Um novo modelo de criptografia simétrica

Ana Kelly de Souza Francisco[1], **Barbara Castro Diniz**[2],
Manoel Victor Ribeiro[3], **Raquel Veloso Guimarães**[4]

[1]Instituto Federal de Educação, Ciência e Tecnologia – Campus Rio Verde (IF Goiano)
Rio Verde, GO – Brasil

Resumo. *Criptografia é a técnica de transformar um texto claro em uma mensagem imcompreensível. Existe dois tipos de criptogria: criptografia simétrica e criptografia assimétrica. Este trabalho abordará uma nova idéia de um algoritmo simétrico. A criptografia está diretamente ligada á segurança digital, pois é utilizando-a que obtém-se mecanismos para proteger a informação desejada.*

1. Introdução

A criptografia surgiu da necessidade de guardar informações em segredo, seja devido à guerras ou a transações econômicas. Aliada à diplomacia, ela foi aperfeiçoada na medida em que segredos de guerra significavam vantagens táticas capazes de garantir que um dos lados saísse vencedor. A motivação para o desenvolvimento de técnicas para mascarar uma mensagem, desenvolver códigos e cifras surgiu da necessidade de garantir que apenas um destinatário específico fosse capaz de decifrar uma mensagem. Ao longo da história as nações compreenderam a importância da segurança da informação criando departamentos especializados em criar sistemas criptográficos ou em quebrá-los. Códigos foram capazes de decidir resultados de batalhas e ainda hoje cumprem um papel ainda maior na sociedade, indo além de questões militares e recebendo o status de ciência.

2. História da criptografia

2.1. Scytale

Já utilizado a mais de 2500 anos atrás e é conhecido como o método de cifra militar mais antigo que existe. Em 404 A.C. O cinto era composto por tiras de couro com letras escritas do lado avesso. Parecia uma sequência sem sentido de caracteres, mas quando o pedaço de couro era enrolado em torno de um pedaço de madeira com um diâmetro pré estabelecido, uma mensagem descriptografada poderia ser lida.

2.2. Cifra de César

Foi utilizada por Júlio César no século 1 A.C. Consiste na substituição de uma letra do alfabeto por seu correspondente três casas adiante, ou seja, a letra A é substituída pela letra D, a letra B pela letra E e assim por diante. Neste caso, o algoritmo da cifra é a troca de uma letra por outra em uma determinada posição. E a chave, neste caso, é o número 3.

2.3. Cifra de Vigenère

A cifra de Vigenère, do século XVI,consiste em até 26 alfabetos distintos para criar a mensagem cifrada. O primeiro passo é montar o chamado quadrado de Vigenère, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. Em resumo, o remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante.

2.4. Criptografia na idade contemporânea

A criptografia e, em parte, o próprio computador, surgiram dos esforços dos aliados durante II Guerra Mundial para decifrar os códigos de comunicação usados pelos submarinos da Alemanha nazista.Em 1918 Scherbius desenvolveu a"Enigma", a Marinha alemã interessou-se pela ideia e em 1926 adotou-a como principal meio de comunicação e criptografia ficando conhecida como Funkschlüssel C. Em 1928, a própria Alemanha desenvolveu sua versão, a Enigma G, e passou a ser usada tendo suas chaves trocadas mensalmente o que impossibilitava aos Aliados manterem-se um passo a frente dos alemães.

Foi o matemático Marian Rejewski, polonês, quem deduziu a estrutura da Enigma em 1932, avanço considerado o mais marcante da criptoanálise desde sua invenção concomitantemente com os ingleses, os franco-poloneses atingiram agilidade e precisão na quebra da Enigma. Entre os britânicos personalidades como Allan Turing, Gordon Welchman e Max Newman atuaram decisivamente para a quebra da Enigma. Max Newman e seus colegas projetaram e implementaram o primeiro computador digital eletrônico programável, o Colossus, para ajudar com sua criptoanálise.

