ANÁLISE DO ALGORITMO VENCEDOR DO AES: O RIJNDAEL

Rafael Antonio da Silva Rosa (IC)
Instituto Tecnológico de Aeronáutica (ITA)
Pça. Mal. Eduardo Gomes, 50, Vila das Acácias, 12228-901, S. José dos Campos – SP
rafael04ita@yahoo.com.br

Antonio Cândido Faleiros (PQ)
Instituto Tecnológico de Aeronáutica (ITA)
Divisão de Ensino Fundamental
faleiros@ief.ita.br

RESUMO

Em 1997, o National Institute of Standards and Technology (NIST) iniciou um processo para selecionar um algoritmo de criptografia de chave simétrica a ser usado para proteger informações Federais devido às suas responsabilidades estatutárias. Em 1998, o NIST anunciou a aceitação de quinze algoritmos candidatos e pediu ajuda da comunidade de pesquisa criptográfica para analisar os candidatos. O NIST revisou os resultados desta pesquisa preliminar e selecionou cinco finalistas. Tendo revisado a análise pública adicional dos finalistas, o NIST decidiu indicar o Rijndael como o Advanced Encryption Standard (AES). Uma análise deste algoritmo é feita neste artigo.

ABSTRACT

In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive Federal information in furtherance of NIST´s statutory responsibilities. In 1998, NIST announced the acceptance of fifteen candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. NIST reviewes the results of this preliminary research and selected five finalists. Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael as the Advanced Encryption Standard (AES). An analysis of this algorithm is done in this paper.

1. O CONCURSO AES

Desde a Segunda Grande Guerra Mundial, a Criptografia eletrônica passou a ser utilizada, mas só a partir de 1974 que o primeiro algoritmo criptográfico foi usado de forma comercial. O *Lucifer* foi desenvolvido pela IBM e, depois de várias alterações realizadas pela NSA (*National Security Agency*) passou a ser chamado de DES (*Data Encryption Standard*), sendo usado então como padrão criptográfico americano.

Especialistas haviam dito que o algoritmo tinha sido muito bem projetado e que para "quebrá-lo" seria necessário a construção de uma máquina específica e muito cara. Mas, apesar de seu uso ser originalmente previsto até 1982, só após um período de cerca de 20 anos de uso do DES, estabeleceu-se que esse algoritmo continuaria como padrão até 1998, quando seria escolhido seu substituto.

E em janeiro de 1997, o NIST (*National Institute of Standards and Technology*), que veio substituir o NSA, anunciou o início dos trabalhos de desenvolvimento do AES (*Advanced Encryption Standard*) e, em setembro do mesmo ano, fez uma chamada oficial para proposta de novos algoritmos para substituir o DES, definindo que os algoritmos que fossem submetidos à avaliação seriam divulgados publicamente, com direitos autorais livres,

e que os algoritmos deveriam ser simétricos suportando blocos de 128 bits e chaves de 128, 192 e 256 bits.

Em agosto de 1998, o NIST apresentou um grupo de 15 algoritmos na Primeira Conferência dos Candidatos AES: Cast-256, Crypton, Deal, DFC, E2, Frog, HPC, LOKI97, Magenta, MARS, RC6, Rijndael, Safer+, Serpent e Twofish. Nesta conferência e em uma publicação simultânea, o NIST solicitou comentários públicos sobre os candidatos, submetendo-os a membros da comunidade criptográfica mundial.

Na Segunda Conferência dos Candidatos AES, em março de 1999, discutiu-se os resultados das análises dos algoritmos candidatos, e através dos comentários recebidos, o NIST selecionou 5 finalistas entre os 15: MARS, RC6, Rijndael, Serpent e Twofish.

Estes 5 algoritmos sofreram análises adicionais e, no final dessa etapa, o NIST realizou a Terceira Conferência dos Candidatos AES em Nova Yorque, onde os criadores dos algoritmos foram convidados a participar das discussões, responder críticas e comentar o seu candidato. Além disso, foi disponibilizado um fórum de discussões públicas da análise dos finalistas do AES.

