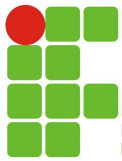
Segurança de Redes

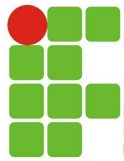
Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 06
Criptografia



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"É muito melhor perceber um defeito em sim mesmo, do que dezenas no outro, pois o seu defeito você pode mudar." (Dalai Lama)



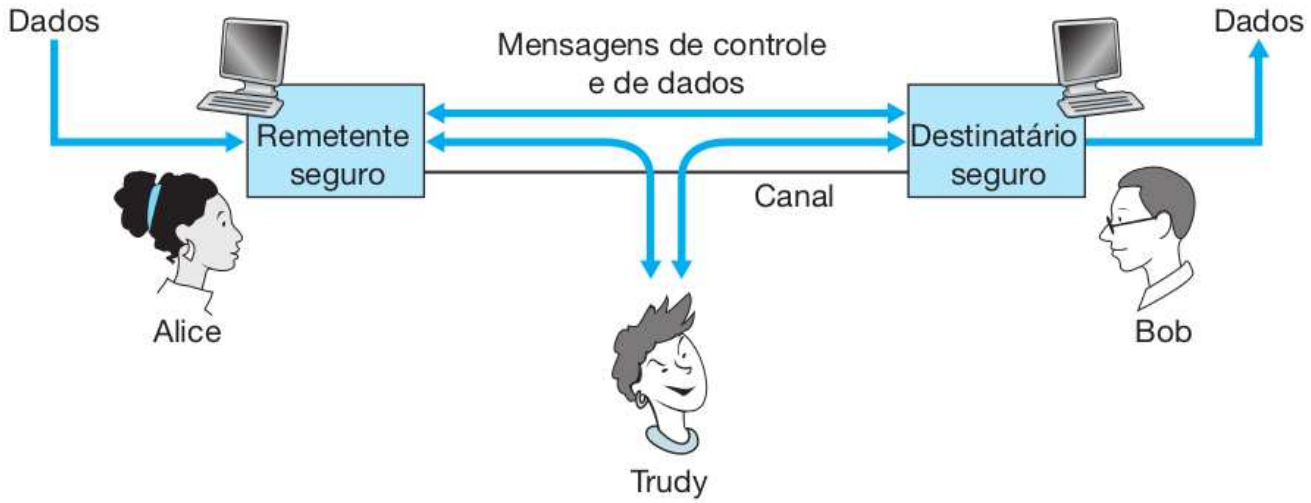
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender o que é criptografia;
- Compreender a importância das chaves de criptografia;
- Quais são os tipos de algoritmos criptográficos;
- Como funcionam os algoritmo de chave simétrica, conhecer um exemplo (AES);
- Como funcionam os algoritmo de chave pública, conhecer um exemplo (RSA);

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

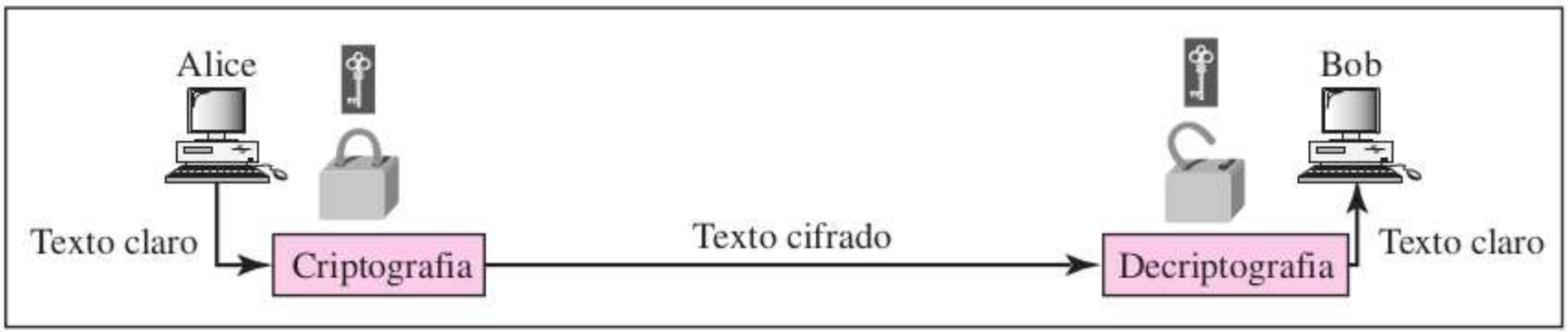
Criptografia é uma palavra de origem grega, significa “escrita secreta”. Entretanto, usamos o termo para nos referirmos à ciência e à arte de transformar mensagens de modo a torná-las seguras e imunes a ataques. Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados (pareça ininteligível). O destinatário, é claro, deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados. Esse técnica visa garantir o sigilo e/ou a autenticidade da informação.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