Claude Shannon é considerado o pai da criptografia matemática, com o livro Communication Theory of Secrecy Systems no Bell System Technical Journal, publicado em 1949, estudou, analisou e abordou a criptografia utilizada na Segunda Guerra Mundial. Este tabalho é considerado a base teórica para a criptografia e também para grande parte da criptoanálise.

2.5. Os usos da criptografia na atualidade

As aplicações da Criptografia atualmente incluem:

- sigilo em banco de dados;
- censos;
- investigações governamentais;
- dossiês de pessoas sob investigação;
- dados hospitalares;
- informações de crédito pessoal;
- decisões estratégicas empresariais;
- sigilo em comunicação de dados;
- comandos militares;
- mensagens diplomáticas;
- operações bancárias;
- comércio eletrônico;
- transações por troca de documentos eletrônicos (EDI);
- estudo de idiomas desconhecidos;
- recuperação de documentos arqueológicos, hieróglifos;
- e até tentativas de comunicações extraterrestres.

3. Criptografia definição

Há varias definições do termo criptografia, mas basicamente é o estudo das técnicas que utilizamos para nos comunicarmos de forma segura, como mandar uma mensagem aleatória de um emissor para um receptor de forma (na criptografia moderna, esta fórmula é chamada de algoritmo), que uma terceira pessoa não consiga ler essa mesma mensagem, sem que possua uma chave correta. A criptografia, também é um processo que se executa por meio de duas operações semelhantes e diretamente inversas: cifração e decifração.

3.1. Principios da criptografia

Existem três princípios fundamentais , que se não forem atendidos, não estamos falando de uma criptografia.

3.1.1. Confidencialidade

Ninguém consegue ler a mensagem que o emissor está enviando para o receptor.

3.1.2. Integridade

A mensagem que o emissor mandou , tem que ser a mesma mensagem que o receptor recebeu. Tem por fundamento evitar corrupção ou modificação não-autorizada de dados e/ou informações, em todas as suas fases de existência, isto é, geração ou produção, difusão e tramitação, uso, avaliação e destinação final.

3.1.3. Autenticidade

Quando o receptor receber a mensagem , o mesmo tem que ter certeza que essa mensagem foi enviada pelo emissor desejado e não outra pessoa aleatória. Mensagem: registro contendo uma representação digital da informação, como um dado criado, enviado, recebido e guardado em forma eletrônica.

4. Exemplo prático da criptografia no cotidiano

Ao acessar qualquer site por um navegador, por exemplo, google chrome, ao lado da barra de endereço ou link do site, terá um desenho de um cadeado ou não. Sendo assim, haverá três possibilidades que se torna possível verificar a ação da criptografia na pratica. São elas.

1. Acessar o site e não ter nenhum cadeado. Significa que sua conexão não está criptografada ou seja nenhum principio de criptografia está garantido.
2. Ter um cadeado com a cor amarela. Significa que sua conexão está sendo criptografada. Porém o navegador não foi capaz possuir autenticidade, ou seja, ninguém conseguirá interferir em sua conexão. No entanto, o servidor não tem a informação se você está conectando realmente no site desejado.
3. Cadeado com a cor verde. Significa que os três princípios foram atendido e a criptografia está realmente funcionado.

5. A importância da criptografia e a segurança de dados

Na atualidade, as técnicas de criptografias mais conhecidas envolvem o conceito das chaves criptográficas, que são formadas por bits, com base em algarismos com capacidade de interpretar as informaççoes, ou seja, capaz de decodificar. A chave do emissor deve ser compatível com a do receptor, para assim, as informações serem extraídas. Há quatro tipos básicos de aplicações criptográficas, tipicamente usadas para conseguir os objetivos de segurança da informação: criptografia simétrica, ou de chave secreta, criptografia assimétrica, ou de chave pública, função hash criptográfico; e assinatura digital.

6. Privacidade na internet:

Privacidade na internet, é o mesmo que a privacidade no material, deve está resguardado quem fornece e quem recebe dados por este meio, não existindo atalhos que outros, que não estejam nesse ciclo de relacionamento possam usar os dados ali conferidos.

