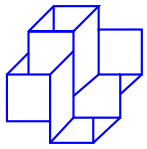
Descrição do Criptossistema AES

Raquel de Araújo de Souza
Fábio Borges de Oliveira
Laboratório Nacional de Computação Científica
{rasouza,borges}@lncc.br



1. Introdução

Em 1997, o NIST *(National Institute of Standards and Technology)* lançou um concurso para adotar o novo algoritmo de criptografia simétrica, que passaria a se chamar AES *(Advanced Encryption Standard)*, para proteger dados confidenciais dos EUA. O algoritmo deveria atender a alguns requisitos como: direitos autorais livres; maior rapidez em relação ao 3DES; cifrar em blocos de 128 bits com chaves de 128, 192 e 256 bits; possibilidade de implementação em software e hardware etc. Em 2000, após análises de especialistas na área de criptografia, é conhecido o vencedor: Rijndael. O algoritmo foi criado pelos belgas Vincent Rijmen e Joan Daemen [Daemen and Rijmen 2002].

2. Estrutura

Estado é a matriz de bytes que iremos manipular entre as diversas rodadas, ou *rounds*. O estado é composto de 4 linhas e *Nb* colunas, onde *Nb* é o número de bits do bloco dividido por 32. A chave é agrupada da mesma maneira que o bloco de dados, com número de colunas *Nk*. O número de rodadas que serão utilizadas durante a execução do algoritmo é denotado por *Nr*, sendo igual a 10, 12 e 14, para *Nk* igual a 4, 6 e 8, respectivamente. A cada rodada do algoritmo de cifragem, realizamos 4 etapas:

SubBytes - Cada byte do estado é substituído por outro em uma S-box (caixa de substituição).

a6	72	c1	f7
45	00	35	d4
82	fc	e6	50
be	15	09	99

$\xrightarrow{SubBytes}$

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

Tabela 1: Exemplo da transformação SubBytes

A inversa da operação SubBytes chama-se **InvSubBytes**, e usa uma S-box inversa. Por exemplo, aplicando a S-box no valor a6, obtemos o valor 24. Então, aplicando a S-box inversa em 24 obtemos o valor a6.

ShiftRows - Consiste em rotacionar à esquerda as linhas do estado, trocando assim a posição dos bytes.

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

$\xrightarrow{ShiftRows}$

24	40	78	68
63	96	48	6e
8e	53	13	b0
ee	ae	59	01

Tabela 2: Exemplo da transformação ShiftRows

A inversa correspondente chama-se **InvShiftRows** e consiste em um rotacionamento similar àquele feito na operação de cifragem, porém à direita.

MixColumns - Nesta etapa, os bytes do estado são tratadas como polinômios sobre o corpo finito $GF(2^8)$ [Klima et al. 2000]. Podemos representar essa transformação por uma multiplicação de matrizes (denotada por $\odot$), onde S é o estado inicial e S' o estado após a transformação.

$$\begin{bmatrix} S'_{1,1} & S'_{1,2} & S'_{1,3} & S'_{1,4} \\ S'_{2,1} & S'_{2,2} & S'_{2,3} & S'_{2,4} \\ S'_{3,1} & S'_{3,2} & S'_{3,3} & S'_{3,4} \\ S'_{4,1} & S'_{4,2} & S'_{4,3} & S'_{4,4} \end{bmatrix} =$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \odot \begin{bmatrix} S_{1,1} & S_{1,2} & S_{1,3} & S_{1,4} \\ S_{2,1} & S_{2,2} & S_{2,3} & S_{2,4} \\ S_{3,1} & S_{3,2} & S_{3,3} & S_{3,4} \\ S_{4,1} & S_{4,2} & S_{4,3} & S_{4,4} \end{bmatrix}$$

Sua inversa, denominada **InvMixColumns**, consiste em uma multiplicação usando a matriz inversa de C, que é a matriz $\mathbf{B} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix}$. Na última rodada, a operação MixColumns é suprimida.

AddRoundKey - É uma operação de XOR entre o estado e a chave de rodada (gerada a partir da chave principal através da *Geração de Chaves*). O XOR é feito byte a byte, ou seja, se $s_{x,y}$ é um byte do estado e $k_{x,y}$ um byte da chave, temos que o byte $s'_{x,y}$ do novo estado é igual a $s_{x,y} \oplus k_{x,y}$. AddRoundKey é sua própria inversa.

3. Conclusões

Esse trabalho apresentou o algoritmo que é o atual padrão de criptografia dos EUA, descrevendo suas etapas. O algoritmo usa uma caixa de substituição (S-box), rotações, a operação de XOR, multiplicação de matrizes, e trabalha sobre o corpo finito $GF(2^8)$.

Referências

Daemen, J. and Rijmen, V. (2002). *The design of Rijndael: AES — The Advanced Encryption Standard*. Springer-Verlag.

Klima, R. E., Sigmon, N., and Stitzinger, E. (2000). *Applications of abstract algebra with Maple*. CRC Press, Boca Raton, FL.

Agradecemos ao apoio financeiro oferecido pelo PIBIC/CNPq.