A mensagem original, antes de ser transformada, é chamada texto claro. Após transformada, ela é denominada simplesmente texto cifrado. Um algoritmo de criptografia (cifra) transforma o texto claro em texto cifrado; um algoritmo de decriptografia transforma o texto cifrado de volta para texto claro. Chave é um número (ou conjunto de números) sobre o qual um algoritmo de criptografia opera.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Importância das Chaves

Atualmente, os algoritmos criptográficos são divulgados à comunidade e o sigilo das informações é garantido apenas pela chave. Quanto maior a chave, mais dificuldade para um ataque por força bruta.

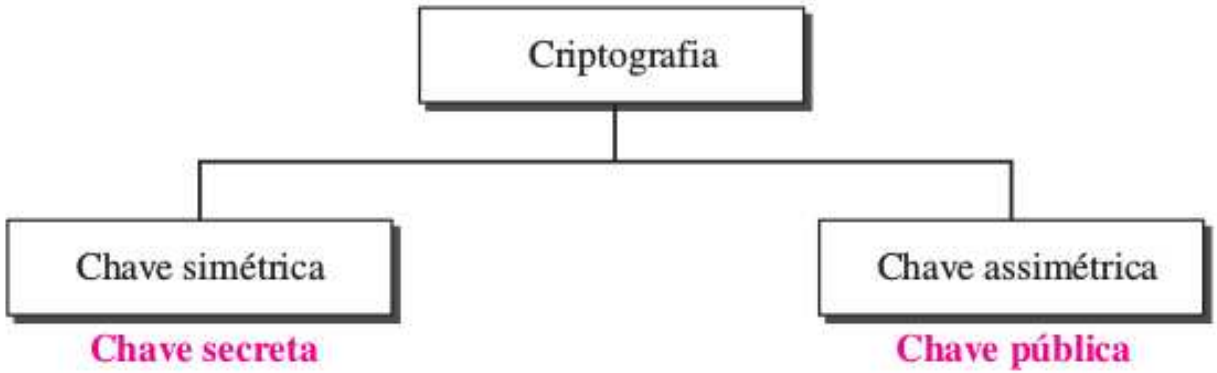
A quebra da criptografia utilizando força bruta (todas as chaves possíveis) é inviável para chaves acima de 128 *bits*, por exemplo:

- Chaves de 64 *bits*: utilizando o computador gerando 90 bilhões de chaves por segundo (*Deep Crack*) temos o tempo de 4 dias e meio para encontrar uma chave.
- Chave de 128 *bits*: utilizando um computador bem melhor (gerando 1 trilhão de chaves por segundo) temos o tempo de 10 milhões de trilhões de anos para testarmos todas as chaves.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Classificação dos Algoritmos Criptográficos

Podemos dividir os principais algoritmos de criptografia (cifras) em dois grupos: algoritmos de criptografia de chave simétrica (também chamados chave secreta) e algoritmos de criptografia assimétrica (também denominados chave-pública).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

A mesma chave é utilizada por ambas as partes. O emissor usa essa chave e um algoritmo de criptografia para criptografar os dados; o receptor usa a mesma chave e o algoritmo de decriptografia correspondente para decriptografar os dados. A chave precisa ser pré-combinada entre os participantes. Os principais algoritmos são: 3DES, RC-4 e AES.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica

Vantagens:

- Velocidade dos algoritmos;
- Facilidade de implementação em *hardware*;
- Chaves menores e simples.