> **Lei nº 12.965 de 23 de Abril de 2014 / Marco Civil da Imternet**
>
> Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
>
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.
>
> § 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Ao se conectar à internet, e acessar os mais diversos sites, o usuário disponibiliza informações pessoais à esses sites. O que poderia gerar uma certa insegurança, tendo em vista que o mesmo poderia ser vitima de crimes cometidos através dos seus dados pessoais. A questão da privacidade está ligada diretamente a segurança e liberdade do usuário. Desse modo, o marco civil da internet no seu art.10 trata dessa questão de privacidade, ao estabelecer que os dados pessoais, as informações de acesso e os registros do usuário devem preservar a intimidade e a vida privada. Não admitindo, assim, a divulgação de dados pessoais de usuários.

6.1. Segurança da Informação

Segurança da Informação é a capacidade de um sistema de informação, uma rede ou um sistema de gestão documental resistir a eventos acidentais e/ou ações ilícitas e/ou maliciosas que possam comprometer as características de dados/informações armazenados, processados ou em trânsito, assim como de serviços relacionados que possam ser oferecidos por esses sistemas [REZENDE 1998].

6.2. Protocolo de segurança

Hoje é importante que todos os dados sensíveis transacionados entre um cliente e um servidor sejam cifrados de modo a que estes não possam ser entendidos por terceiros. Na prática, quando "buscamos" um serviço online que nos solicita dados pessoais ou credenciais de acesso (ex. sites de bancos) é importante que a toda a informação passada seja cifrada de modo a tornar-se ilegível. No caso dos servidor Web (entre outros serviços de uma rede), uma das formas de proceder a cifra dos dados é recorrendo um protocolo de segurança [BORGES et al. 2014].

6.2.1. Protocolo SSL:

O SSL é um protocolo criptográfico baseado em cifras assimétricas (chave privada + chave pública) que tem como principal objectivo providenciar segurança e integridade dos dados transmitidos em redes inseguras como é o caso da Internet. Quando um utilizador acede a um site que recorre ao SSL, o servidor envia ao cliente a chave pública para que esta possa cifrar a informação que vai ser passada ao servidor. Quando o servidor recebe essa informação, usa a sua chave privada para decifrar a informação transmitida pelo cliente. Existem várias aplicações para este protocolo, como por exemplo o comércio electrónico, servidores Web,servidores FTP, etc. Para identificar facilmente se estão a visualizar um site seguro basta verificar no URL que em vez de estar o normal http:// se encontra https://.

6.2.2. Protocolo HTTP:

O HTTP abreviação de Hyper Text Transfer Protocol (Protocolo de Transferência de Hipertexto) é um protocolo de comunicação entre cliente e servidor, nesta comunicação quem faz as solicitações (ou requisições) é o cliente HTTP conhecido também como user agent, que pode ser um browser, um robô (googlebot por exemplo), um script, ou qualquer outro programa que conheça e saiba como seguir o protocolo. Quem atende estas solicitações é o servidor HTTP (ou servidor web), ou seja, quando você digita o endereço de um site em seu navegador web (Internet Explorer, Firefox, Opera, Safari, etc) ele envia uma requisição ao servidor que responde ao cliente que a requisição teve sucesso e o recurso foi encontrado exibindo a página do site.

6.2.3. Protocolo HTTPS:

HTTPS (HyperText Transfer Protocol Secure)é a combinação do protocolo HTTP com o SSL(Secure Sockets Layers, que pode ser traduzido como Camada de Sockets Protegida). É a maneira mais comum atualmente de trafegar documentos via HTTP de maneira segura. Provê encriptação de dados, autenticação de servidor, integridade de mensagem e autenticação de cliente.Com o uso do HTTPS, que é o HTTP seguro, adiciona-se alguns princípios de segurança, como confidencialidade, integridade e autenticação. Por confidencialidade, entende-se que a mensagem só é lida pelo destinatário real da mensagem. A integridade representa que a mensagem não foi alterada e o princípio da autenticação

prova que o servidor é realmente quem diz ser. Nesse artigo, apresenta-se, portanto, os mecanismos utilizados pelo HTTPS para atingir esses três princípios básicos.

