Criptografia Simétrica

Cifra de bloco

Prof. Roberto Rodrigues-Filho
Dept. de Ciência da Computação (CIC)
Universidade de Brasília (UnB)

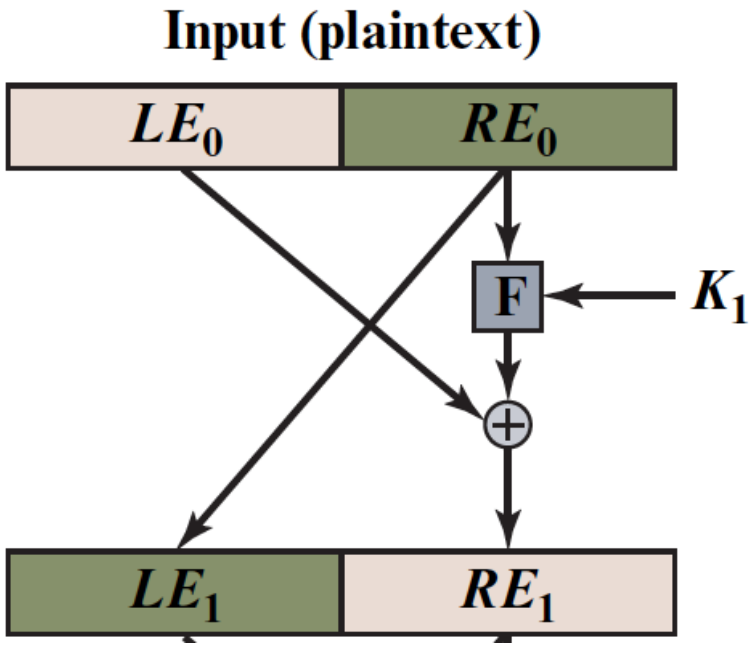
Criptografia Simétrica

- Confusão e Difusão
  - O ideal seria ter cifras que não transpareça propriedades estatíscas
  - **Shanon**: Vamos combinar substituição e transposição
  - Difusão: aumentar a complexidade da relação entre texto cifrado e texto claro
  - Confusão: aumenta a complexidade da relação entre texto cifrado e o valor da chave