Desvantagens:

- Distribuição das chaves dificulta gerenciamento. Soluções para distribuição de chaves:
  - Algoritmo Diffie-Hellman.
  - Utilização de criptografia assimétrica.
- Não permite autenticação e não repúdio do remetente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica – AES

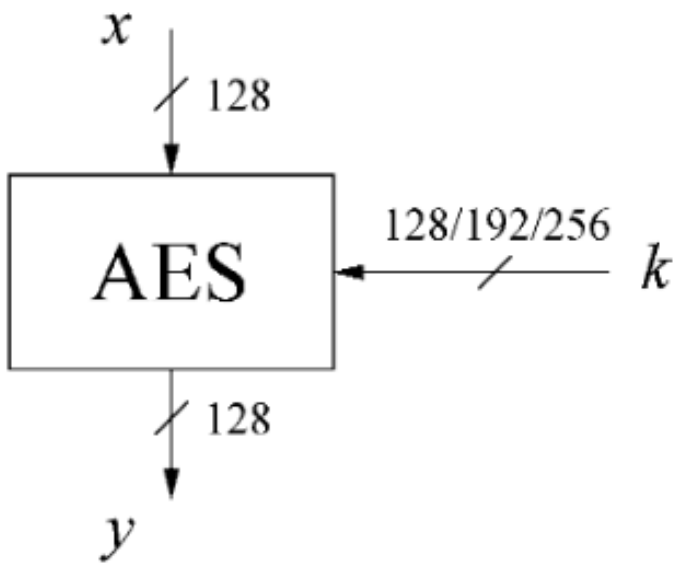
Na década de 90, o principal algoritmo de criptografia era o DES (*Data Encryption Standard*), entretanto foi encontrada falhas nele que permitiam a quebra da confidencialidade. Dessa forma, em 1997, o NIST (*National Institute of Standards and Technology*) Americano decidiu investir em um novo padrão criptográfico.

Pesquisadores do mundo inteiro foram convidados a submeter propostas para este novo padrão, a ser chamado AES (*Advanced Encryption Standard*). Em outubro de 2000, o NIST anunciou o algoritmo vitorioso (o Rijndael). O Rijndael, agora AES, se tornou um padrão de criptografia simétrica do Governo dos Estados Unidos. Outros governos e instituições depois passaram a utilizá-lo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