6.3. Como funciona a segurança da criptografia

A segurança depende da quantidade de bits, enquanto mais bits, mais segurança criptográfica. Para se referir à segurança, usam-se os termos 64 ou 128 bits para expressar o tamanho da chave, que enquanto maior mais segura. Um algoritmo de oito bits, por exemplo, possui 256 combinações de chaves, que é o resultado de 2 elevados a 8. Assim, se alguém tentar gerar 256 combinações, para decodificar a mensagem, embora seja complicado, é possível. Por isso, quanto maior o número de bits, maior a segurança, que ainda tem as do tipo simétricas e a assimétricas.

7. Tipos de criptografia

A criptografia pode ser feita de duas maneiras, com códigos ou cifras. Os códigos foram as primeiras técnicas de criptografia e são feitas através da troca dos caracteres da mensagem por códigos pré-definidos. As cifras fazem a substituição e/ou transposição na mensagem. Na criptografia de cifras incluem o conceito de chaves e existem dois tipos de algoritmos: os assimétricos e os simétricos [MORENO et al. 2005].

7.1. Criptografia Assimétrica

A criptografia assimétrica é o método que utiliza duas chaves: uma para cifrar e outra para decifrar. A chave para cifrar é pública, ou seja, todos possuem conhecimento dela, qualquer pessoa pode enviar uma mensagem criptografa para outro, desde que saiba su chave pública. Já a chave para de cifrar é privada, somente quem recebe uma mensagem cifrada pode decifrar com a sua chave pública. Esse processo é mais seguro que simétrico em termos de sigilo da chave, já que possui duas chaves, porém possui processos matemáticos mais complexos e com isso os algoritmos assimétricos não são tão eficientes quanto os simétricos.

7.2. Criptografia Simétrica

O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra [OLIVEIRA 2012].

- Vantagem: A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.
- Desvantagem: O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para decifra-mento, ou esta última pode facilmente ser obtida a partir do conhecimento da

primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem.

8. Relação Simetrica

Antes de começarmos a falar sobre relação simétrica, é preciso entender o que é uma relação, e ela pode ser definida da seguinte maneira:

Um conjunto R, é uma relação de A em B (AxB) se e somente se R está contido em AxB. Exemplo:
A = $\{0, 1\}$ e B= $\{2, 4\}$
AxB = $\{(0, 2), (0, 4), (1, 2), (1, 4)\}$
Duvidas que podem surgir:

1. R = Ø é uma relação de A em B? Sim pois o conjunto vazio esta contido em qualquer conjunto.
2. R = $\{(0, 4), (1, 4)\}$ é uma relação de A em B? Sim pois todos os elementos de R estão em AxB, ou seja R $\subset$ AxB.
3. R = $\{(1, 2)\}$ é uma relação de A em B? Sim pois todos os elementos de R estão em AxB, ou seja R $\subset$ AxB.
   Agora que compreendemos o conceito de relação, podemos entender melhor o que é uma relação simétrica. Seja R uma relação de A em A, (R $\subset$ AxA), dizemos que R é SIMÉTRICA se dado (x,y) $\in$ R, então (y,x) $\in$ R.

Se para quaisquer que sejam x, y $\in$ A, tem-se :

$$xRy \rightarrow yRx$$

ou seja se tem na relação (x,y) tem que ter o contrário (y,x) para ser simétrica [SCHNEIDER 2003].
Exemplo:
A = $\{a, b, c\}$
R = $\{(a, b), (a, a), (b, a), (c, c)\}$ é simétrica pois o contrário de cada elemento da relação existe.
S = $\{(a, b)\}$ não é simétrica pois deveria ter (b,a) o contrário na relação
T = $\{(a, b), (b, a)\}$ é simétrica [de AMORIM 2009].

9. Cifras de Substituiçao Simples

Em criptografia, uma cifra de substituição é um método de criptografia que opera de acordo com um sistema pré-definido de substituição. Para criptografar uma mensagem, unidades do texto - que podem ser letras isoladas, pares ou outros grupos de letras - são substituídas para formar a cifra. As cifras de substituição são decifradas pela substituição inversa.