roberto.filho@unb.br

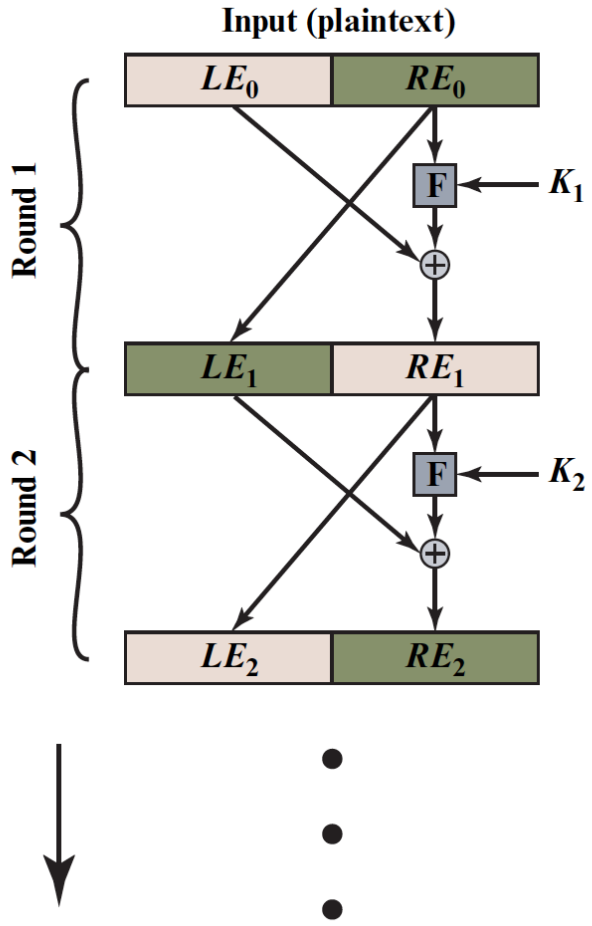
Criptografia Simétrica

- Estrutura Feistel



Criptografia Simétrica

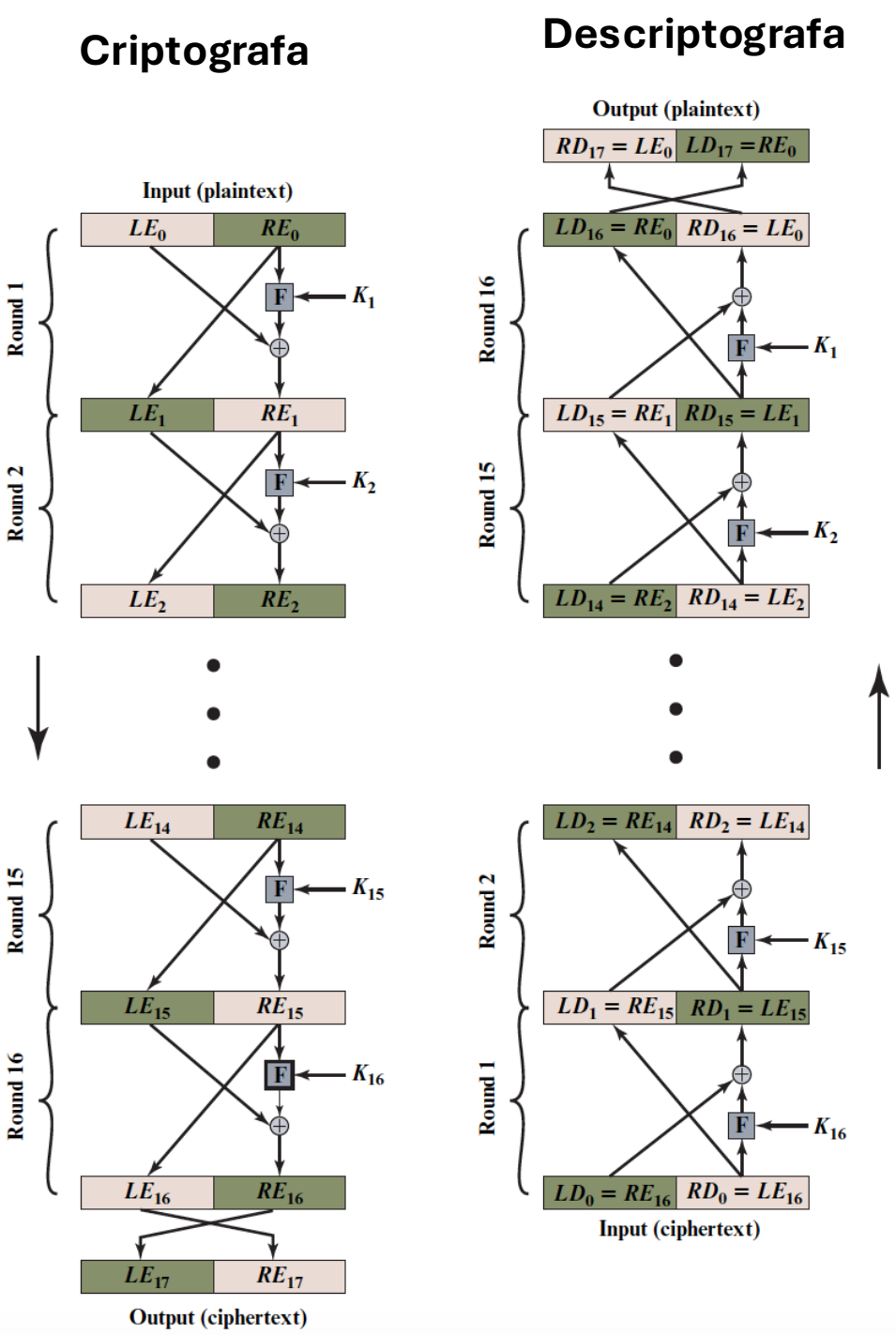
- Rede de Feistel



roberto.filho@unb.br

roberto.filho@unb.br

Algoritmo

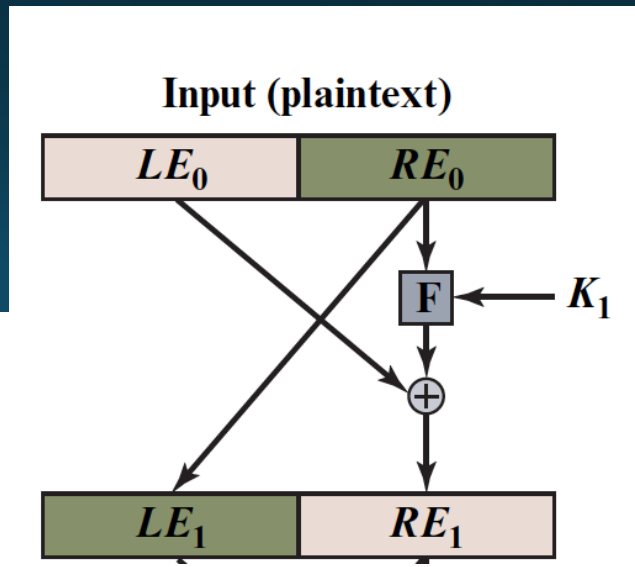


Criptografia Simétrica

- Exemplo:
  - Mensagem: 10100101
  - Chave: k0 = 0011; k1 = 0111; k2 = 0010; k3 = 0101;
  - F (R, K) = S[R + K]

Entrada	Saida	Entrada	Saida
0000	1110	1000	0011
0001	0100	1001	1010
0010	1101	1010	0110
0011	0001	1011	1100
0100	0010	1100	0101
0101	1111	1101	1001
0110	1011	1110	0000
0111	1000	1111	0111

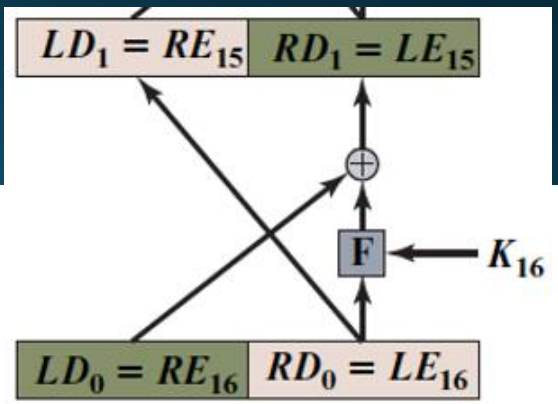
Criptografia Simétrica



- Exemplo:
  - Mensagem: 11010110
  - Chave: k0 = 0011; k1 = 1010; k2 = 0101; k3 = 1111;
  - F(R,K) = $S(R \oplus K)$

Entrada	Saida	Entrada	Saida
0000	1110	1000	0011
0001	0100	1001	1010
0010	1101	1010	0110
0011	0001	1011	1100
0100	0010	1100	0101
0101	1111	1101	1001
0110	1011	1110	0000
0111	1000	1111	0111

Criptografia Simétrica



- Exemplo:
  - Mensagem: 11010110
  - Chave: k0 = 0011; k1 = 1010; k2 = 0101; k3 = 1111;
  - F(R,K) = $S(R \oplus K)$

Entrada	Saida	Entrada	Saida
0000	1110	1000	0011
0001	0100	1001	1010
0010	1101	1010	0110
0011	0001	1011	1100
0100	0010	1100	0101
0101	1111	1101	1001
0110	1011	1110	0000
0111	1000	1111	0111