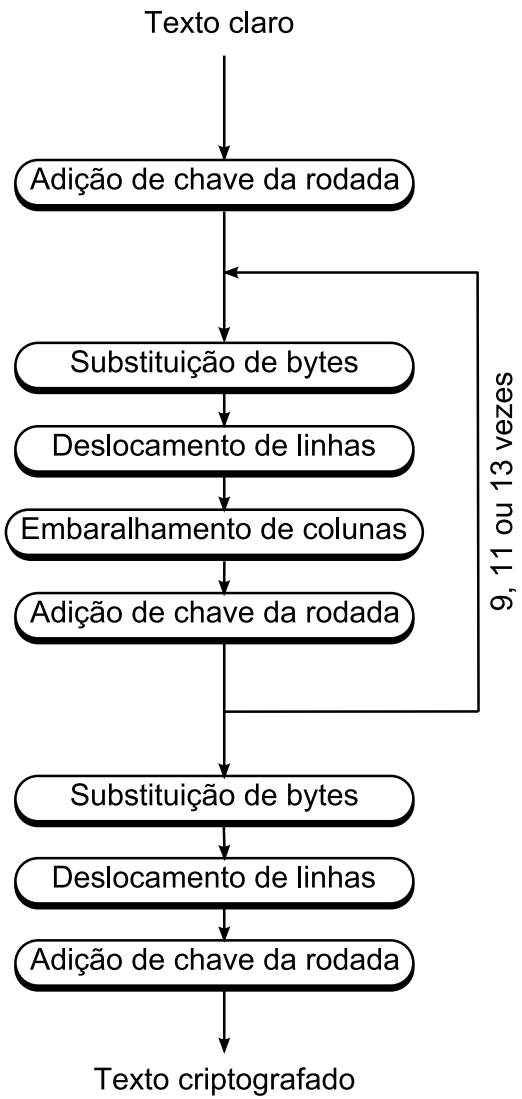
Criptografia de Chave Simétrica – AES

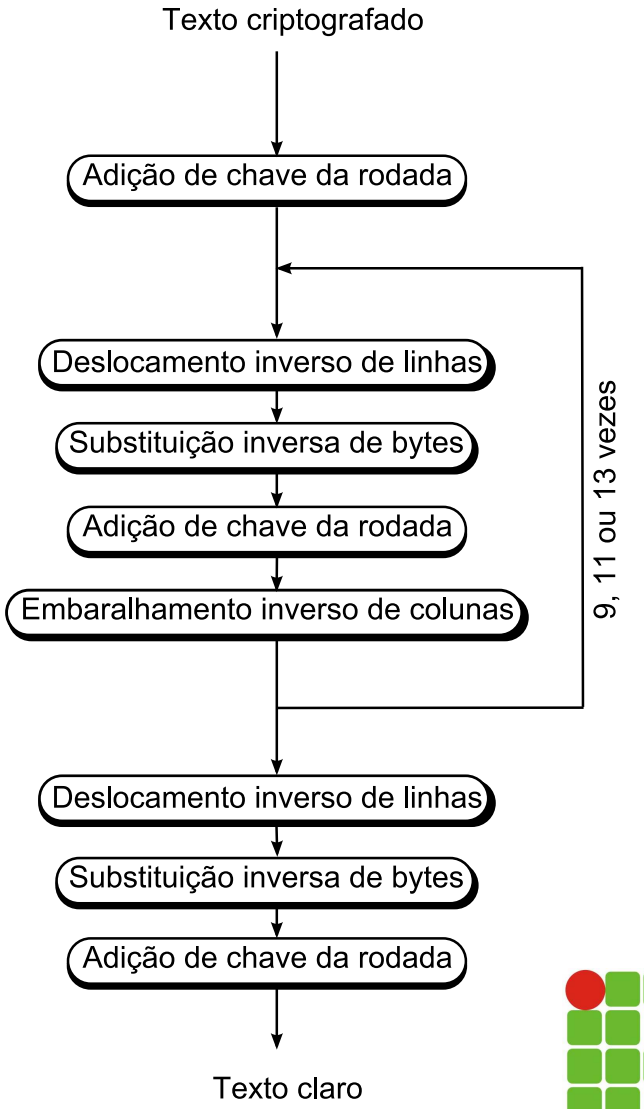
O AES permite tamanhos de chaves de 128 *bits*, 192 e 256 *bits*. Ele utiliza substituição e permutações em várias rodadas (10,11 ou 13 para 128, 192 e 256 *bits*, respectivamente).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica – AES





INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criptografia de Chave Simétrica – AES

No algoritmo AES o texto original é inserido em uma matrizes bidimensionais de bytes chamadas de "Estado". Por exemplo, blocos de 128 bits são copiados em um array organizado em 4 colunas, cada coluna contendo 4 bytes.

Estado

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Simétrica – AES

Para criptografar, cada rodada do AES (exceto o último) consiste em quatro operações sobre as matrizes de Estado:

- Adição de chave da rodada: cada *byte* do estado é combinado com uma subchave (*RoundKey*);
- Substituição de *bytes*: cada *byte* é substituído por outro de acordo com uma tabela de referência.
- Deslocamento de linhas: é uma etapa de transposição, onde cada fileira do estado é deslocada de um determinado número de posições.
- Embaralhamento de colunas: é uma operação que opera nas colunas do estado e combina os quatro *bytes* de cada coluna.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

AES – Adição da chave de rodada

A transformação de adição da chave de rodada (AddRoundKey) consiste em modificar a matriz de Estado, realizando uma operação XOR byte a byte desta com a matriz com uma outra matriz gerada pela chave.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

