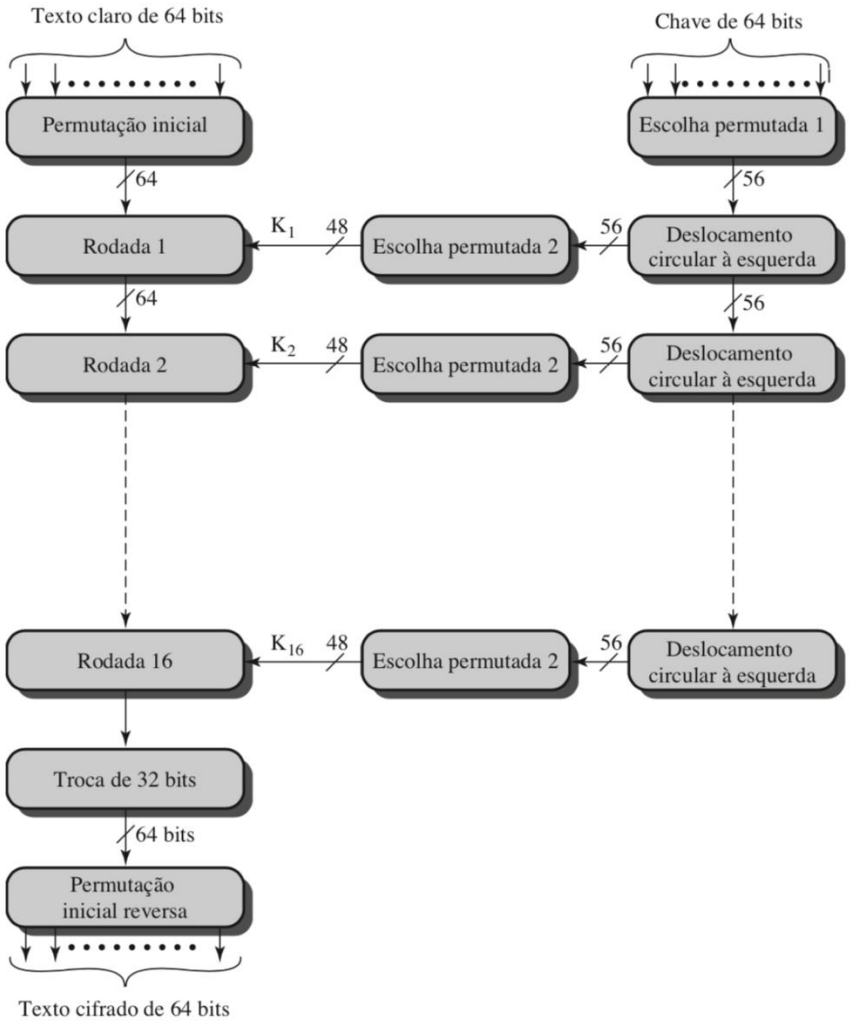
Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Aula passada

Segurança da Informação– GBC083

DES – representação geral



DES – diferenças com a cifra de Feistel

- Com exceção das permutações inicial (IP) e final (IP^{-1}), o DES tem a estrutura exata de uma cifra de Feistel;
  - Já conhecemos a estrutura de uma cifra de Feistel!

- Dois itens foram esclarecidos:
  1. Geração das subchaves;
  2. Conteúdo da função F.

DES – Geração das subchaves

- As subchaves são necessárias por dois motivos:
  1. Projeto do algoritmo (cifra de produto) envolve uma série de rodadas;
  2. Usar chaves repetidas (ou até a mesma chave!) em cada uma das rodadas do algoritmo enfraquece a ideia de tornar obscura a relação entre texto claro e texto cifrado.

DES – Geração das subchaves

- Algoritmo
  1. Entrada de 64 bits -> K
  2. Escolha permutada de 56 bits -> K_p
  3. Deslocamento circular à esquerda em K_p -> K_{pe}
  4. Escolha permutada de 48 bits em K_{pe} -> K_1

DES – Rodadas e função F

A função rodada F é o coração de um algoritmo de criptografia simétrica;

- O DES faz o seguinte:
  1. Misturar um trecho do texto claro (RE) com a chave – como isso é feito mesmo?
     - XOR!
  2. Aplicar substituições no texto que foi misturado com a chave – como isso é feito mesmo?
     - Tabela de substituição –S-Box (também permitirá diminuir o número de bits)
  3. Permutações

DES – Segurança (tamanho da chave)

Tamanho de chave (bits)	Cifra	Número de chaves alternativas	Tempo exigido a 10^9 decriptações/s	Tempo exigido a 10^{13} decriptações/s
56	DES	$2^{56} \approx 7{,}2 \times 10^{16}$	2^{55} ns = 1,125 ano	1 hora
128	AES	$2^{128} \approx 3{,}4 \times 10^{38}$	2^{127} ns = $5{,}3 \times 10^{21}$ anos	$5{,}3 \times 10^{17}$ anos
168	Triple DES	$2^{168} \approx 3{,}7 \times 10^{50}$	2^{167} ns = $5{,}8 \times 10^{33}$ anos	$5{,}8 \times 10^{29}$ anos
192	AES	$2^{192} \approx 6{,}3 \times 10^{57}$	2^{191} ns = $9{,}8 \times 10^{40}$ anos	$9{,}8 \times 10^{36}$ anos
256	AES	$2^{256} \approx 1{,}2 \times 10^{77}$	2^{255} ns = $1{,}8 \times 10^{60}$ anos	$1{,}8 \times 10^{56}$ ano

Princípios de projeto de cifra de bloco

Embora tenha havido muito progresso no projeto de cifras de bloco criptograficamente fortes, os princípios básicos não mudaram tanto desde o trabalho de Feistel e da equipe de projeto do DES, no inicio da década de 1970.

Três aspectos críticos para o projeto de cifra de bloco são:

1. Número de rodadas;
2. Projeto da função F;
3. Algoritmo de geração de subchave.

Tópicos da aula

Segurança da Informação– GBC083

Tópicos da aula

- Breve história sobre o AES
- AES em detalhes?
- Estrutura básica do AES
- Discussão sobre a estrutura do AES
- Expansão da chave
- Discussão

Breve histórico sobre o AES

Segurança da Informação– GBC083

Definição

- O *Advanced Encryption Standard* ou AES, foi publicado pelo *National Institute of Standards and Technology (*NIST) em 2001;

- O AES é uma cifra simétrica de bloco elaborada para substituir o DES como o algoritmo padrão de criptografia para diferentes tipos de aplicações.

Cenário antes do AES...

- DES e 3DES;
- DES opera com um tamanho de bloco pequeno (64 bits) e um tamanho de chave ainda menor (56 bits);
- Como o DES já era adotado em muitas aplicações, a solução mais simples foi criar uma variação...
- 3DES – Usar o DES três vezes! Cifrar com a chave 1, decifrar com a chave 2 e cifrar com a chave 1;
  - A comunidade estudou exaustivamente o algoritmo e a força-bruta sempre acabou sendo a "melhor" opção para os criptoanalistas...

Cenário antes do AES...

- O tamanho da chave aumentou...
- O tamanho do bloco não!
- O DES foi projetado para implementações baseadas em hardware dos anos 70, ou seja, não produz um software muito eficiente;
- O 3DES acaba sofrendo do mesmo problema.

Mudanças são necessárias...

Qual a melhor forma para propor um novo algoritmo de criptografia que, potencialmente, seria o novo padrão?

Call for proposals!

- Em 1997 o NIST lançou um *call for proposals* (chamada de propostas pública) para propor um novo algoritmo de criptografia simétrica;
- O algoritmo deveria ter uma segurança igual ou melhor do que o 3DES e ser significativamente mais eficiente do que ele;
- A chamada definiu os seguintes termos:
  - Tamanho de bloco de 128 bits
  - Tamanhos de chave de 128, 192 e 256 bits

Call for proposals!

- A primeira rodada de avaliação terminou com 15 propostas aprovadas;
- A segunda rodada diminuiu esse número para 5;
- Após um novo processo de avaliação (em uma conferência), o algoritmo *Rijndael* levou a maioria dos votos;
- Após novos testes e apresentações dos 5 finalistas, o NIST anunciou em outubro de 2000 a vitória do Rijndael.
  - Dois pesquisadores belgas: Dr. Joan Daemen and Dr. Vincent Rijmen

Call for proposals - Critérios

- Diversos critérios foram usados para avaliar os algoritmos ao longo dos anos:
  - Segurança – resistência do algoritmo a diferentes ataques de criptoanálise;
  - Custo computacional
  - Possibilidade de implementação em hardware e software
  - Cifrar x decifrar
  - Entre outros...

- De forma geral, o Rijandael teve um bom desempenho em praticamente todos os quesitos.

Call for proposals – Mais um?!

Temos um novo "Call for proposals" sobre algoritmos criptográficos em andamento?

Call for proposals – Mais um?!

Temos um novo "Call for proposals" sobre algoritmos criptográficos em andamento?

- Sim! Qual o intuito? AES está com problemas?

Novo - Call for proposals

- Post-quantum cryptography ou criptografia quântica!
- A ideia da chamada é buscar algoritmos resistentes a computação quântica;
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals

Novo - Call for proposals

- A chamada foi lançada em abril de 2016;
- O processo ainda está acontecendo e em 2022 a lista com os algoritmos selecionados foi divulgada;
- Isso mostra a preocupação dos órgãos de regulação com a criptografia.

Novo - Call for proposals

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced (26 algorithms)
March 15, 2019	Deadline for updated submission packages for the Second Round
May 8-10, 2019	NIST Presentation at PQCrypto 2019: Round 2 of the NIST PQC "Competition" - What was NIST Thinking? (Spring 2019), *Dustin Moody*
August 22-24, 2019	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

AES em detalhes?

Segurança da Informação– GBC083

Como o AES será apresentado?

- Comparada às cifras de chave pública como a RSA ou a cifra simétrica DES, a estrutura do AES é bastante complexa e não pode ser explicada tão facilmente;

- O AES, em particular, trabalha com uma aritmética em uma estrutura algébrica conhecida como corpo.

Como o AES será apresentado?

- Compreender com detalhes cada uma das operações do AES envolve ter uma boa noção sobre operações em corpos finitos – o que está fora do escopo desse curso!

- O objetivo é mostrar o funcionamento, em linhas gerais, do AES;
  - Ilustrar algumas decisões de projetos que o diferenciam do DES e permitem que ele seja adotado como padrão em se tratando de criptografia simétrica.

Estrutura básica do AES

Segurança da Informação– GBC083

Entradas

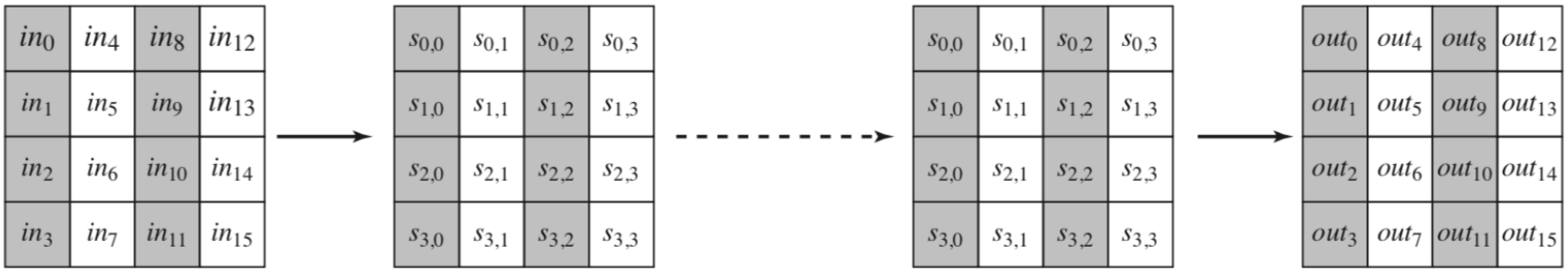
- AES recebe como entrada:

1. Um bloco de texto de 128 bits (16 bytes);
2. Uma chave que pode ter 128, 192 ou 256 bits (16, 24 e 32 bytes).

Representação do bloco de texto claro/cifrado

- O bloco de texto em claro/cifrado é representado como uma matriz de bytes 4x4;

- Esse bloco é copiado para um array **Estado**, que é modificado a cada etapa do processo de cifrar/decifrar;



Representação da chave

- A chave também é representada como uma matriz (4x4, 4x6, 4x8);
- Assim como no DES, chaves intermediárias (de rodada) devem ser geradas;
- As chaves intermediárias devem ter 128 bits pois o AES trabalha sob todo o bloco de texto claro/cifrado.

Rodadas

- O AES possui N rodadas com N dependendo do tamanho da chave;

- N=10 rodadas para o AES-128
- N=12 rodadas para o AES-192
- N=14 rodadas para o AES-256

Rodadas

Pergunta!

Porque o número de rodadas aumenta de acordo com o número de chaves?

Rodadas

Pergunta!

Porque o número de rodadas aumenta de acordo com o número de chaves?

Resposta:

- mais rodadas => mais segurança
- Como a chave é maior, é preciso um número maior de rodadas para que os bits "extras" da chave possam atingir de maneira adequada o texto cifrado.
- Decisão de projeto – para cada aumento de 32 bits de chave, uma rodada foi inserida.