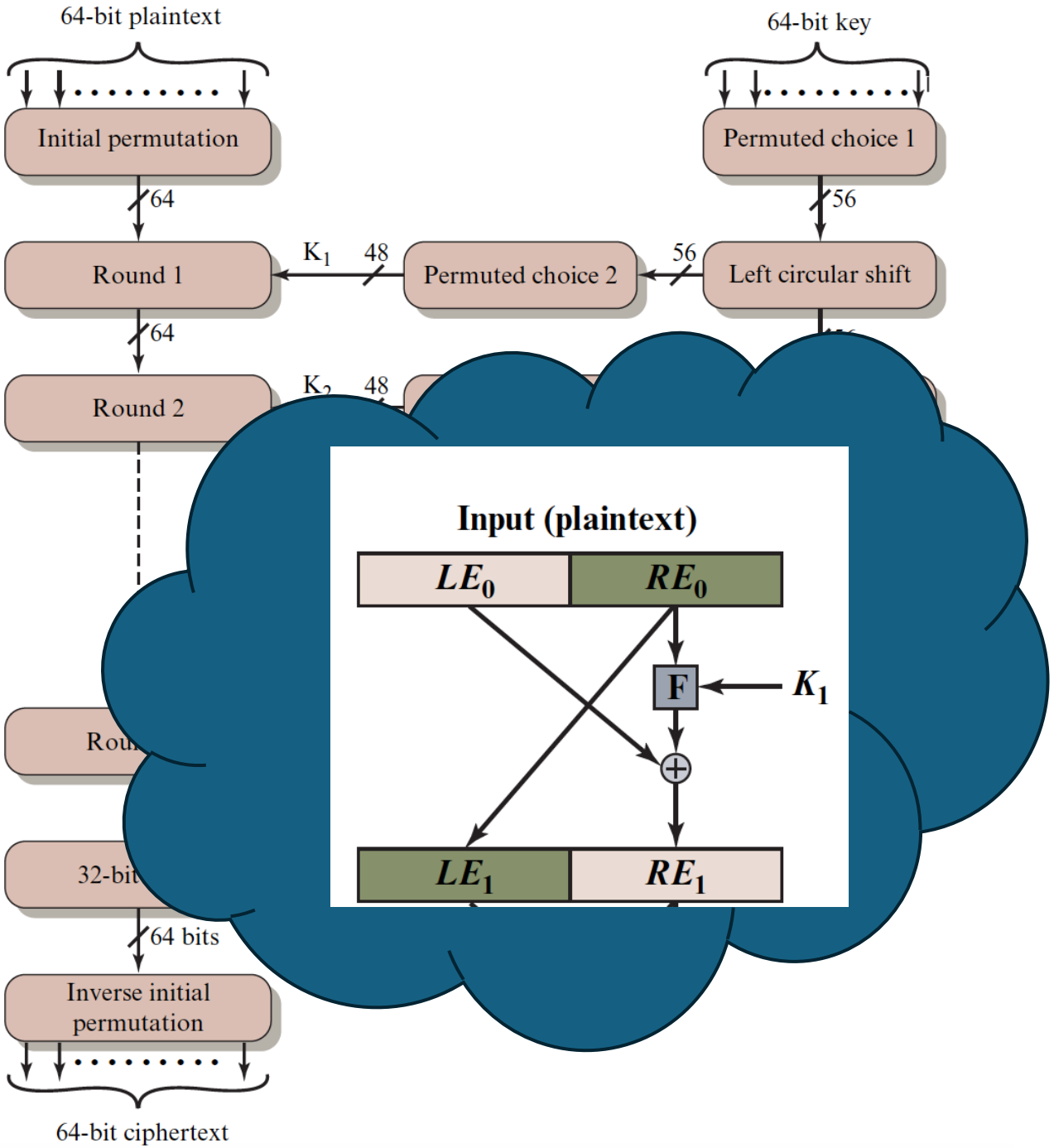
Criptografia Simétrica

- Data Encryption Standard (DES)
  - Bloco de **64 bits** de entrada (texto claro).
  - Chave de **56 bits** (efetivos).
  - **16 rodadas** da rede de Feistel.
  - Função **F(R, K)** baseada em:
    - Expansão (de 32 para 48 bits).
    - XOR com subchave.
    - Passagem pelas **S-boxes** (não linearidade).
    - Permutação final (mistura os bits).

