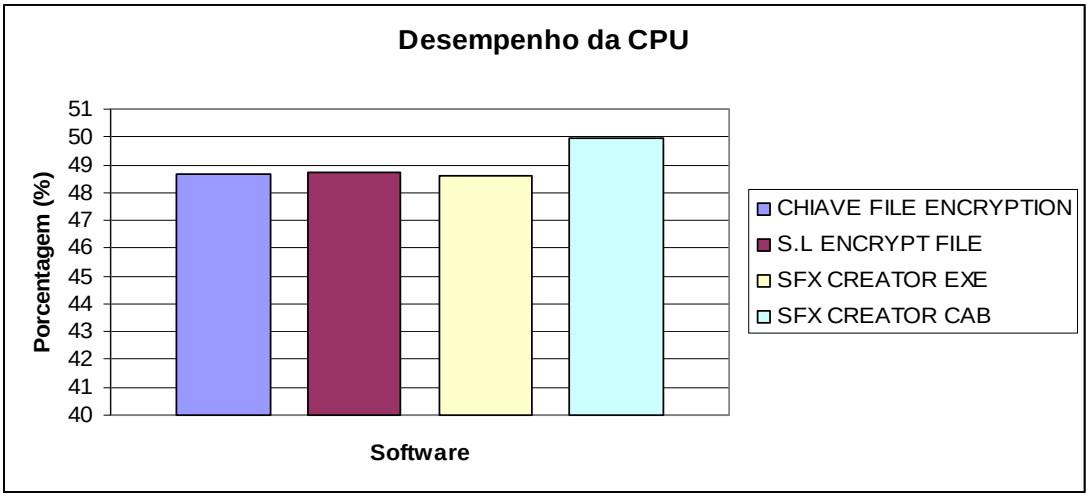

Gráfico 5 - Desempenho da CPU utilizadas pelos softwares

Já a memória utilizada sofreu uma variação maior e o Gráfico 7 mostra a media de memória utilizada por cada software. O Chiave File Encryption foi o que mais utilizou a memória cerca de 20 MB quase 7 vezes mais que o

segundo colocado. Entretanto a memória utilizada por eles representam um baixo custo em relação das memórias disponíveis atualmente no mercado que passam de 32 GB.

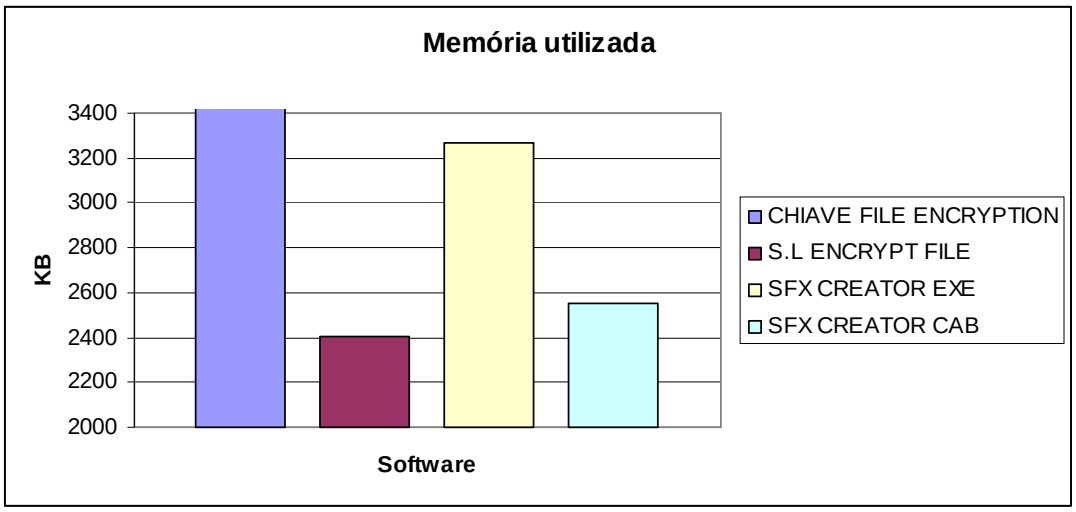

Gráfico 6 - Memória utilizada pelos softwares

5 Considerações finais

Para o levantamento teórico do presente trabalho foram estudas as principais criptografias simétricas e assimétricas, bem como as cifras de substituição e transposição que são as bases para as novas criptografias.

Depois de realizado o levantamento bibliografia, foram escolhidos três softwares freeware que possuíam como base a criptografia AES, criptografia padrão nos EUA, para a realização dos testes.

Os testes realizados por esses softwares utilizaram um único computador e aplicaram dois tamanhos de chaves: 128 e 256 bits em quatro tipos de arquivos: música, imagem, documentos e filme e por fim estes tipos de arquivos foram unidos transformando em um arquivo “todos”.

Com os testes concluídos, podemos verificar que o Software SFX Creator alcançou o melhor desempenho em todos os testes, conseguindo atingir o melhor tempo. O S.L Encrypt File conseguiu o segundo lugar superando o Chiave File Encryption em sete testes dos dez realizados quando utilizando a chave de 128 bits e em seis quando a chave foi dobrada.

O SFX Creator junto com o S.L Encrypt possui a desvantagem no momento da escolha dos arquivos, pois só é permitido a escolha de um arquivo para a realização tanto da criptografia como a decriptografia, necessitando assim fazer uma compactação ou outra forma para transformar estes arquivos em um.

Ao contrario do Chiave File Encryption que permite ao usuário escolher vários arquivos de uma única vez, além de oferecer a opção de apagar os arquivos originais após a criptografia, acrescentando assim segurança e praticidade para o utilizador.

Finalmente, como contribuição acadêmica, espera-se que este trabalho desperte o interesse de outros acadêmicos pelo tema criptografia e leve-os a dar continuidade aos testes realizados, escolhendo outras criptografias para que assim haja uma comparação com a criptografia AES.

6 Referência Bibliográfica

BENITS, Waldyr Dias. **Sistemas Criptográficos baseados em identidades pessoais**. São Paulo, 2003.Disponível em: http://www.ime.usp.br/dcc/posgrad/teses/benits.pdf . Acesso em: 15 mar 2011

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança: o guia oficial RSA**. 1ª ed. Rio de janeiro: Campus Ltda., 2002.

DOMINGUES, M.; HEUBEL, M.T.C.D.; ABEL, I.J.; **Base metodológica para o trabalho científico para alunos iniciantes.** Bauru, São Paulo: Edusc, 2003. 188p.

FLORIANO, Guilerme Martinez. **Camouflaged security system: protótipo de software que emprega técnicas de criptografia, assinatura digital e esteganografia paracomunicacao segura**. Porto Alegre, 2007. Disponível em: < http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k7-2/GuilhermeMartinezFloriano.pdf>. Acesso em: 03 mar 2011

GARFINKEL, Simson; SPAFFORD, Gene. **Comércio & Segurança na Web – Riscos, Tecnologias e Estratégias**. São Paulo: Market Press, 1999

MENDES, Aliane V. **Estudo de Criptografia com chave pública baseada em curvas elípticas.** Montes Carlos, 2007. Disponível em: < http://www.ccet.unimontes.br/arquivos/monografias/261.pdf >. Acessado em: 15 mar 2011

SCHNEIER, Bruce. **Applied Cryptography: protocols, algorithms, and source code in C**. 2ª ed. New Jersey: Wiley, 1996

STALLINGS, William. **Criptografia e segurança de redes**. 4ª ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew S. **Redes de computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003

TKOTZ, Vicktoria. **Criptografia – Segredos embalados para viagem**. 1ª ed: São Paulo: Novatec, 2005.