Uma substituição simples pode ser expressa escrevendo o alfabeto numa ordem diferente, que se designa alfabeto de substituição. Pode ser deslocado de um passo fixo (como na cifra ROT13, exemplo de uma cifra de César) ou baralhado de forma mais complexa[CORMEN 2015].

É habitual que se escolha uma palavra fácil de lembrar e sem letras repetidas para que se inicie o alfabeto de cifragem por ela, e completando-o com as letras não usadas. Por exemplo, com a chave 'PORTUGAL' teremos os seguintes alfabetos:

- Alfabeto normal: abcdefghijklmnopqrstuvwxyz
- Alfabeto para a cifragem: PORTUGALBCDEFHIJKMNQSVWXYZ

Assim, a mensagem Fujam todos depressa! Fomos descobertos! é cifrada para
GSCPF QITIN TUJMUNNP! GIFIN TUNRIOUMQIN!

Tradicionalmente, o texto cifrado é escrito em blocos de comprimento fixo (''grupos'') sem pontuação nem espaços para que não se perceba o comprimento das palavras individuais. O mais comum são grupos de cinco letras, muito usados nos tempos do telégrafo. Assim a mensagem cifrada seria:

GSCPF QITIN TUJMU NNPGI FINTU NRIOU MQIN

Uma desvantagem deste método é que as últimas letras do alfabeto (que geralmente têem menos frequência de uso) tendem a ficar no fim.

10. Principais Algoritmos de criptografia simétrica

Os principais algoritmos de criptografia simétrica são: DES, 3DES, AES, RC4 e IDEA.

10.1. Data Encryption Standard: DES

DES é tipo de cifra em bloco, ou seja, um algoritmo que toma uma string de tamanho fixo de um texto plano e a transforma, através de uma série de complicadas operações, em um texto cifrado de mesmo tamanho. No caso do DES, o tamanho do bloco é 64 bits. DES também usa uma chave para personalizar a transformação, de modo que a descriptografia somente seria possível, teoricamente, por aqueles que conhecem a chave particular utilizada para criptografar. A chave consiste nominalmente de 64 bits, porém somente 56 deles são realmente utilizados pelo algoritmo. Os oito bits restantes são utilizados para checar a paridade e depois são descartados, portanto o tamanho efetivo da chave é de 56 bits, e assim é citado o tamanho de sua chave [da Rede 2010].

Criado pela IBM em 1977, usa criptografia de 56 bits, o que corresponde a cerca de 72 quadrilhões de chaves diferentes. Apesar de ser um valor bastante alto, foi quebrado por em 1997 por força bruta (tentativa e erro), em um desafio feito na Internet.

10.2. Triple Data Encryption Standard: 3DES

O 3DES(Triplo DES), sigla para Triple Data Encryption Standard é um padrão de criptografia baseado no algoritmo de criptografia DES adotado como padrão em 1977. 3DES usa 3 chaves de 64 bits (o tamanho máximo da chave é de 192 bits, embora o comprimento atual seja de 56 bits). Os dados são encriptados com a primeira chave, decriptado com a segunda chave e finalmente encriptado novamente com a terceira chave. Isto faz do 3DES ser mais lento que o DES original, mas oferece maior segurança. Em vez de 3 chaves, podem ser utilizadas apenas 2, fazendo-se K1 = K3 [da Rede 2010].

10.3. International Data Encryption Algorithm: IDEA

O *International Data Encryption Algorithm (IDEA)* foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo [OLIVEIRA 2012].

Assim como o DES, o IDEA é um algoritmo de criptografia simétrica, ou seja, utiliza a mesma chave para cifrar e decifrar o texto. Como foi desenvolvido para substituir o DES, o IDEA proporciona um maior nível de segurança e também maior velocidade que o DES.

10.4. Advanced Encryption Standard: AES

O algoritmo *AES(Advanced Encryption Standard)* foi uma proposta para substituir o DES, que era o modelo padrão de criptografia usado mundialmente até 1997. Em setembro daquele ano, a agência decide por abrir uma chamada pública por novos algoritmos, devendo estes suportarem blocos de tamanho de 128 bits, e chaves de 128, 192 e 256 bits. Inicialmente, a chamada também exigia que o novo padrão suportasse blocos de tamanho de 192 e 256 bits, porém este requisito foi retirado logo antes da publicação da chamada. Apesar disso, algumas propostas mantiveram este suporte, como uma funcionalidade extra, tal como RC6 e *Rijndael*(AES). Em outubro de 2000 o veio a público o anuncio de que o AES sem nenhuma modificação seria sucessor do DES [RINALDI 2012].

No AES o numero de rodadas depende do tamanho da chave, sendo Nr igual a 10, 12 e 14, para Nk igual a 4, 6 e 8, respectivamente. O algoritmo possui uma chave principal e, a partir dela, são geradas Nr + 1 chaves, geralmente chamadas de chaves de rodada, pois cada uma será usada em uma rodada diferente. Além disso, a própria chave principal é usada antes da primeira rodada. A chave principal é alocada em uma matriz de 4 linhas e Nk colunas, e cada chave de rodada é agrupada da mesma maneira que o bloco de dados [da Rede 2010].

Em cada etapa, são executados substituições e transposições, essas são:

- Substituição de bytes (*byte substitution*);
- Permutação de bytes entre grupos (*shift rows*);
- Substituição usando matrizes dos grupos (*mix collumns*);
- Execução de um XOR com a chave (*add round key*);

10.5. RC4

Em 1987 Ron Rivest desenvolveu o algoritmo RC4 para a empresa *RSA Data Security*, Inc., líder mundial em algoritmos de criptografia. Foi, durante tempos, um segredo comercial muito bem guardado, muito popular, e utilizado largamente em software, como *Lotus Notes, Apple Computer's AOCE, Oracle Secure SQL, Internet Explorer, Netscape* e *Adobe Acrobat* [da Rede 2010].

As transformações neste algoritmo são lineares, não são necessários cálculos complexos, já que o sistema funciona basicamente por permutações e somas de valores in-

teiros, o que torna este algoritmo muito simples e rápido, um raro exemplo de *Barato, Rápido e Bom*.

Em criptografia, RC4 (ou ARC4) é o algoritmo de criptografia de fluxo mais usado no software e utilizado nos protocolos mais conhecidos, como Secure Socket Layers (SSL) (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios. RC4 não é considerado um dos melhores sistemas criptográficos pelos adeptos da criptografia, e em algumas aplicações podem converter-se em sistemas muito inseguros. No entanto, alguns sistemas baseados em RC4 são seguros o bastante num contexto prático [da Rede 2010].

11. Uma nova chave simétrica

O algoritmo a ser apresentado é uma ideia simples de uma chave simétrica, onde são feitas várias operações a nível de bits.

11.1. Cifragem

A seguir estão os passos para a cifragem de um byte;

1. Gerar o valor ASCII do caractere;
2. Gerar o valor binário correspondente;
3. Inverter o número binário de 8 dígitos;
4. Escolher um divisor de 4 dígitos ($>= 1000$) como a chave;
5. Dividir o número invertido com o divisor;
6. Armazenar o restante nos 3 primeiros dígitos e quociente nos próximos 5 (O restante e o quociente não seriam mais do que 3 dígitos e 5 dígitos, respectivamente. Se qualquer um destes for inferior a 3 e 5 respectivamente, precisamos adicionar o número necessário de 0s (zeros) em O lado esquerdo. Portanto, este seria o ciper-text i.e. criptografado texto. Agora armazene o restante nos primeiros 3 dígitos e quociente nos próximos 5 dígitos.