roberto.filho@unb.br

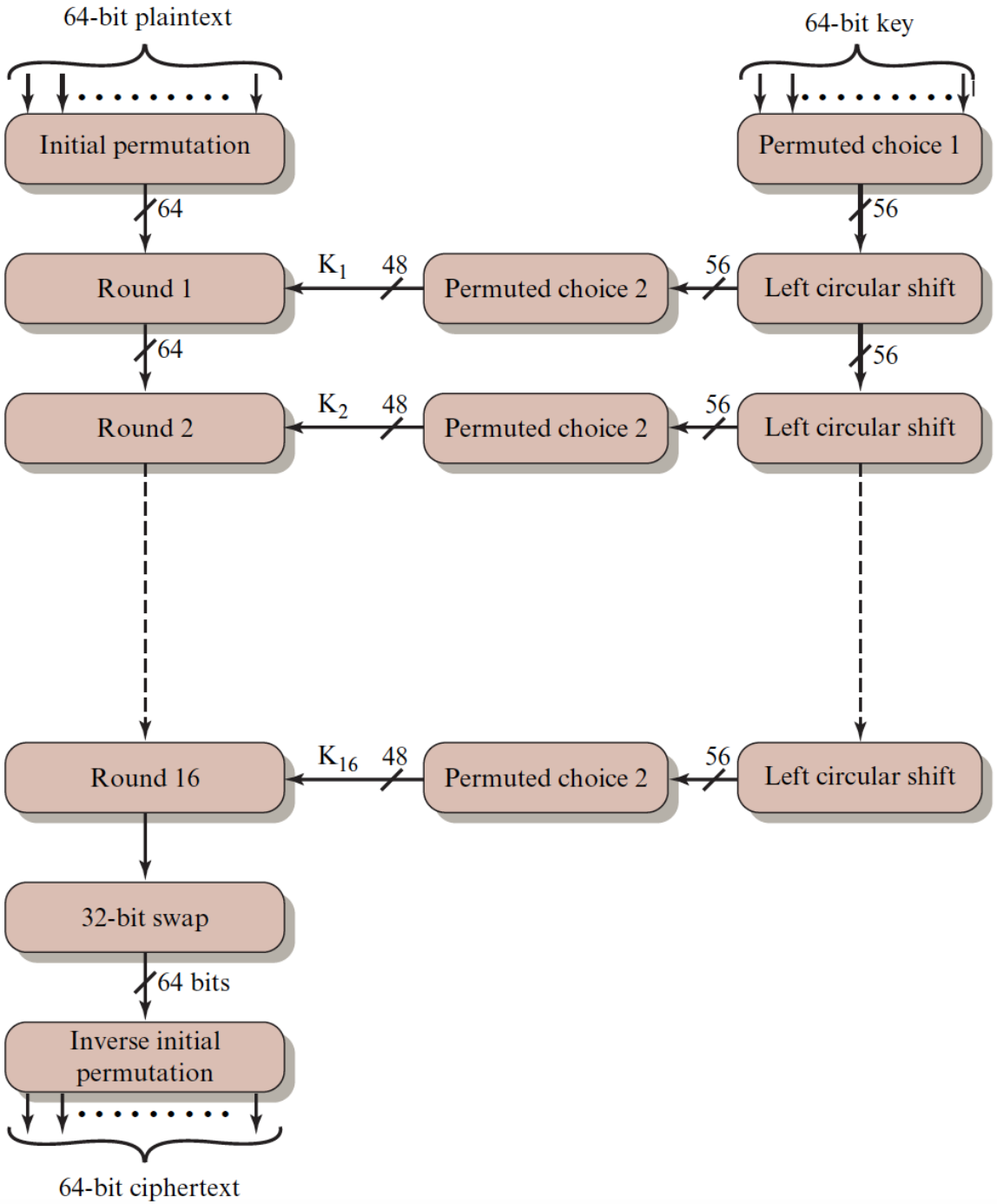
roberto.filho@unb.br

DES



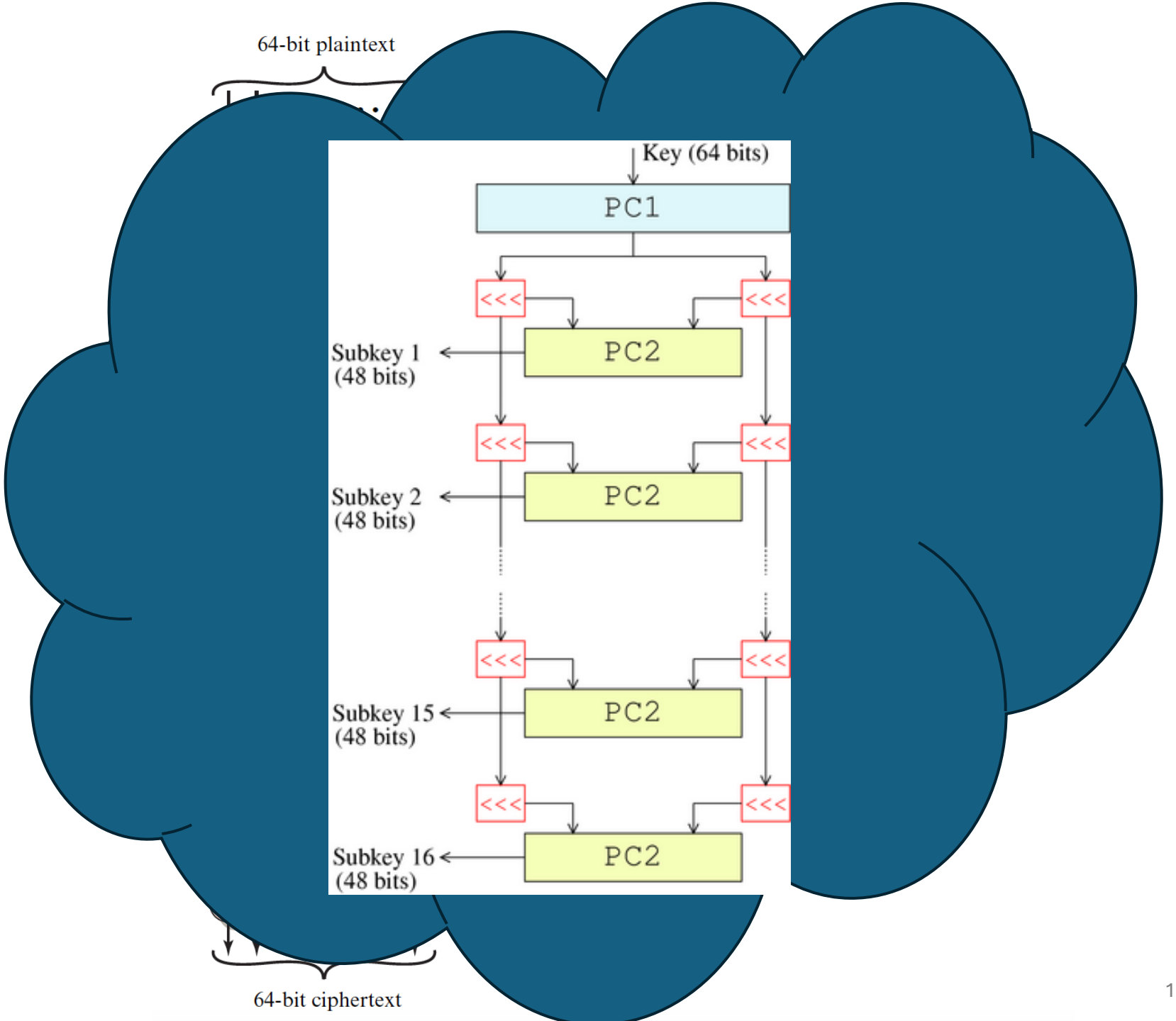
roberto.filho@unb.br

DES



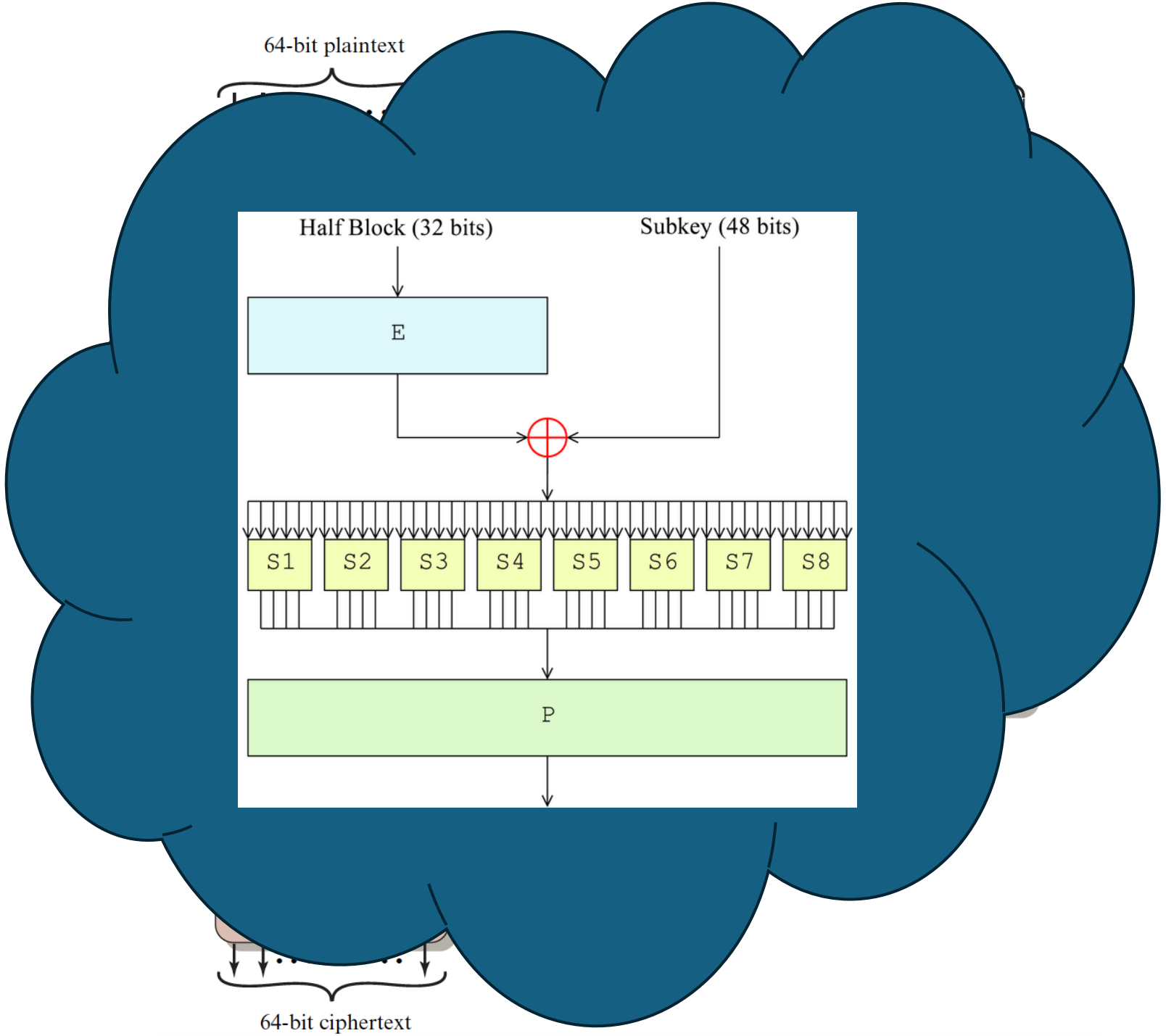
roberto.filho@unb.br

DES