O NIST iniciou em maio de 2000 a análise de todas as informações disponíveis para selecionar o algoritmo vencedor. E finalmente, em 2 de outubro do mesmo ano, foi anunciado como algoritmo selecionado o Rijndael.

2. O ALGORITMO RIJNDAEL

O programa criptográfico Rijndael (sua nomeação tem origem do nome de seus criadores: Vincent Rijmen e Joan Daemen) foi projetado para usar somente simples operações de bytes completos. Também, fornece flexibilidades a mais da requerida de um candidato ao AES, como o tamanho da chave e do bloco que podem ser escolhidos entre 128, 192, ou 256 bits. E o Rijndael é em muitos aspectos um programa relativamente simples.

O Rijndael tem um número variável de “rounds”. Não contando um “round” extra executado ao término da cifragem como um passo omitido, o número de “rounds” do Rijndael é:

- 9 se o bloco e a chave forem de 128 bits;
- 11 se o bloco ou a chave forem de 192 bits, e nenhum deles for maior que isso;
- 13 se o bloco ou a chave forem de 256 bits.

Para criptografar um bloco de dados com o Rijndael, é executado primeiro um passo “Add Round Key” (fazendo uma lógica XOR entre uma sub-chave e o bloco), os “rounds” regulares notados acima, e como já notado, o “round” final com o passo “Mix Column”, como descrito abaixo, omitido.

Cada “round” regular envolve quatro passos. O primeiro é o passo “Byte Sub”, onde cada byte do bloco é trocado por seu substituto em uma “S-box”.

A especificação do Rijndael só fornece uma explicação de como a “S-box” foi calculada: o primeiro passo é substituir cada byte pelo seu recíproco no mesmo Corpo de Galois GF(2^8) como usado abaixo no passo “Mix Column”, a não ser o 0 que não possui nenhum recíproco, e que é substituído por ele mesmo; então uma matriz módulo dois é multiplicada, e finalmente o número hexadecimal 63 (não C6) é somado com o resultado (lógica XOR).

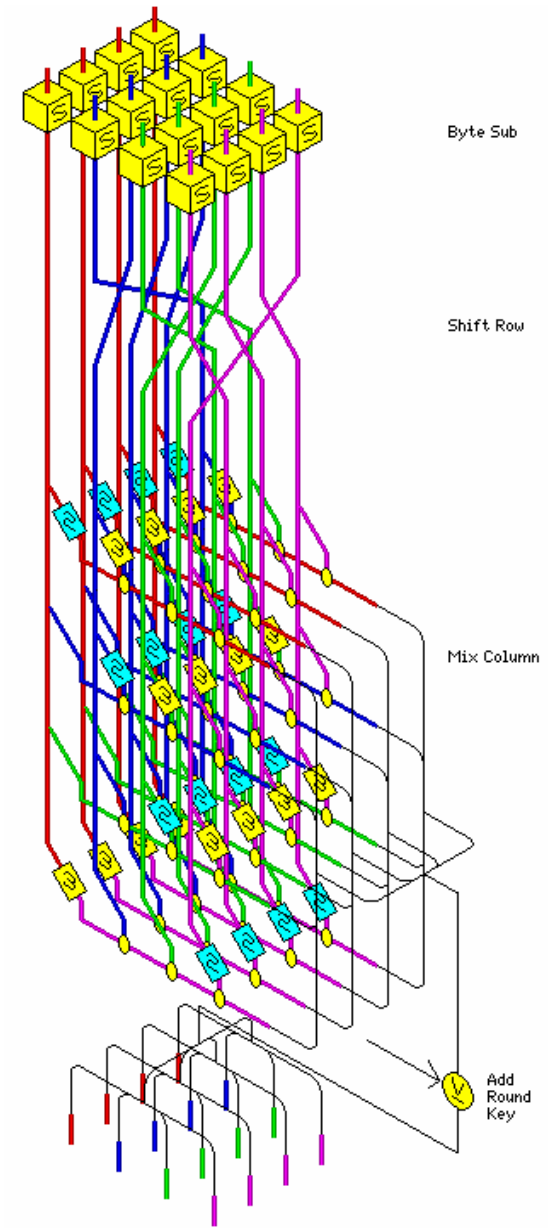

Figura 1: Diagrama Tridimensional dos Passos do Rijndael.

A “S-box” é:

```
 99 124 119 123 242 107 111 197
 48   1 103  43 254 215 171 118
202 130 201 125 250  89  71 240
173 212 162 175 156 164 114 192
183 253 147  38  54  63 247 204
 52 165 229 241 113 216  49  21
  4 199  35 195  24 150   5 154
  7  18 128 226 235  39 178 117
  9 131  44  26  27 110  90 160
 82  59 214 179  41 227  47 132
 83 209   0 237  32 252 177  91
106 203 190  57  74  76  88 207
208 239 170 251  67  77  51 133
```

```
 69 249   2 127  80  60 159 168
 81 163  64 143 146 157  56 245
188 182 218  33  16 255 243 210
205  12  19 236  95 151  68  23
196 167 126  61 100  93  25 115
 96 129  79 220  34  42 144 136
 70 238 184  20 222  94  11 219
224  50  58  10  73   6  36  92
194 211 172  98 145 149 228 121
231 200  55 109 141 213  78 169
108  86 244 234 101 122 174   8
186 120  37  46  28 166 180 198
232 221 116  31  75 189 139 138
112  62 181 102  72   3 246  14
 97  53  87 185 134 193  29 158
225 248 152  17 105 217 142 148
155  30 135 233 206  85  40 223
140 161 137  13 191 230  66 104
 65 153  45  15 176  84 187  22
```

Note que 63 em hexadecimal são 3 mais 6x16, e isso é 99, como começa a tabela.

O próximo passo é o "Shift Row". Considerando o bloco sendo composto dos bytes 1 a 16, estes bytes são organizados em uma matriz, e trocados como se segue:

de para

```
 1  5  9 13      1  5  9 13
 2  6 10 14      6 10 14  2
 3  7 11 15     11 15  3  7
 4  8 12 16     16  4  8 12
```

Os blocos que possuem 192 e 256 bits são trocados assim:

de para

```
 1  5  9 13 17 21      1  5  9 13 17 21
 2  6 10 14 18 22      6 10 14 18 22  2
 3  7 11 15 19 23     11 15 19 23  3  7
 4  8 12 16 20 24     16 20 24  4  8 12
```

e

de para

```
 1  5  9 13 17 21 25 29      1  5  9 13 17 21 25 29
 2  6 10 14 18 22 26 30      6 10 14 18 22 26 30  2
 3  7 11 15 19 23 27 31     15 19 23 27 31  3  7 11
 4  8 12 16 20 24 28 32     20 24 28 32  4  8 12 16
```

Note que no caso de 256 bits, as linhas são rotacionadas 1, 3, e 4 posições à esquerda, em vez de 1, 2, e 3 posições como nos outros dois tamanhos de bloco.

Em seguida vem o passo "Mix Column". Uma multiplicação de matriz é executada: cada coluna, no arranjo visto acima, é multiplicado pela matriz:

```
2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
```

Porém, esta multiplicação é feita no GF(2^8). Isto significa que os bytes que são multiplicados são tratados como polinômios em lugar de números. Assim, um byte "multiplicado" por 3 é aquele byte somado (lógica XOR) com o próprio byte "shiftado" uma vez à esquerda.

Se o resultado tiver mais de 8 bits, os bits extras não são simplesmente descartados: ao invés, eles são cancelados pela soma (lógica XOR) do número binário de 9 bits 100011011 com o resultado ("shiftado" à direita se necessário). Este número representa o *polinômio gerador* da versão particular do GF(2^8) usado.

Por exemplo, a multiplicação do número binário 11001010 por 3 neste Corpo de Galois, é da seguinte forma:

```
  11001010
*        11
 ---------
 11001010
  11001010
 ---------
 101011110    (XOR ao invés de adição)
 100011011    (é feito este XOR, ao invés de subtrair 256)
 ---------
   1000101
```

O passo final é o "Add Round Key". Que é simplesmente uma lógica XOR com uma sub-chave do "round" atual.

O "round" final extra omite o passo "Mix Column", mas é como um "round" regular.

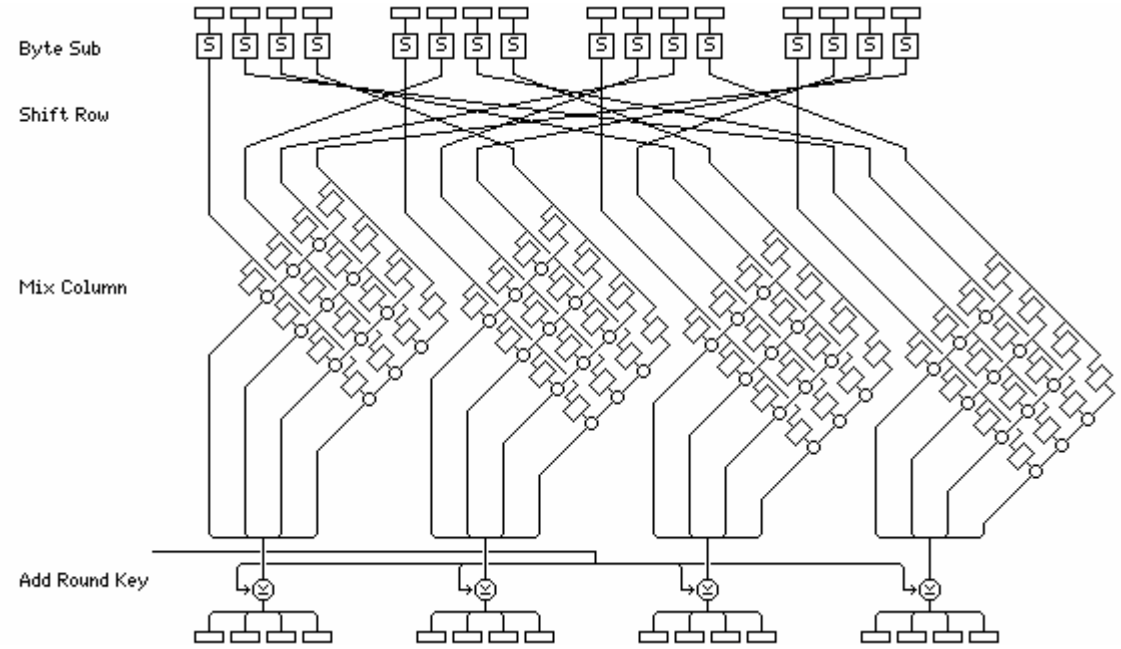

Figura 2: Diagrama dos Passos do Rijndael.

Essa sucessão de operações também é importante para facilitar a decifragem, que é feita por um programa diferente. Cada passo possui sem passo inverso, a não ser o "Add Round Key", cujo inverso é ele mesmo. O inverso do "Shift Row" é rotacionar as linhas ao contrário; o inverso do "Byte Sub" utiliza uma outra matriz (tabela); e o "Mix Column" utiliza a matriz inversa no GF(2^8):

```
14 11 13  9
 9 14 11 13
13  9 14 11
11 13  9 14
```

AGRADECIMENTOS

O autor agradece ao ITA e ao CNPq por todo o apoio fornecido; à Professora Tania Nunes Rabelo pela ajuda e pelo acompanhamento neste trabalho; e principalmente ao seu Professor Orientador Antonio Cândido Faleiros por todo seu apoio, sua transmissão de experiências, sua compreensão, seu companheirismo e sua engrandecedora amizade cultivada nesses dois anos sem iguais de bolsa de iniciação científica e de vida.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Carvalho, D.B.; *Segurança de Dados com Criptografia: Métodos e Algoritmos*; Book Express; **2000**.
2. Stinson, D.R.; *Cryptography: Theory and Practice*; CRC Press; **1995**.
3. Terada, R.; *Segurança de Dados: Criptografia em Redes de Computadores*; Editora Edgard Blücher Ltda; **2000**.
4. NIST, National Institute of Standards and Technology; *Advanced Encryption Standard*; Gaithersburg; **2000**.
5. Ribeiro, V. G.; *Um estudo sobre métodos de pesquisa utilizados em segurança computacional – criptografia*; PPGC da UFRGS; **2000**.
6. Stallings, W.; *Cryptography and network security: principles and practice*; Prentice-Hall; **1999**.