AES – Substituição de bytes

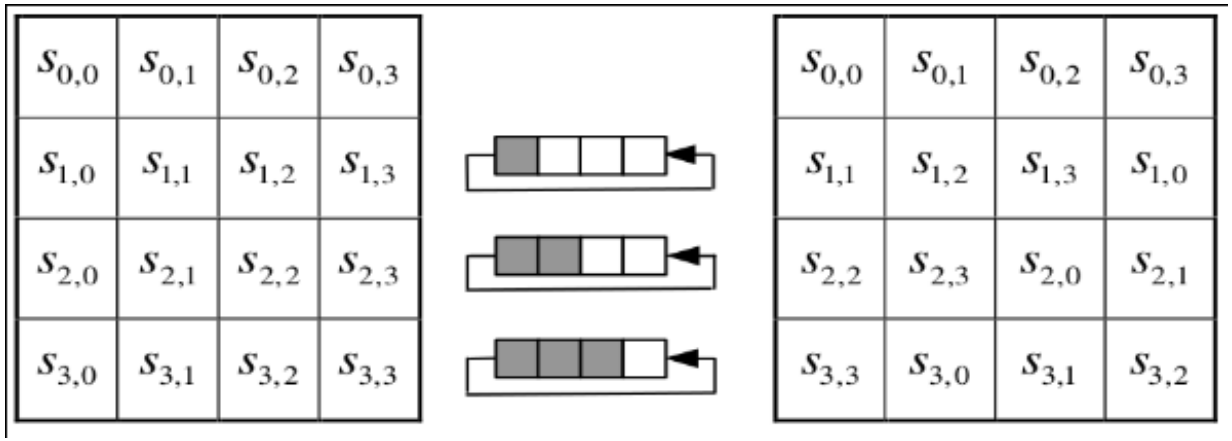
Consiste em aplicar uma caixa de substituição (S-box) em cada byte da matriz estado. Na tabela faz a intersecção da linha equivalente ao valor dos quatro bits mais significativos do byte e da coluna equivalente ao valor dos quatro bits menos significativos deste mesmo byte. Por exemplo, considere o valor 53.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

AES – Deslocamento de linhas

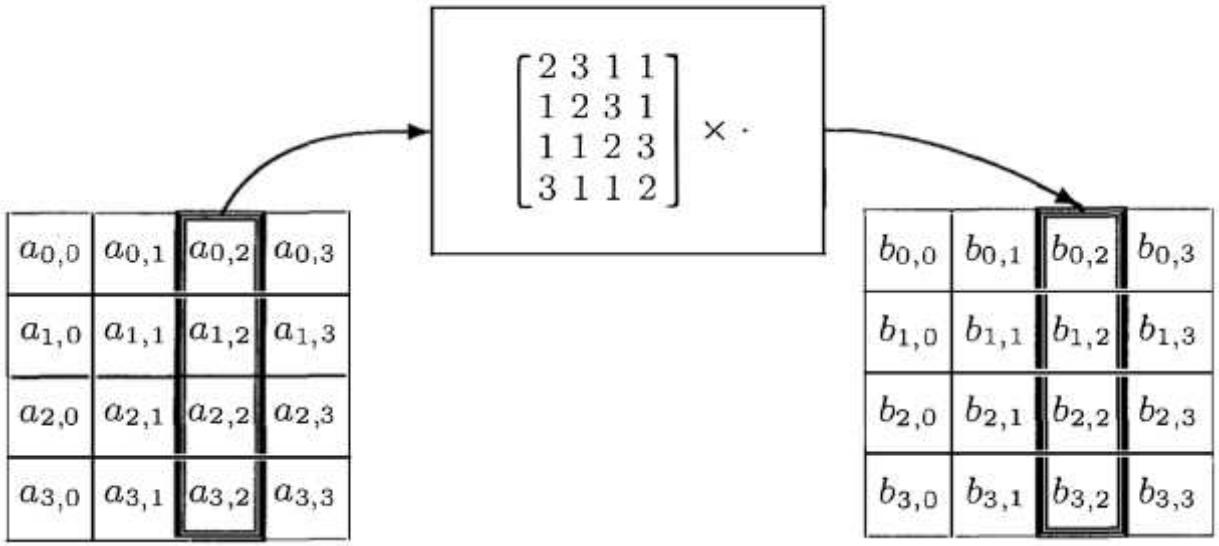
Consiste em uma transposição de deslocamento cíclico dos bytes da matriz estado, onde cada linha é deslocada por um número fixo, de acordo com a linha em questão (0, 1, 2 e 3).