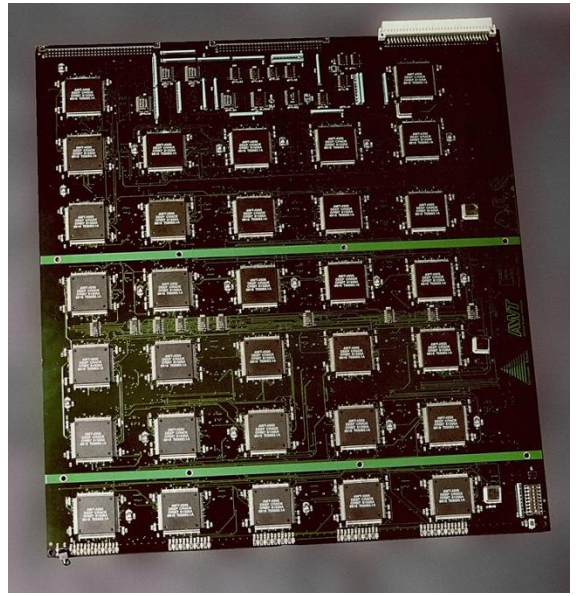
roberto.filho@unb.br

DES



Criptografia Simétrica

- Data Encryption Standard (DES)
  - Efeito avalanche:
    - Uma mudança no texto ou na chave → grande mudança
    - 1 bit modificado muda em torno da metade dos bits de saída
  - Chave de 56-bit → 2^56 = 1.8 * 10^16 possibilidades
  - Força?
    - 1997 – meses
    - 1998 – dias – deep crack
    - 1999 – 22 horas
  - Obsoleto:
    - 3DES
    - AES



roberto.filho@unb.br