Rodadas

1. Transformação inicial
   - AddRoundKey
2. As primeiras N-1 rodadas consistem em quatro funções de transformações distintas
   - SubBytes
   - ShiftRows
   - MixColumns
   - AddRoundKey
3. A última rodada consiste de três funções
   - SubBytes
   - ShiftRows
   - AddRoundKey

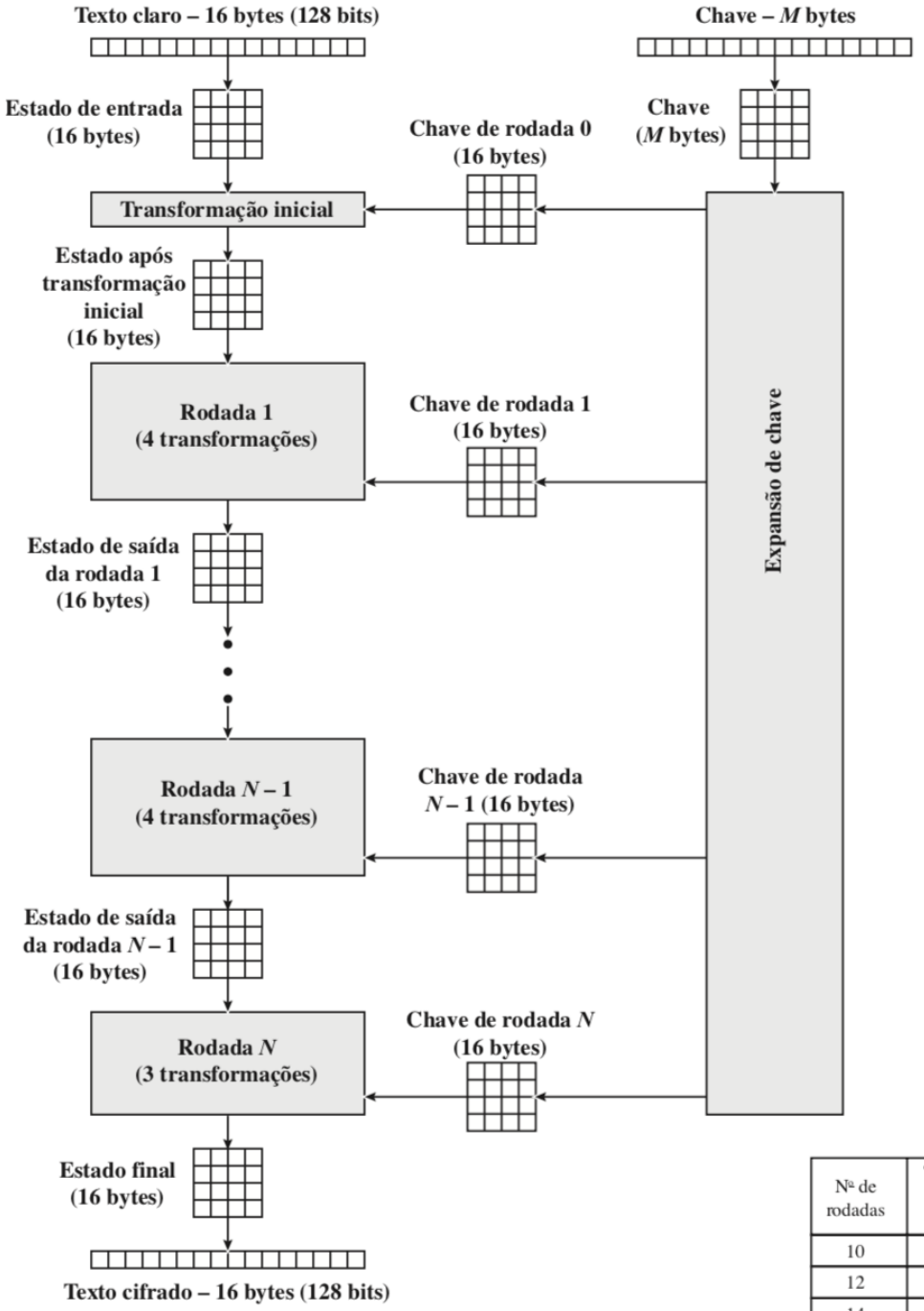
Resumo

Tamanho da chave (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Tamanho do bloco de texto claro (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Número de rodadas	10	12	14
Tamanho da chave de rodada (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Tamanho da chave expandida (words/bytes)	44/176	52/208	60/240

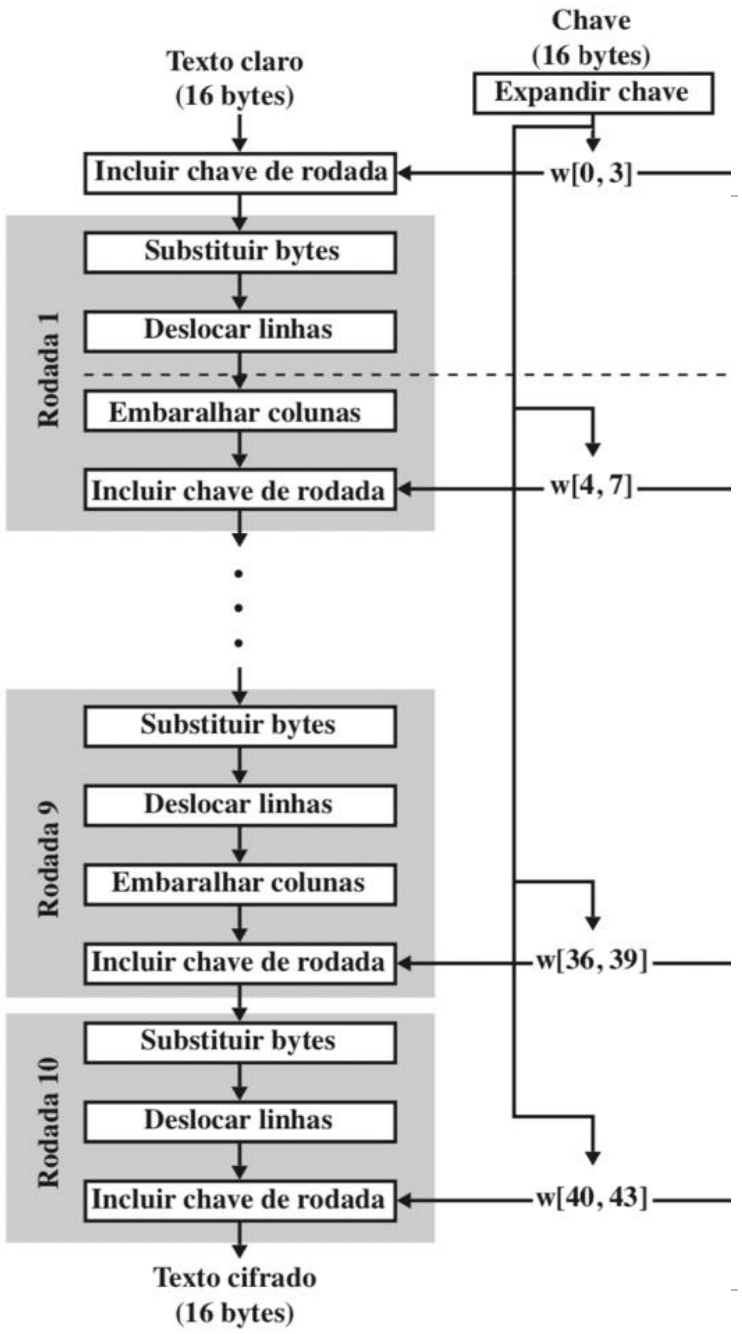
Resumo

Tamanho da chave (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Tamanho do bloco de texto claro (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Número de rodadas	10	12	14
Tamanho da chave de rodada (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Tamanho da chave expandida (words/bytes)	44/176	52/208	60/240

Alguém saberia dizer a razão da chave expandida ter esse tamanho??



Nº de rodadas	Tamanho da chave (bytes)
10	16
12	24
14	32


Chave
(16 bytes)
Texto claro
(16 bytes)
Expandir chave
Incluir chave de rodada
w[0, 3]
Substituir bytes
Deslocar linhas
Rodada 1
Embaralhar colunas
Incluir chave de rodada
w[4, 7]
Substituir bytes
Deslocar linhas
Rodada 9
Embaralhar colunas
Incluir chave de rodada
w[36, 39]
Substituir bytes
Deslocar linhas
Rodada 10
Incluir chave de rodada
w[40, 43]
Texto cifrado
(16 bytes)

Discussão sobre a estrutura do AES

Segurança da Informação– GBC083

Estrutura do AES - Feistel

- Notem que o AES não é uma cifra de Feistel!
- Lembrem-se que na cifra de Feistel metade do bloco de dados é usada para modificar a outra metade e depois elas são invertidas;
- O AES processa o bloco de dados (claro/cifrado) inteiro como uma única matriz durante cada rodada.

Estrutura do AES - Feistel

- Apesar de não ser uma cifra de Feistel, o modelo básico de cifra de produto está lá...
  1. XOR do bloco com a chave
  2. Difusão e confusão sob o bloco
  3. XOR do bloco com a chave
  4. E assim por diante...

- Esse processo mostrou-se bem seguro ao longo do tempo.

Estrutura do AES - Simplicidade

- A estrutura do algoritmo é bem simples:
  1. Mistura o texto com a chave;
  2. Nove rodadas com as quatro funções (permutação e confusão)
  3. Décima rodada com três funções

- Outros algoritmos concorrentes não possuíam essa simplicidade no fluxo de execução ou nos componentes que formam as funções principais.

Estrutura do AES - Funções

- **SubBytes:** utiliza **uma** S-box para realizar uma substituição byte a byte do bloco (confusão);
  - Quantas S-box o DES tinha mesmo?
- **ShiftRows:** permutação sobre as linhas (difusão);
- **MixColumns:** operação sobre as colunas – cada coluna passará por uma multiplicação (difusão);
- **AddRoundKey:** um XOR bit a bit simples do bloco atual com uma parte da chave expandida.