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

AES – Embaralhamento de colunas

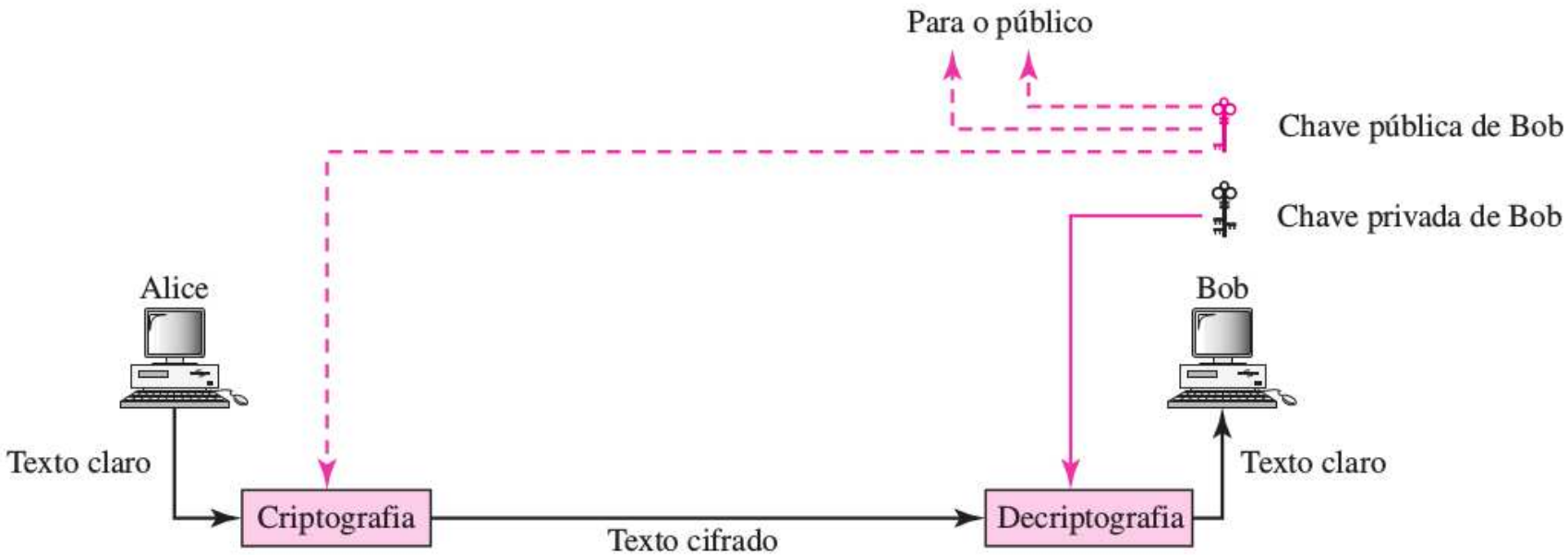
É uma permutação linear e opera sobre as colunas da matriz de estado.
Pode ser representado como uma multiplicação matricial.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica (Pública)

A criptografia assimétrica, também chamado de chave pública, é uma forma de criptossistema em que a criptografia e a descriptografia são realizadas com chaves diferentes: uma chave pública e uma chave privada. O transmissor usa a chave pública do receptor para criptografar a mensagem. O receptor usa a sua chave privada para decriptografar.



Criptografia de Chave Assimétrica

O criptossistema de chave pública mais utilizado atualmente é o RSA, sendo envolvido o conceito de números primos, de modo que é difícil de explorar, pela complexidade de se encontrar números primos de um número composto. Outros exemplos de algoritmos são: DSA, El Gamal e DSS.

A chave privada é mantida em segredo pelo receptor. Enquanto que a chave pública é distribuída publicamente. Uma restrição, com relação a estas chaves, é que a chave privada não pode ser obtida a partir da chave pública. Em geral, os algoritmos assimétricos utilizam tamanhos de chave de 1024, 2048 ou 4096 bits.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica

Vantagens

- Pode ser utilizada para garantir a confidencialidade, a autenticidade ou ambos;

Desvantagens

- Complexidade dos algoritmos que leva a uma quantidade de tempo de processammento relativamente grande.
- A distribuição das chaves públicas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica – RSA

