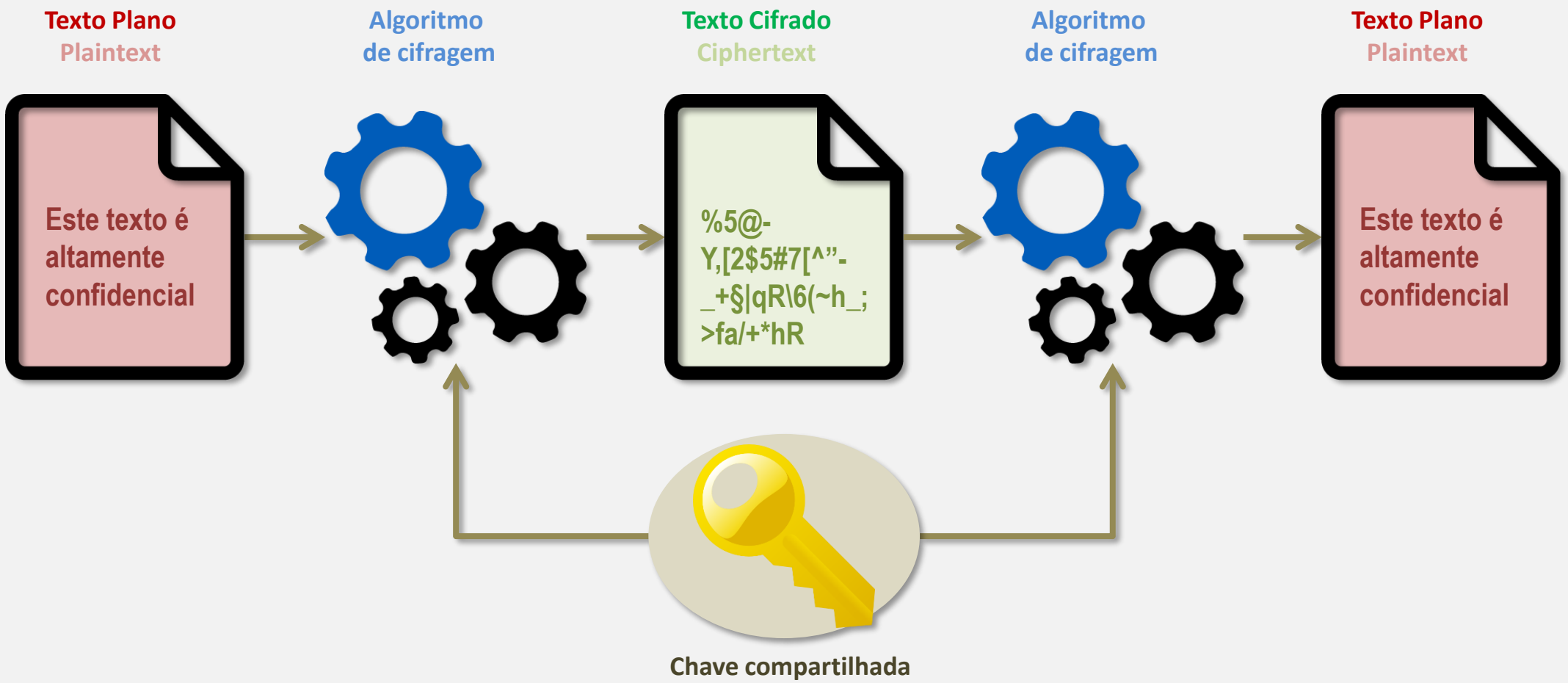
INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA
PARAÍBA

Criptografia Simétrica

Dênio Mariz, PhD
denio@ifpb.edu.br

Fevereiro, 2020

Criptografia Simétrica



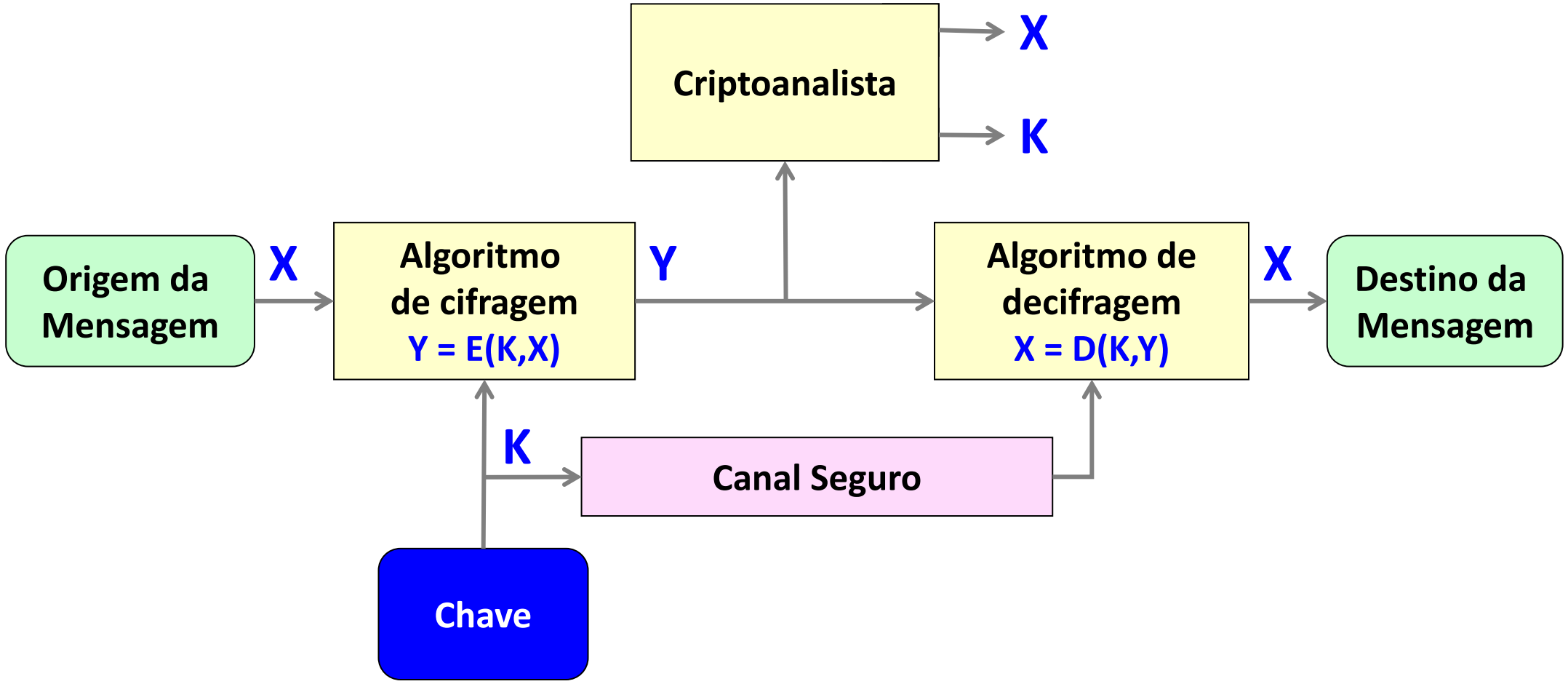
Criptografia Simétrica

- Alice e Bob concordam com
  - um método de criptografia
  - uma chave compartilhada (shared key)
- Alice
  - usa a chave e o método de criptografia para crifrar a mensagem
  - envia a mensagem cifrada para Bob
- Bob
  - usa o mesmo método e a mesma chave para decifrar a mensagem

- Criptografia Simétrica
- Criptografia clássica
- Criptografia de chave secreta

Mesmo significado

Criptografia Simétrica



Obs: O texto cifrado Y não contém informações sobre a chave K

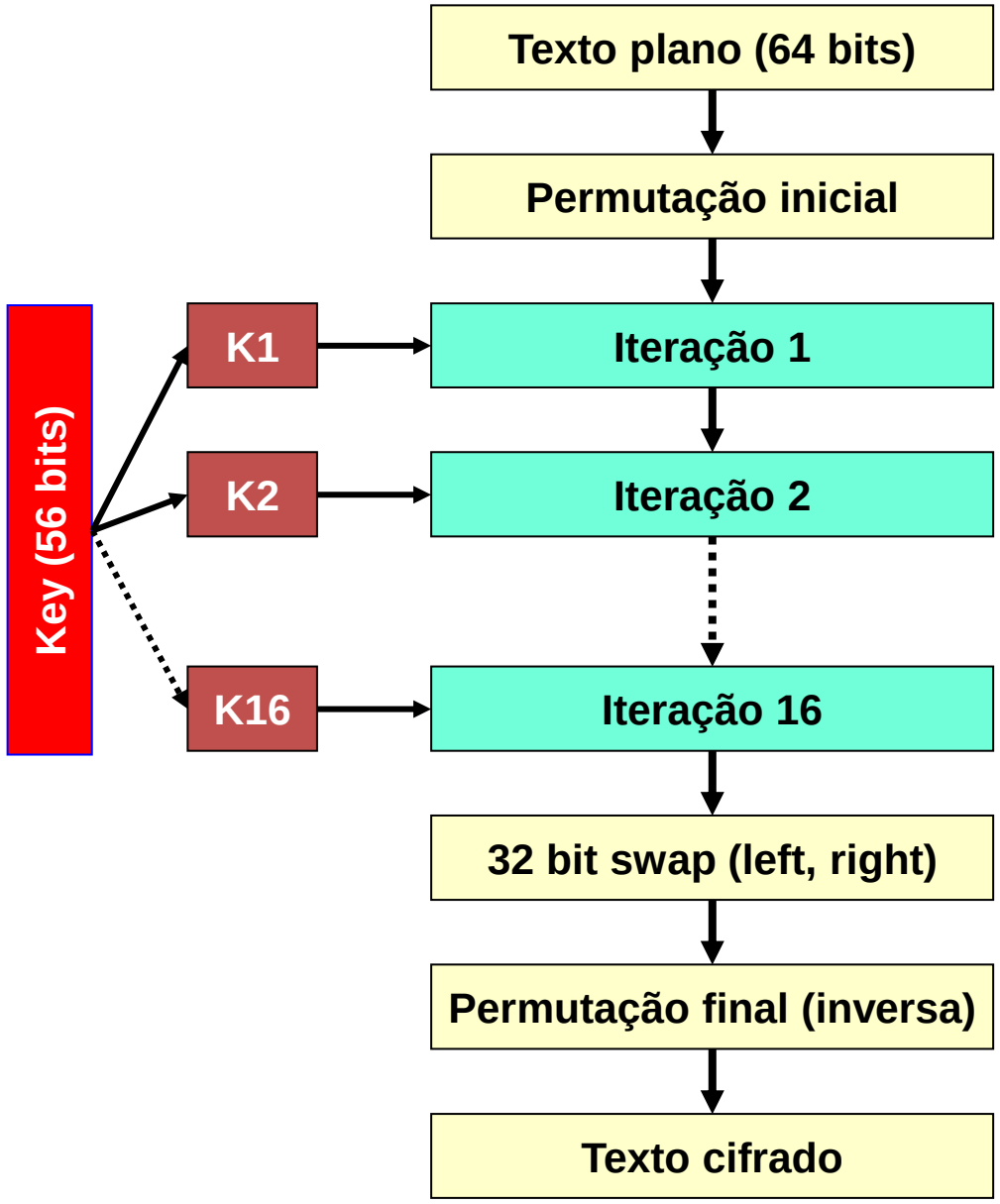
Vantagens da criptografia simétrica

- Vantagens
  - Os algoritmos são rápidos !
- Desvantagens
  - Requer a transmissão segura da chave
  - Alice precisa de uma uma chave separada para cada pessoa com a qual deseja se comunicar
  - Não permite implementar "Não-repúdio"

Data Encryption Standard

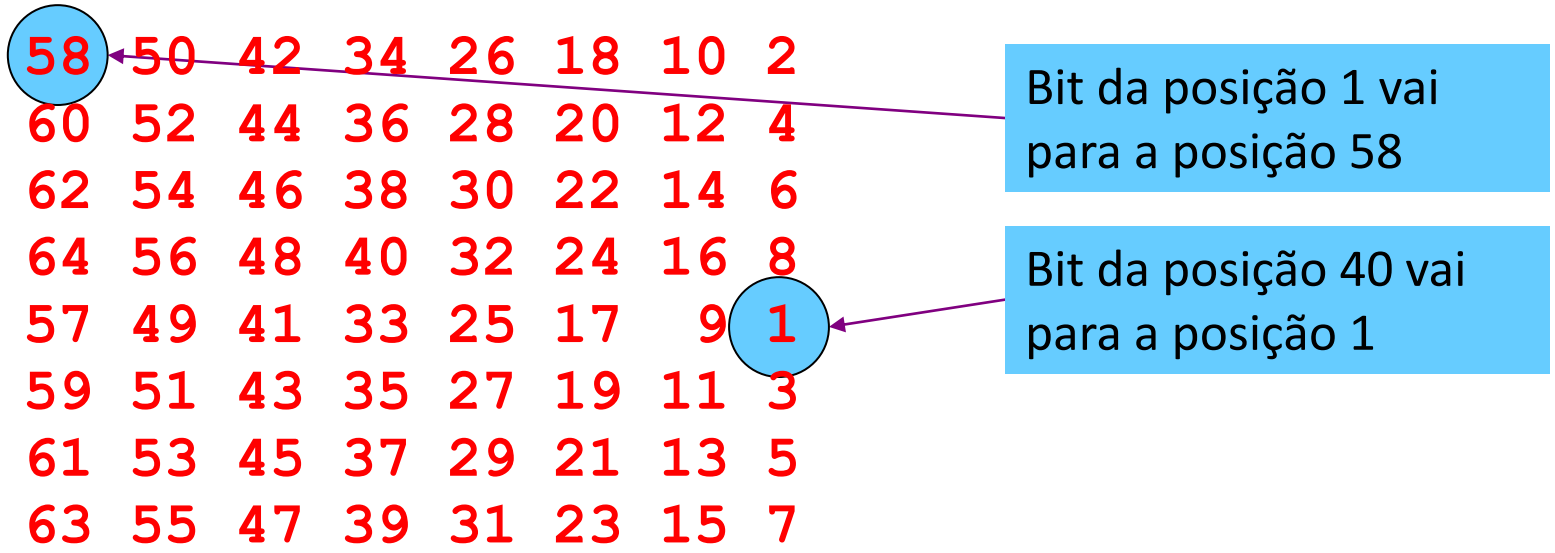
- DES (Data Encryption Standard)
  - Exemplo mais difundido de cifrador simétrico
  - Desenvolvido pela IBM
  - Adotado como padrão nos EUA em 1977-1996
- Divide a mensagem em blocos de 64 bits (8 caracteres)
- Cifra cada bloco com uma chave de 56 bits
- Cria inicialmente 16 chaves derivadas
- DES trabalha em 16 rodadas (rounds)
- Cada rodada aplica uma transformação da entrada e combina com uma chave

DES (visão geral)



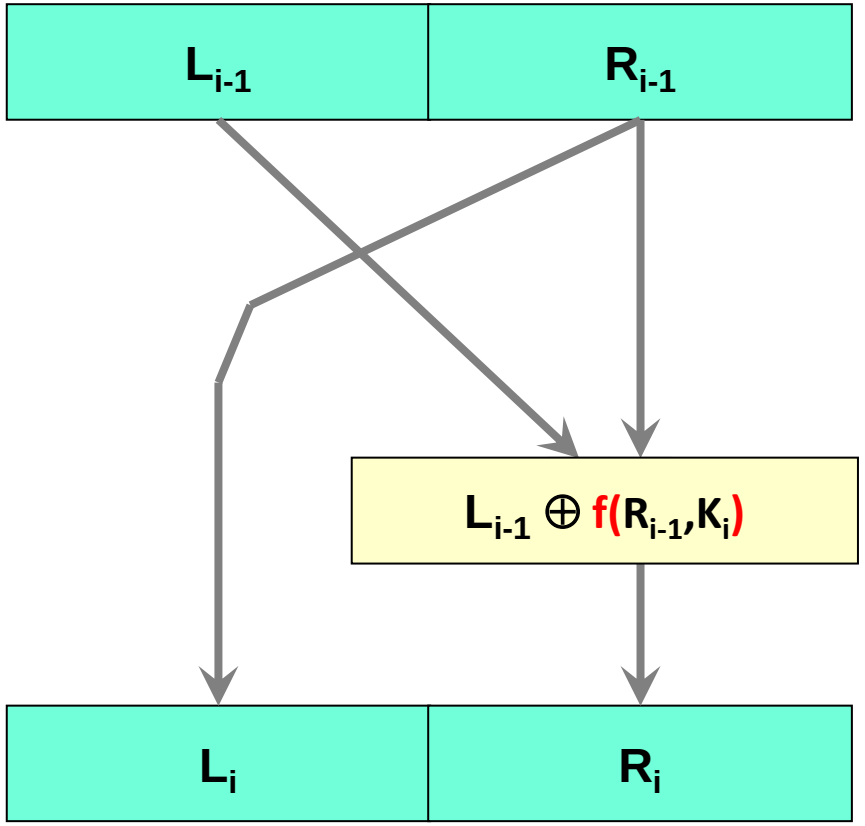
DES (permutações)

- Permutação inicial



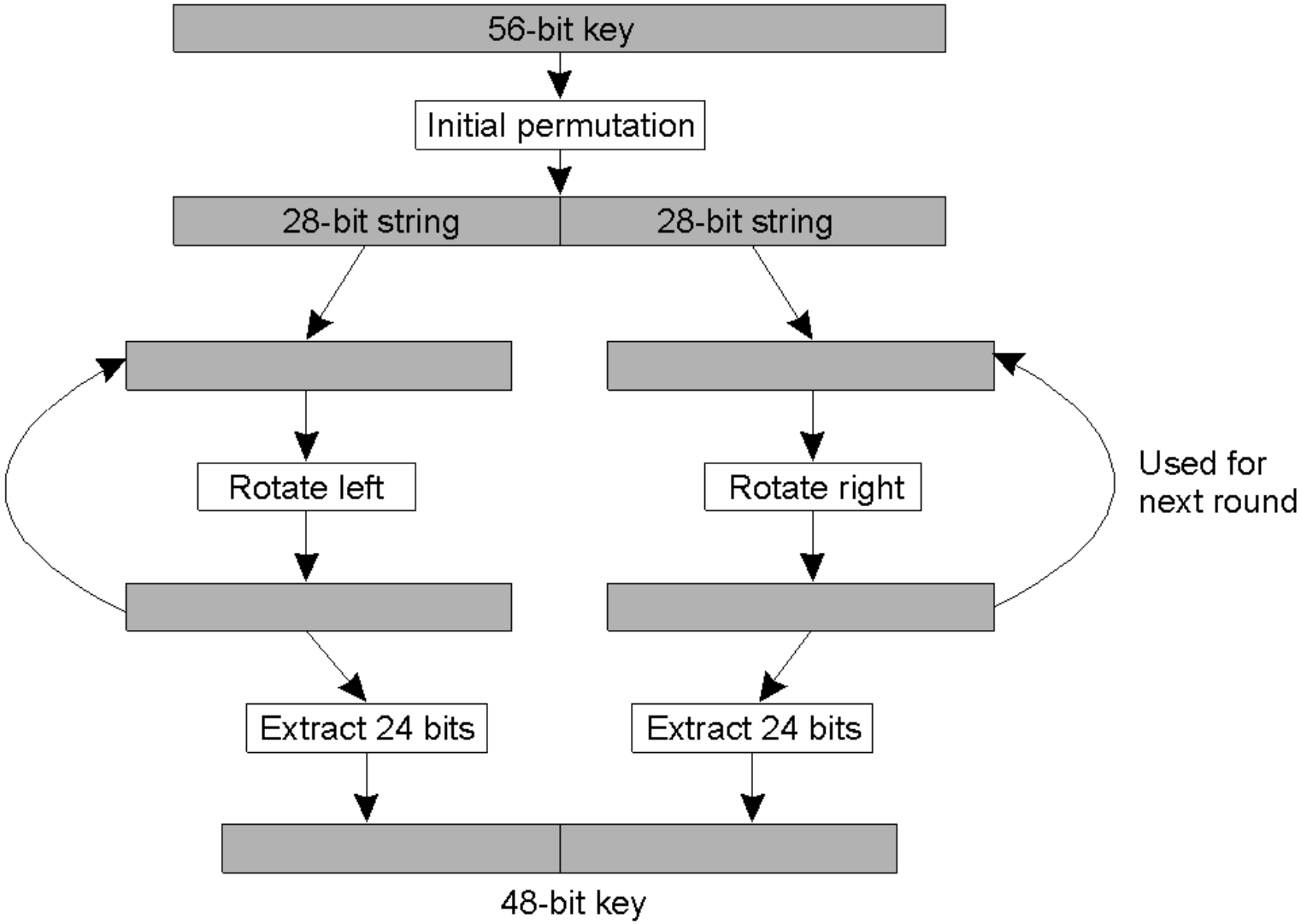
- Permutação final faz o inverso

DES (iteração)



A cada iteração i, a função **f()** mescla o texto plano com pedaços da chave

DES (sub-chaves)



XOR (Exclusive OR)

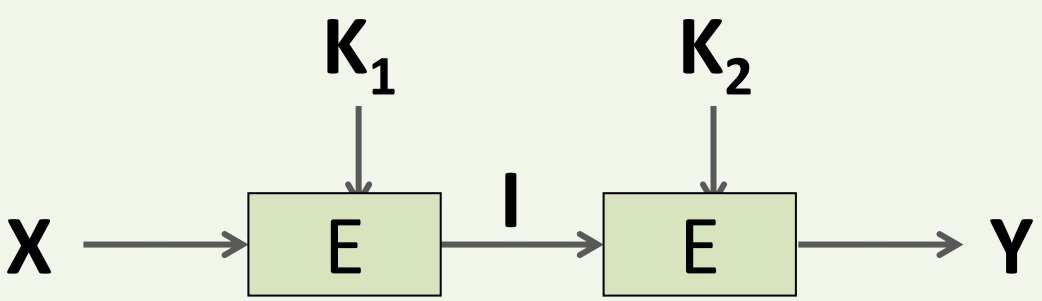
X	K	Y
0	1	1
0	0	0
1	1	0
1	0	1

DES ficou obsoleto

- Poder computacional “enfraquece” sistemas
- Seguro até quando ?
- DES é vulnerável a ataques de força bruta
  - 2^{56} chaves possíveis (72 057 594 037 927 936)
  - 96^{8} chaves digitáveis (reduz ~10 vezes)
  - 2^{47} ou 2^{43} tentativas (outras técnicas)
- Solução?
  - Cifragem Múltipla

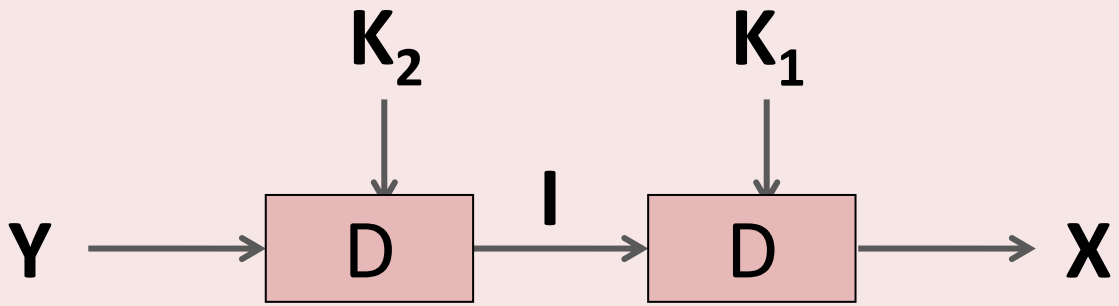
Cifragem Dupla

$Y=E(K_2, E(K_1, X))$



Cifrar

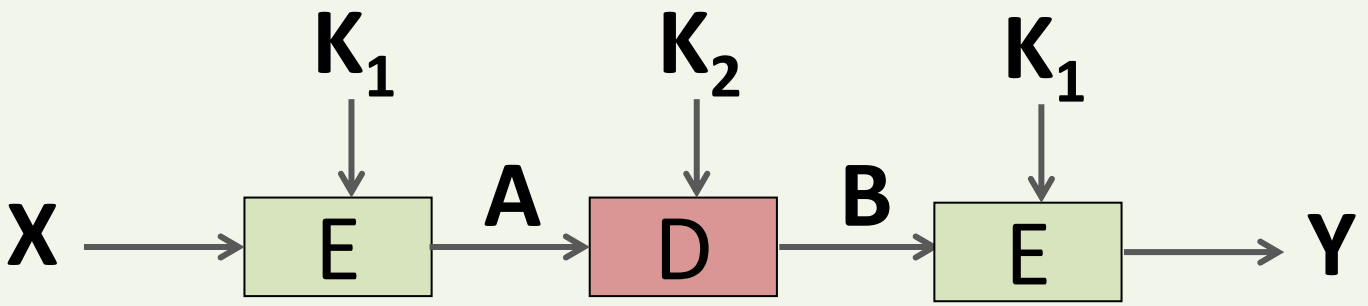
$X=D(K_1,D(K_2,Y))$



Decifrar

3DES (triple DES)

$$Y=E(K_1, D(K_2, E(K_1, X)))$$



Cifrar

3DES

- Ataque da força bruta no 3-DES é da ordem de 2^{112}
  - 5 192 296 858 534 827 628 530 496 329 220 096
- Outros algoritmos de chave simétrica
  - Lucifer, Madryga, NewDES, FEAL-N, REDOC II e III
  - LOKI, Khufu e Khafre, Blowfish, IDEA,
  - SAFER, RC4, RC5, RC6, Rijndael

AES - Advanced Encryption Standard

- Padrão de criptografia simétrica definido pelo NIST, EUA
- O Algoritmo **DES** foi o **AES** de 1977 até 2000
- Em 1997 NIST abriu um concurso para o sucessor para o DES
  - Finalistas: Rijndael, Serpent, Twofish, RC6, MARS
- Em Out-2000 NIST anuncia **Rijndael** como vencedor
- O Algoritmo **Rijndael** é o atual o **AES** desde 2000

> "O NIST estima que a menos que a computação quântica se torne realidade, o Rijndael irá permanecer seguro pelos próximos 30 anos. Computadores atuais levariam 149 trilhões de anos para quebrá-lo."
>
> **The New York Times, 3-Oct-2000**
> http://www.nytimes.com/2000/10/03/technology/03CODE.html

- Demonstração do Algoritmo Rinjdael
  - https://www.youtube.com/embed/gP4PqVGudtg