Estrutura do AES – Funções – Sbox (cifrar)

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

Estrutura do AES – Funções – Sbox (decifrar)

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

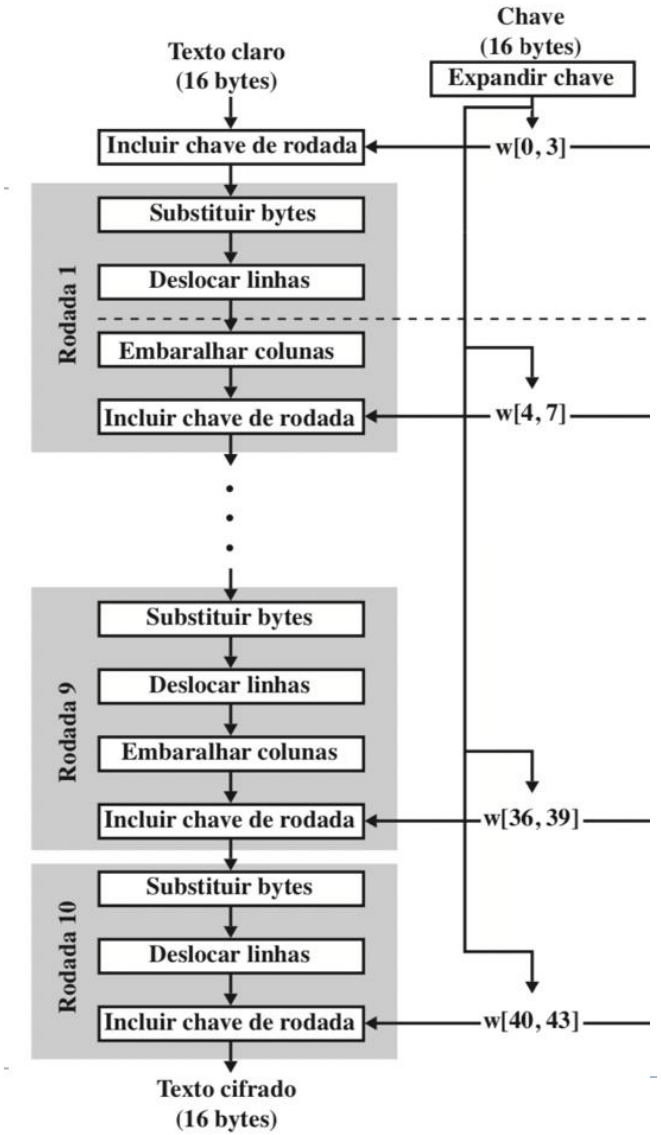
Estrutura do AES - Decifrar

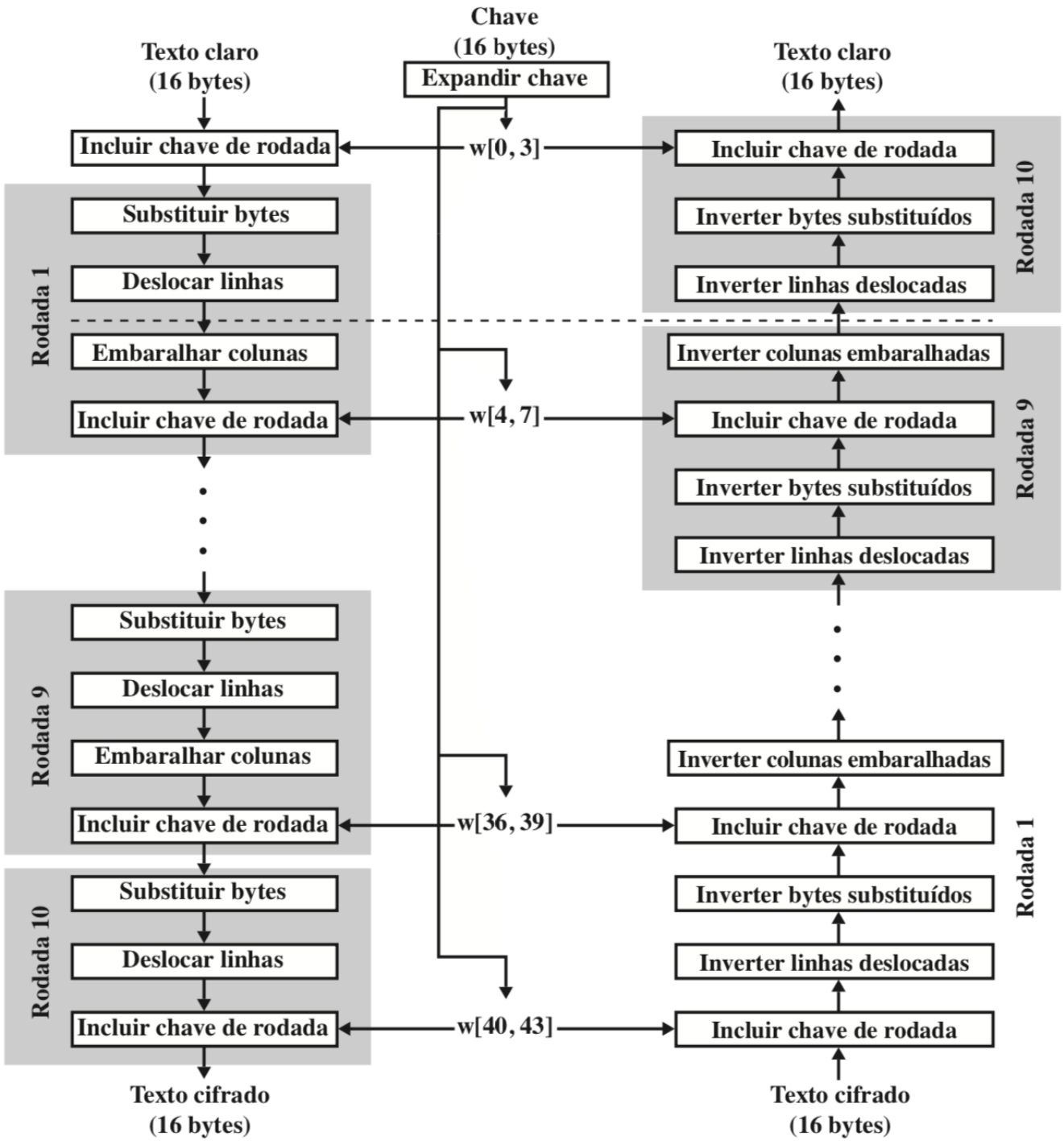
- Assim como na maioria das cifras em bloco, o algoritmo para decifrar o texto utiliza a chave expandida em ordem reversa;

- Porém, o algoritmo de decifrar não é igual ao do algoritmo de cifrar. Isso é uma consequência da estrutura do AES em particular.

Estrutura do AES - Decifrar

Alguém tem um palpite sobre como a decifragem do AES deveria funcionar?




Chave
(16 bytes)
Expandir chave
Texto claro
(16 bytes)
Incluir chave de rodada
w[0, 3]
Substituir bytes
Deslocar linhas
Embaralhar colunas
Incluir chave de rodada
w[4, 7]
Rodada 1
Substituir bytes
Deslocar linhas
Embaralhar colunas
Incluir chave de rodada
w[36, 39]
Rodada 9
Substituir bytes
Deslocar linhas
Incluir chave de rodada
w[40, 43]
Rodada 10
Texto cifrado
(16 bytes)
Texto claro
(16 bytes)
Incluir chave de rodada
Inverter bytes substituídos
Inverter linhas deslocadas
Rodada 10
Inverter colunas embaralhadas
Incluir chave de rodada
Inverter bytes substituídos
Inverter linhas deslocadas
Rodada 9
Inverter colunas embaralhadas
Incluir chave de rodada
Inverter bytes substituídos
Inverter linhas deslocadas
Incluir chave de rodada
Rodada 1
Texto cifrado
(16 bytes)

Estrutura do AES - Decifrar

- Cada um dos estágios (ou funções) deve ser facilmente reversível;
  - Essa é uma diferença para a cifra de Feistel;
  - Isso exige uma implementação diferente para o algoritmo de decifragem.

- Isso permitirá que entre cada um dos estágios (figura que descreve a estrutura do AES) o **Estado** é o mesmo para a função de cifrar e decifrar.

Estrutura do AES – última rodada

- A omissão da função MixColumns na última rodada foi uma decisão de projeto dos pesquisadores;

- A principal justificativa foi o desempenho;
  - A difusão proporcionada pelo MixColumns não chegaria ao próximo round, pois não existe um novo round...

Estrutura do AES – última rodada

- Os autores demonstraram que tal omissão não impacta na segurança do algoritmo;
- Contudo, alguns pesquisadores mostram que tal omissão pode enfraquecer o algoritmo;
- https://eprint.iacr.org/2010/041.pdf

Expansão da chave

Segurança da Informação– GBC083

Expansão da chave (128 bits)

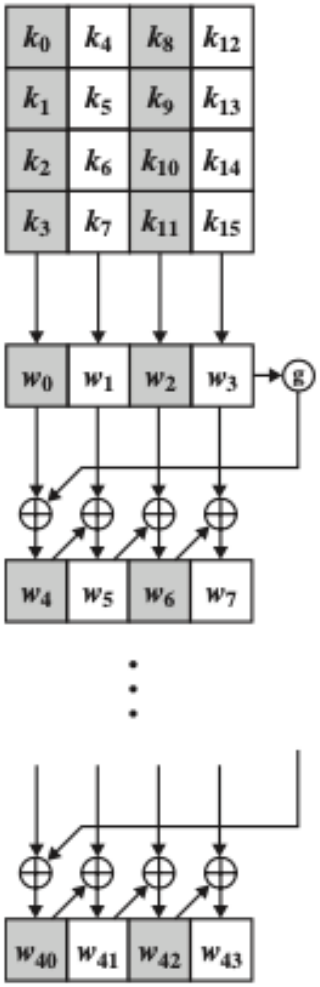
- O algoritmo de expansão da chave utiliza como entrada uma palavra (chave!) de 128 bits (16 bytes ou 4 palavras – 1 coluna);
- A saída do algoritmo será um vetor de 1408 bits ou 176 bytes ou 44 palavras;
- Isso é suficiente para gerar 11 subchaves, uma para o AddRoundKey inicial e as outras 10 para serem usadas nas rodadas.
  - Porque?

Expansão da chave (128 bits)

1. A chave original é copiada para as primeiras quatro posições de palavras do vetor de 44 palavras;
2. O restante do vetor é preenchido com quatro palavras de cada vez;

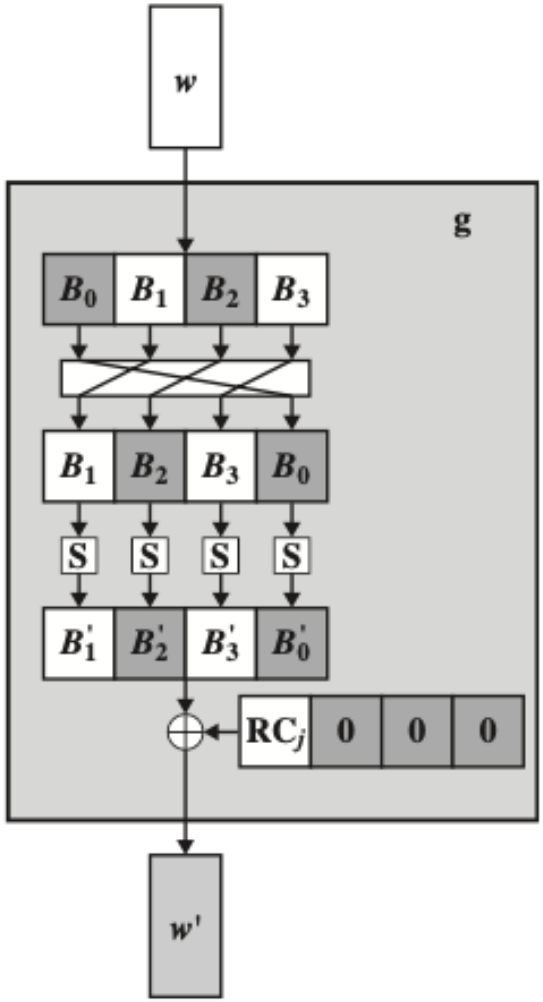
Expansão da chave (128 bits)

3. Três das quatro palavras são simplesmente um XOR da palavra imediatamente anterior (w[i-1]) e da palavra quatro posições atrás (w[i-4]);



Expansão da chave (128 bits)

4. A outra palavra (múltiplas de 4 – última coluna) é preenchida da seguinte forma (usando a função "g", presente no slide anterior):
   a) O primeiro byte vira o último byte;
   b) Todos os quatro bytes passam por uma substituição;
   c) A nova palavra passa por um XOR com uma constante da rodada;
   d) Finalmente, um novo XOR é feito entre o resultado do passo 6 com a palavra quatro posições atrás (w[i-4]).



Raciocínio por trás do algoritmo

- Resistente a ataques conhecidos;
- Desempenho;
- Conhecer uma parte da chave ou da chave da rodada não permite o cálculo de muitos outros bits dela.

Roteiro de estudos

1. Leitura das seções 5.2, 5.3, 5.4, 5.5 e 5.6 do livro "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
   - Alguns detalhes das operações estão por lá mas não foram vistos aqui. É importante que seja feito um filtro na leitura das seções.
2. Estudo das vídeo-aulas referentes ao tópico 7;
3. Assistir o seguinte vídeo sobre o AES:
   - https://www.youtube.com/watch?v=gP4PqVGudtg
4. Resolução do TP3

Roteiro de estudos

Outras referências:

- http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html
- https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
- https://medium.com/@mstahir/how-aes-algorithm-works-701ef5cebc7c