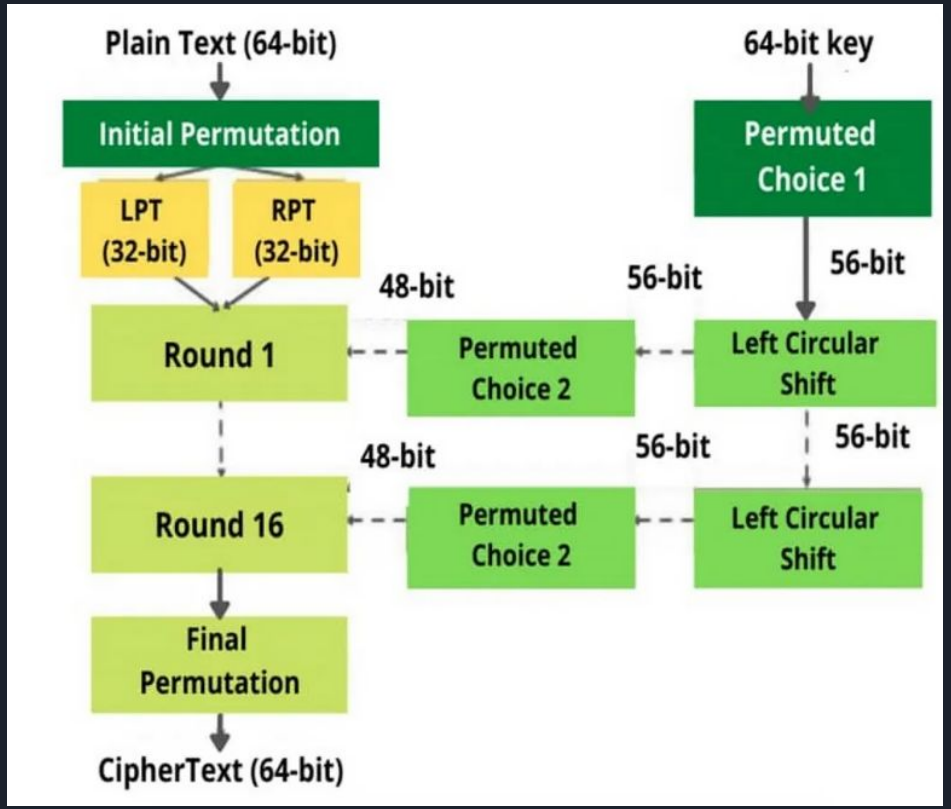
Análise comparativa entre os algoritmos de criptografia DES e AES

Discentes: Breno Cupertino, Gabriel Baptista e Yan Brandão

Algoritmo DES (Data Encryption Standard)

- Bloco de texto simples de 64 bits <-> Bloco de texto cifrado de 64 bits
- Input: 64 bits
- Output: 64 bits
- Chave principal: 64 bits
- Subchave: 56 bits
- Chave da rodada: 48 bits
- Num. de rodadas : 16



Algoritmo DES - Funcionamento

1. Permutação Inicial
2. Geração de Chave
3. Rodadas de criptografia
4. Permutação Final

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Geração de Chaves

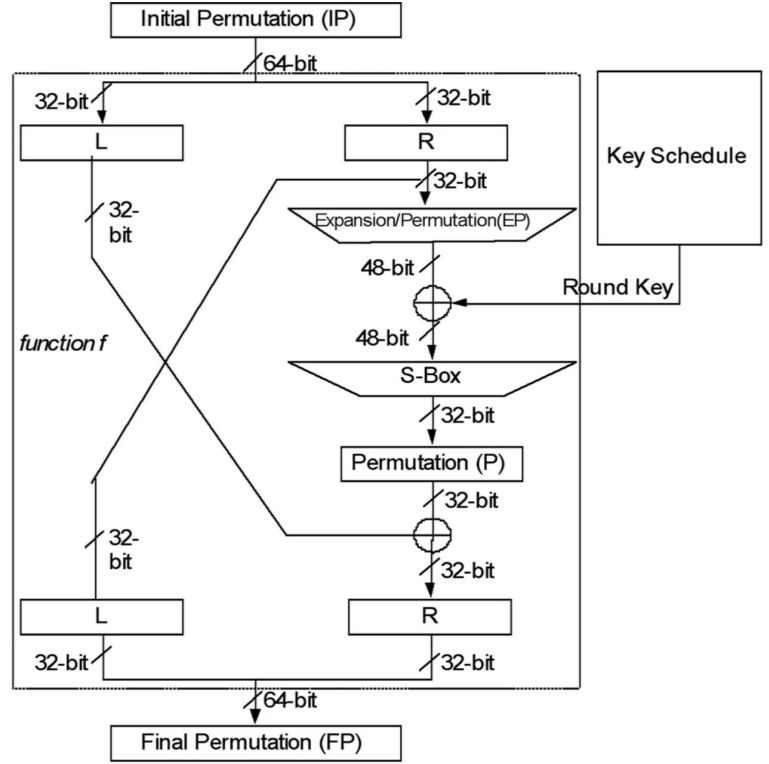
Permutation Table

	1	2	3	4	5	6	7	8
0	57	49	41	33	25	17	9	1
1	58	50	42	34	26	18	10	2
2	59	51	43	35	27	19	11	3
3	60	52	44	36	63	55	47	39
4	31	23	15	7	62	54	46	38
5	30	22	14	6	61	53	45	37
6	29	21	13	5	28	20	12	4

Key Compression Table

	1	2	3	4	5	6	7	8
1	14	17	11	24	01	05	03	28
2	15	06	21	10	23	19	12	04
3	26	08	16	07	27	20	13	02
4	41	52	31	37	47	55	30	40
5	51	45	33	48	44	49	39	56
6	34	53	46	42	50	36	29	32

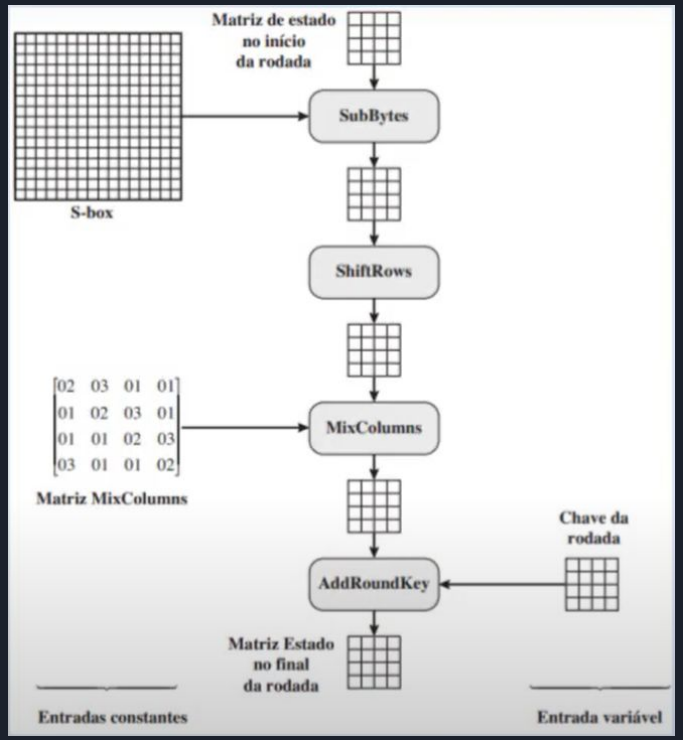
Rodada de Criptografia e Permutação Final



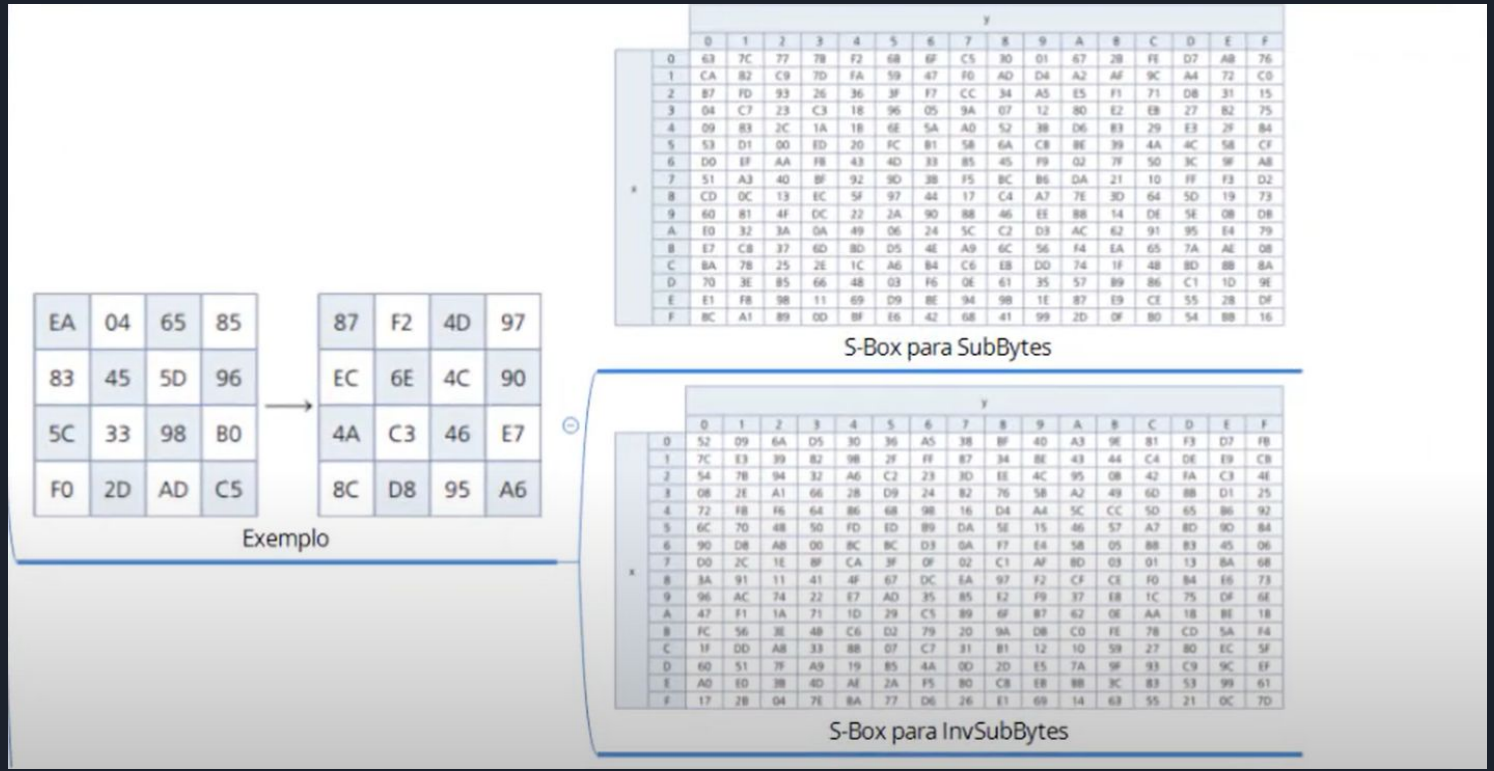
IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

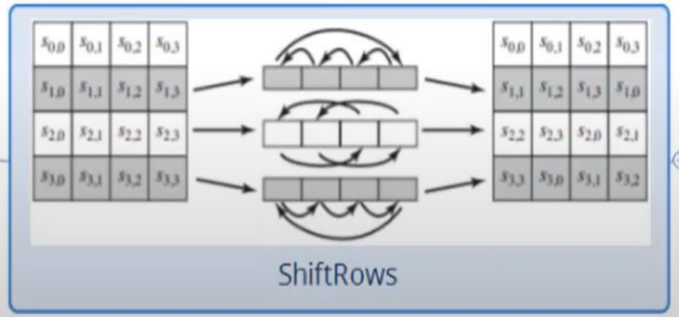
Explicação do funcionamento do AES



Fase de Substituição de Bytes



Fase de Permutação de Linhas

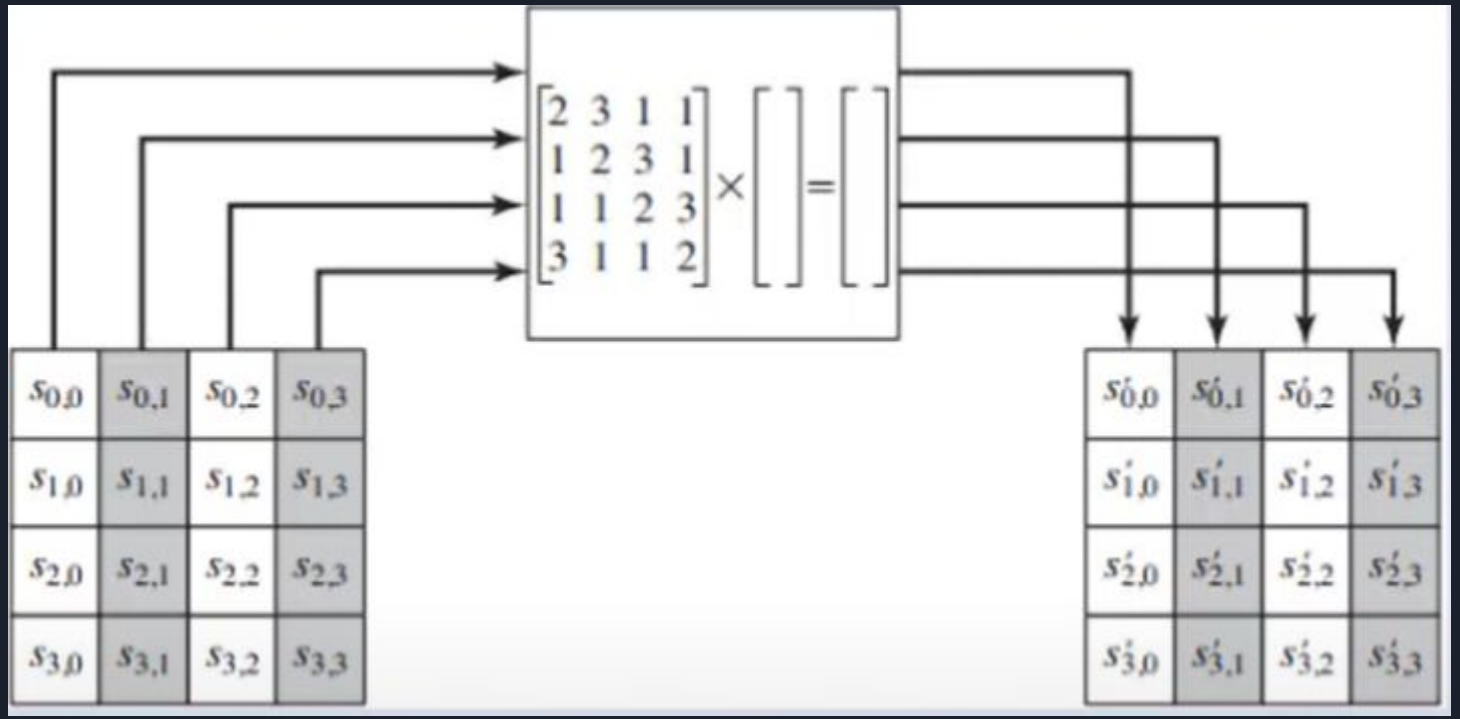


Transformação direta de deslocamento de linhas

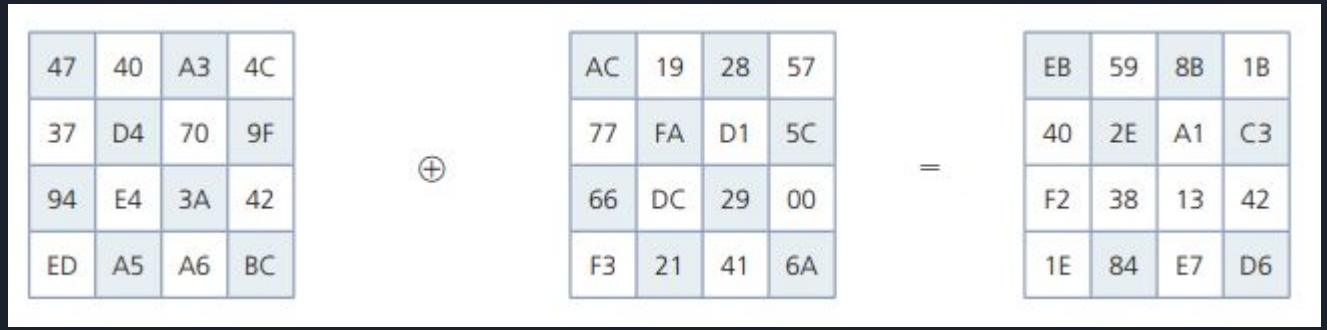
Único estágio de permutação do AES, os demais são de substituição de bytes

- Deslocamento
  - Primeira linha — não é alterada
  - Segunda linha — deslocamento circular a direita de 1 byte
  - Terceira linha — deslocamento circular a direita de 2 bytes
  - Quarta linha — deslocamento circular a direita de 3 bytes
- InvShiftRows — realiza o deslocamento circular na direção oposta

Fase de Mixagem de Colunas



Fase de Adição de Chave de Rodada



47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

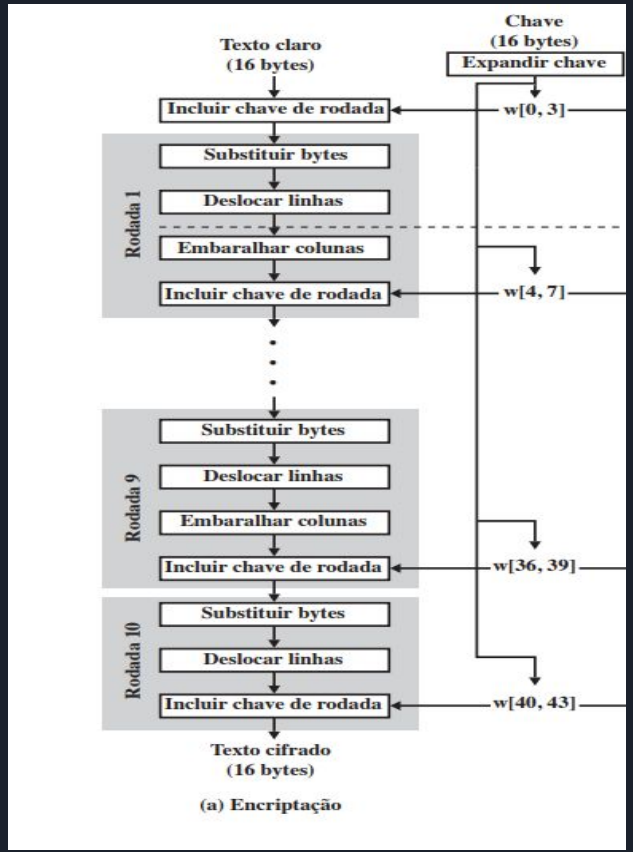
⊕

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

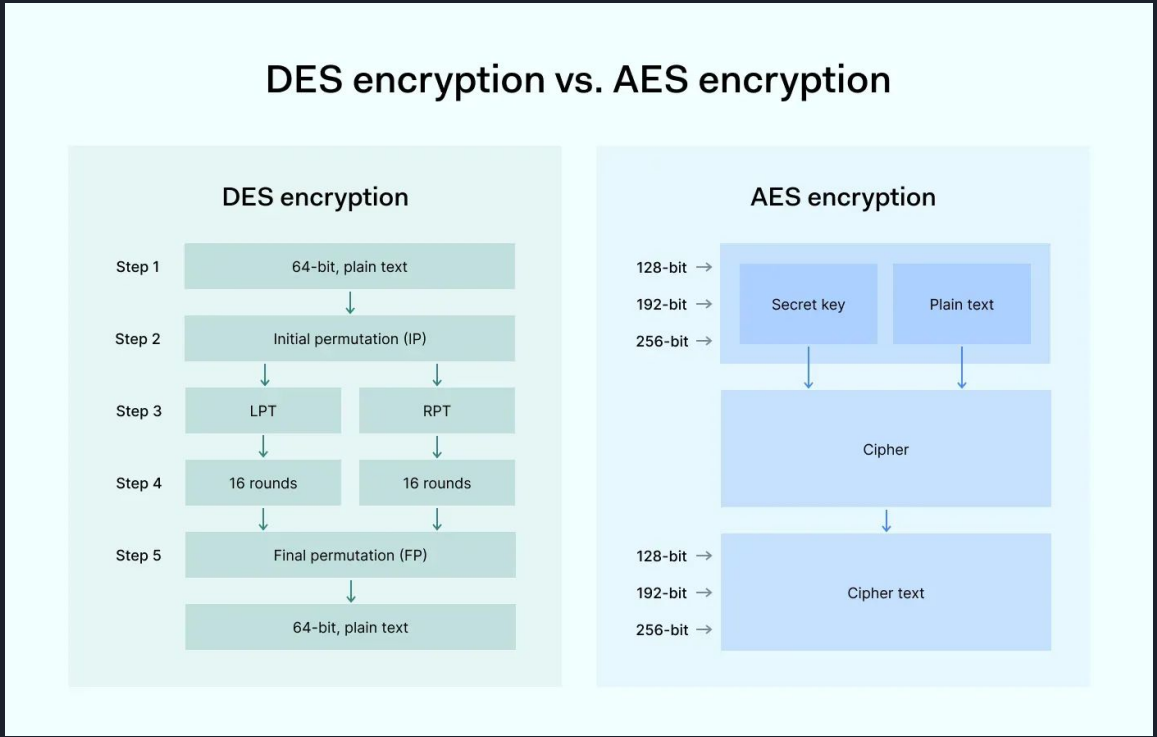
Dado criptografado



Referência Bibliográfica

STARLLINGS, Willian. Criptografia e Segurança de Redes Princícios e Práticas. 6. ed.

Teste comparativo das duas estratégias de criptografia



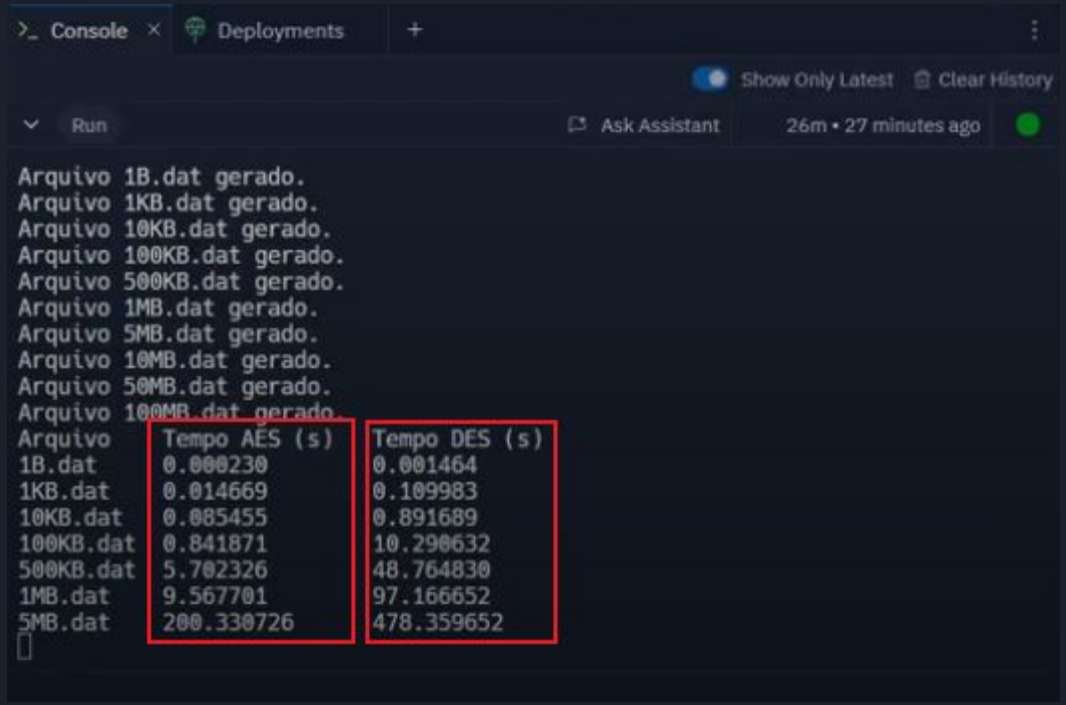
Resultado da análise dos nossos testes

AES

- Desempenho e eficiência maior, chegando da GB/s
- Mais difícil de implementar, mas tem muito suporte devido à adoção mundial do seu uso, com bibliotecas e módulos otimizados facilmente encontrados
- É o padrão para criptografia simétrica, não tem vulnerabilidades práticas, o uso de blocos grandes e de chaves maiores protege contra ataques de força bruta também

DES

- Desempenho mais baixo, especialmente em arquivos muito grandes
- Mais simples a implementação, mas ela vem acompanhada de limitações de segurança sérias
- Blocos e chaves mais diminutas consideradas insuficientes pros padrões atuais, técnicas avançadas de força bruta quebram o DES, deixando informações vulneráveis.


Console
Deployments
Show Only Latest
Clear History
Run
Ask Assistant
26m • 27 minutes ago
Arquivo 1B.dat gerado.
Arquivo 1KB.dat gerado.
Arquivo 10KB.dat gerado.
Arquivo 100KB.dat gerado.
Arquivo 500KB.dat gerado.
Arquivo 1MB.dat gerado.
Arquivo 5MB.dat gerado.
Arquivo 10MB.dat gerado.
Arquivo 50MB.dat gerado.
Arquivo 100MB.dat gerado.
Arquivo Tempo AES (s) Tempo DES (s)
1B.dat 0.000230 0.001464
1KB.dat 0.014669 0.109983
10KB.dat 0.085455 0.891689
100KB.dat 0.841871 10.290632
500KB.dat 5.702326 48.764830
1MB.dat 9.567701 97.166652
5MB.dat 200.330726 478.359652

Obrigado!