11.1.1. Exemplo

Usando o caracter ”T”, de acordo com os passos acima:

1. O valor do ”T”na tabela ASCII é 84 em decimal;
2. O binário de 84 é 1010100. Caso o número não tenho 8 bits, é preciso fazer com que ele tenha 8 bits, para isso é só preencher com 0’s à esquerda. O binário será 01010100;
3. Inverter o binário, o binário invertido é 00101010;
4. Escolher uma chave. Nesse caso a chave escolhida foi 1000;
5. Dividir o binário invertido pela chave;
6. O resto da divisão é 10, e o quociente é 101. A mensagem cifrada seŕa 01000101, que é 69 em decimal e o caractere ”E”da tabela ASCII.

11.2. Decifragem

Para decifrar é só fazer o caminho inverso:

1. Multiplicar os últimos 5 dígitos do texto cifrado pela chave;

2. Adicione os primeiros 3 dígitos do texto cifrado com o resultado produzido no passo anterior;
3. Se o resultado produzido no passo anterior o passo 2 não for um número de 8 bits, precisamos fazer dele um número de 8 bits;
4. inverter o número para obter o texto original;

11.3. Análise do algoritmo

O algoritmo conta com uma chave de 4 bits, o que é um número muito pequeno, já que nos deixa com 2^4 combinações de chaves. Esse tamanho de chave não garante a segurança de uma grade quantidade de informações, pois a segurança de um algoritmo de criptografia está diretamente ligada ao tamanho da chave e também ao tamanho do bloco cifrado. No caso desse algoritmo o tamanho do bloco cifrado é 1 *byte*, o que corresponde à 8 bits.

As operações utilizadas no processo de cifragem são bastante interessantes e que ajudam a segurança do algoritmo, como por exemplo o ato de inverter o número binário, isso transforma em outro caractere. No caso de serem utilizadas para uma quantidade pequena de informação, o algoritmo pode funcionar muito bem. Como todo algoritmo simétrico, todas as operações feitas são facilmente reversíveis.

11.4. Vantagens desse algoritmo

O algoritmo é de natureza simples, e apesar disso tem duas operações reversas o que o torna mais seguro. A verificação do CRC (Cyclic Redundancy Check) termina mais rápido. Para uma pequena quantidade de dados esse algoritmo funciona bem [AYUSHI 2010].

12. Conclusão

O estudo da criptografia atualmente é muito importante, pois a criptografia é uma das ações feitas para garantir a segurança em diversas outras ações que praticamos, desde transações bancárias à mensagens trocadas no *whatsApp*. A criptografia simétrica possui vantagem em ser estudada, por ter uma premissa de operações matemáticas mais simples, já que utiliza apenas uma chave, isso faz com que o custo computacional seja menor que o da criptografia assimétrica e que os algoritmos simétricos sejam mais eficientes. Essa nova proposta de algoritmo simétrico criptografa um *byte* por vez, ou seja, o tamanho do bloco a ser criptografado é de 1 *byte*, seria interessante se pensar em blocos de textos maiores e tamanhos de chave maiores, pois a segurança da criptografia simétrica está nas chaves e no blocos, quanto maior for o tamanho destes, maior número de combinações entre eles e com isso maior segurança. Com esses estudos poderia ser estudo a fundo e testado a segurança desse algoritmo.

Referências

AYUSHI, A. (2010). Symmetric key cryptographic algorithm.

BORGES, F., Fagundes, B. A., and CUNHA, G. N. d. (2014). Vpn: Protocolos e segurança.

CORMEN, T. (2015). *Desmistificando algoritmos*, volume 1. Elsevier Brasil.

da Rede, T. (2010). Algoritmos de criptografia (des, 3des, aes, rc4).

de AMORIM, T. S. (2009). Discutindo as relacoes (relacoes entre conjuntos) 01.

MORENO, E. D., PEREIRA, F. D., and CHIARAMONTE, R. B. (2005). Criptografia em software e hardware. *São Paulo: Novatec*.

OLIVEIRA, R. R. (2012). Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, 31:11–15.

REZENDE, P. A. D. (1998). Criptografia e segurança na informática. *Apostila-Capítulos*, 1(2):3.

RINALDI, G. D. (2012). Análise do aes e sua criptoanálise diferencial.

SCHNEIDER, E. R. (2003). *Matemática Discreta - Uma Introdução*. Thomson, 1 ed edition.