Desenvolvido em 1977 (por Ron Rivest, Shamir e Adleman no MIT) o RSA é o algoritmo de chave pública mais utilizado. Atualmente, um tamanho de chave de 1.024 bits é considerado forte o suficiente para praticamente todas as aplicações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica – RSA

Cifração e decifração são realizadas da seguinte forma, considere um texto original (M) e o texto criptografado (C). A relação entre eles é:

Criptografia:

$$C = M^e (\mod n)$$

Decriptografia:

$$M = C^d (\mod n)$$

A chave pública consiste no par (e, n) e a chave privada consiste em (d, n).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica – RSA

Algoritmo RSA

1. Escolha dois números primos, p e q, onde p $\neq$ q.
2. Calcule $n = p \times q$ e $z = (p-1)(q-1)$.
3. Escolha um número e tal que $(1 < e < z)$ e z e e sejam primos entre si.
4. Encontre d de forma que $(e \times d) \mod z = 1$. Em outras palavras, o resto da divisão de $e \times d$ por z seja o número 1.

obs.: chamamos números primos entre si (ou coprimos) ao conjunto de números onde o único divisor comum a todos eles é o número 1.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Exemplo:

1. Supondo $p = 17$ e $q = 11$,
2. Calculando

$$\begin{array}{rclrcl} n & = & p \times q & z & = & (p-1)(q-1) \\ n & = & 17 \times 11 & z & = & (17-1) \times (11-1) \\ n & = & 187 & z & = & 16 \times 10 = 160 \end{array}$$

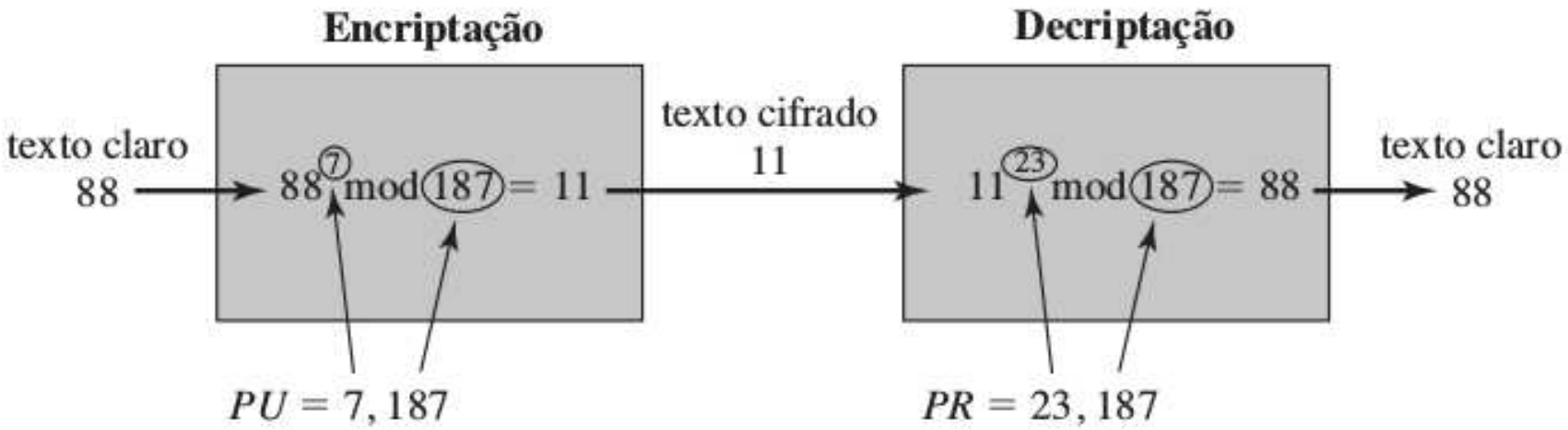
3. Um valor adequado para e é 7, visto que $1 < 7 < 160$ e 7 e 160 são primos entre si.
4. Escolhe $d = 23$, pois:

$$\begin{array}{rcl} (e \times d) \mod z & = & 1 \\ (7 \times 23) \mod 160 & = & 1 \\ 1 & = & 1 \end{array}$$

A chave pública: (7, 187) e a chave privada: (23,187).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia de Chave Assimétrica – RSA



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE