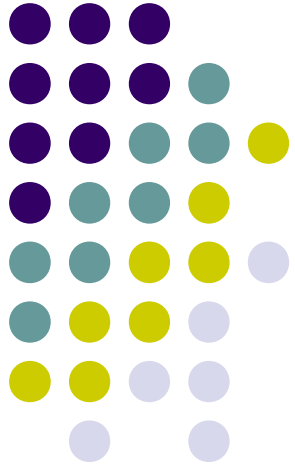
Segurança Computacional

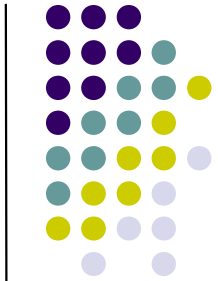
Aula 03: Criptografia, Algoritmos e Criptoanálise

Prof.
Valério Rosset



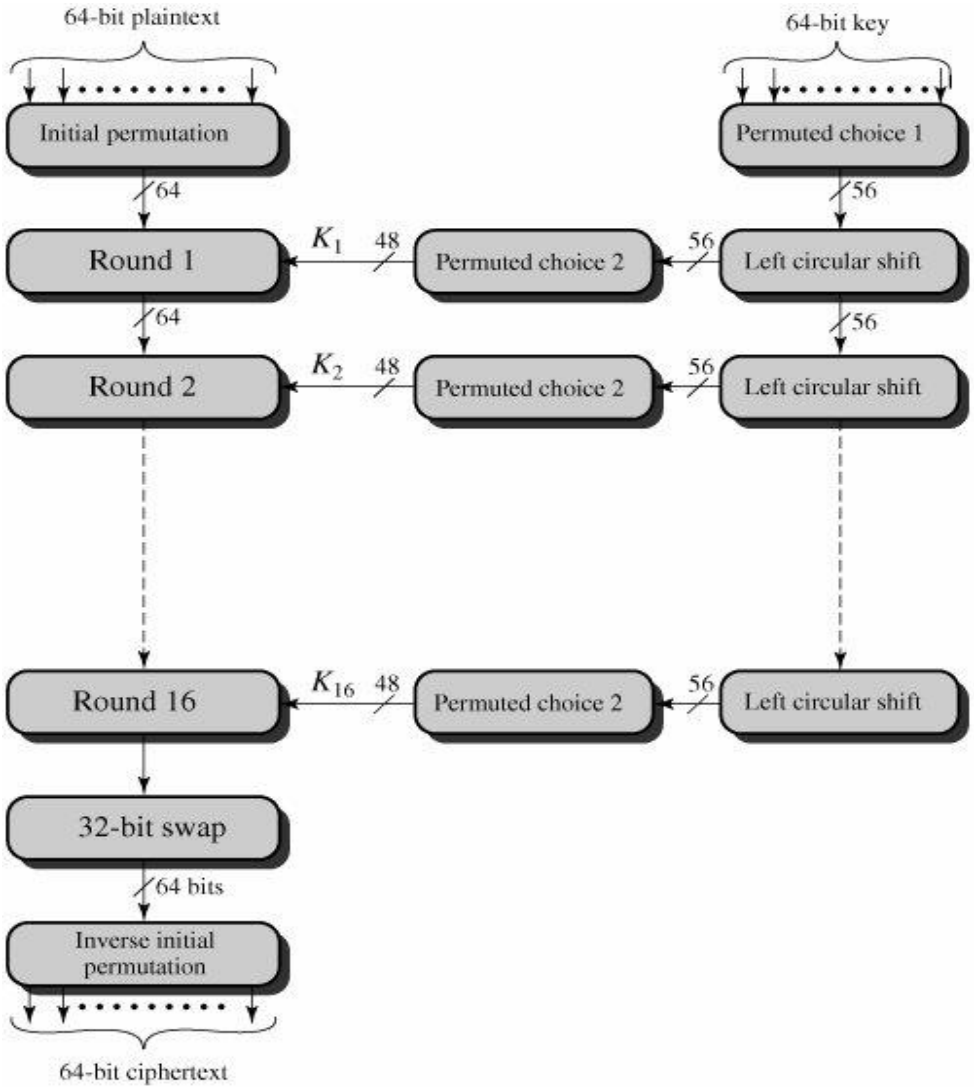
Apresentação baseada no Livro Criptografia e Segurança de Redes: Princípios e Prática, 4a Ed. de William Stallings.

Data Encryption Standard – DES/DEA



- DEA- *Data Encryption Algorithm* foi adotado pelo *National Institute of standards and Technology* (NIST) em 1977.
- Dados são codificados em blocos de 64 bits
  - (8 bits do S-DES)
- Chave tem tamanho 56 bits
  - (10 bits do S-DES)
- 16 Rodadas com 16 sub-chaves geradas

Data Encryption Standard – DES/DEA



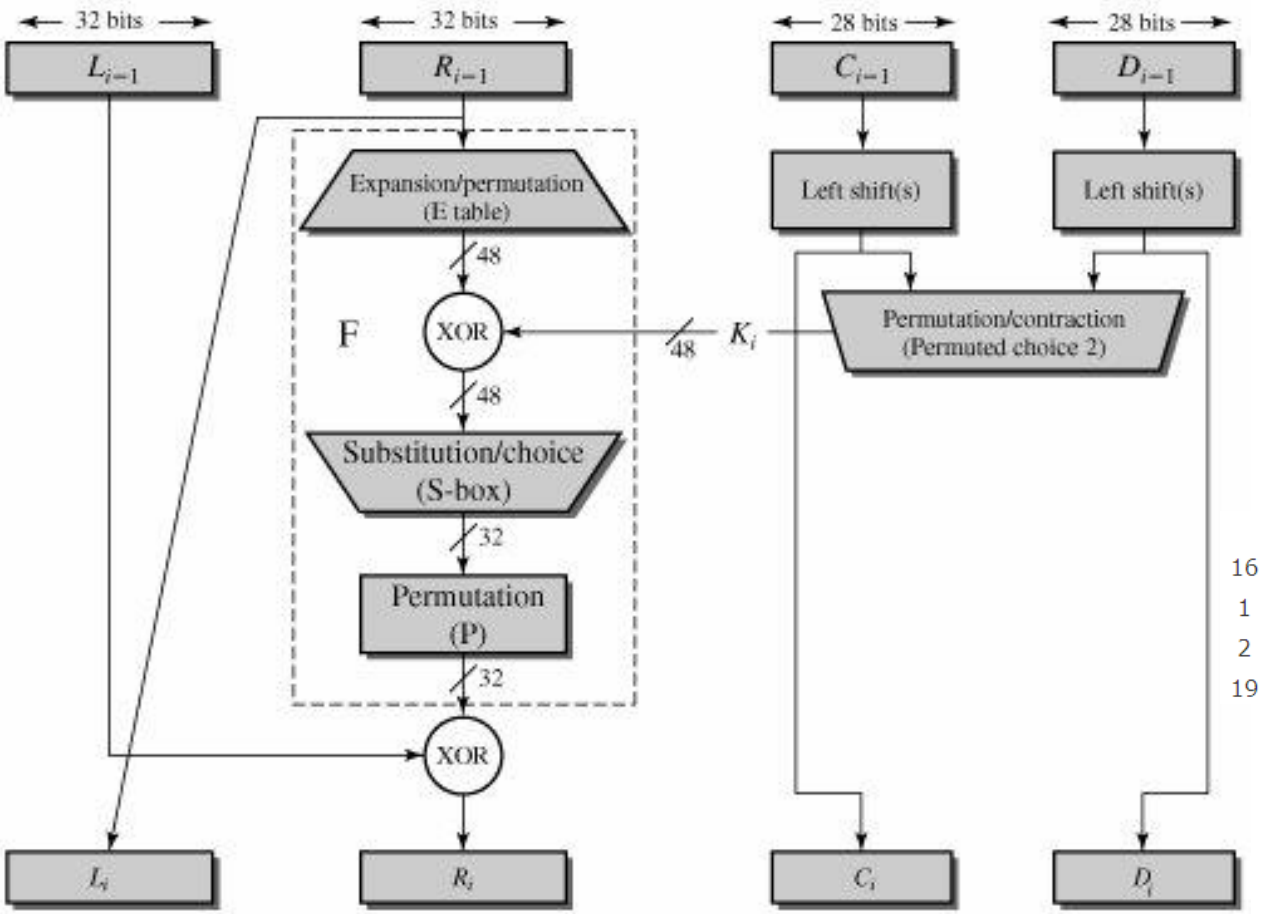
(a) Initial Permutation (IP)

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

(b) Inverse Initial Permutation (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

Data Encryption Standard – DES/DEA



(c) Expansion Permutation (E)

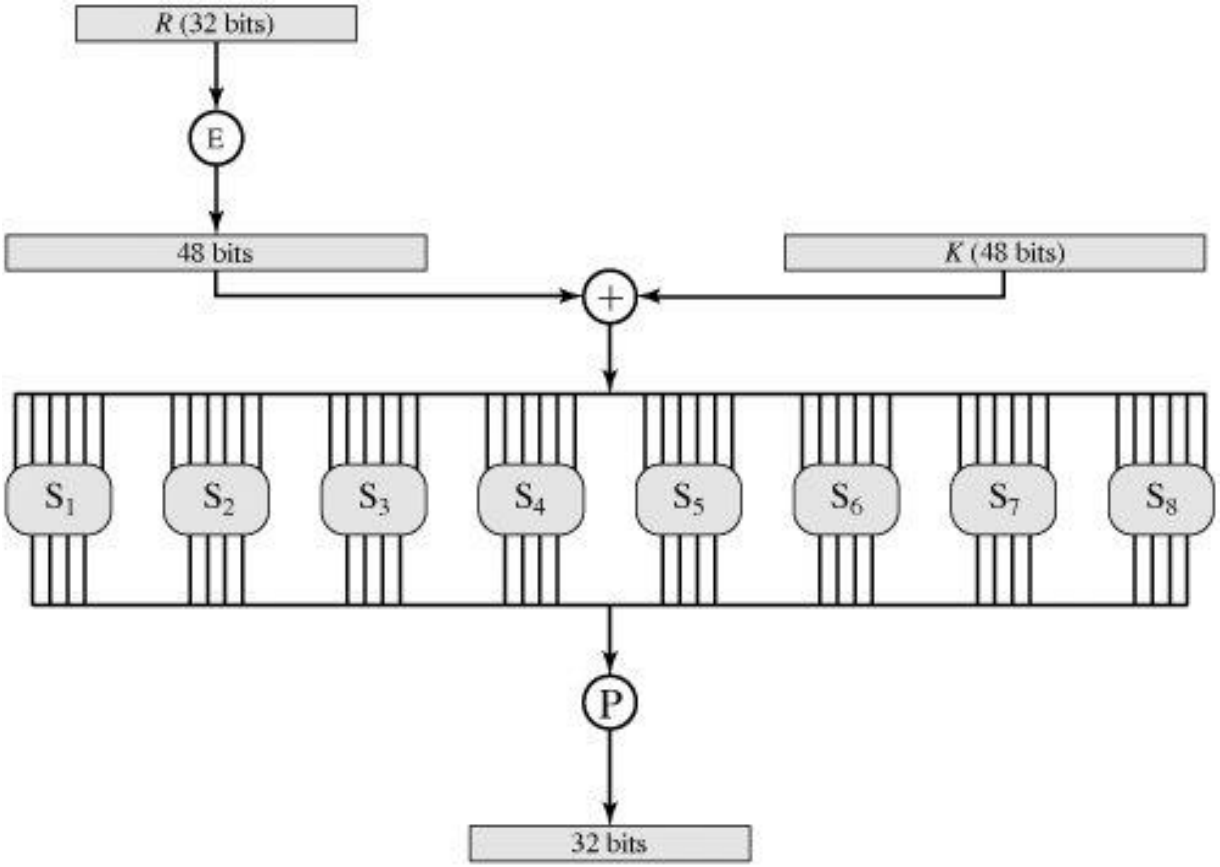
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Data Encryption Standard – DES/DEA

- **F(R,K)**



S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

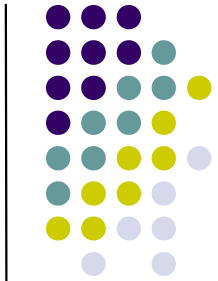
S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Efeito avalanche do DES



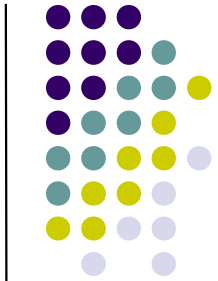
Texto Claro:

- **0**0000000 00000000 00000000 00000000
  00000000 00000000 00000000 00000000
- **1**0000000 00000000 00000000 00000000
  00000000 00000000 00000000 00000000

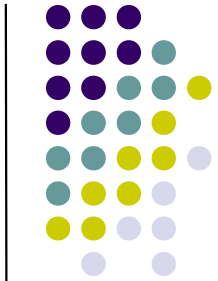
Chave

- 0000001 1001011 0100100 1100010
  0011100 0011000 0011100 0110010

(a) Change in Plaintext	
Round	Number of bits that differ
0	1
1	6
2	21
3	35
4	39
5	34
6	32
7	31
8	29
9	42
10	44
11	32
12	30
13	30
14	32



Efeito avalanche do DES

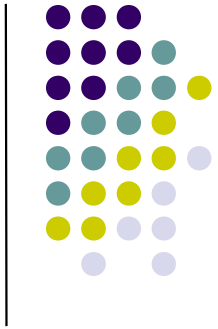


Texto Claro:

- 01101000 10000101 00101111 01111010 00010011 01110110 11101011 10100100

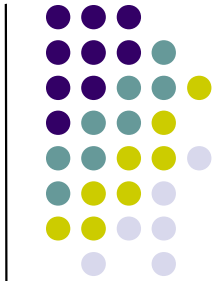
Chave

- **1**1110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100
- **0**110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100



(b) Change in Key	
Round	Number of bits that differ
0	0
1	2
2	14
3	28
4	32
5	30
6	32
7	35
8	34
9	40
10	38
11	31
12	33
13	28
14	26
15	34

DES Triplo (3-DES)

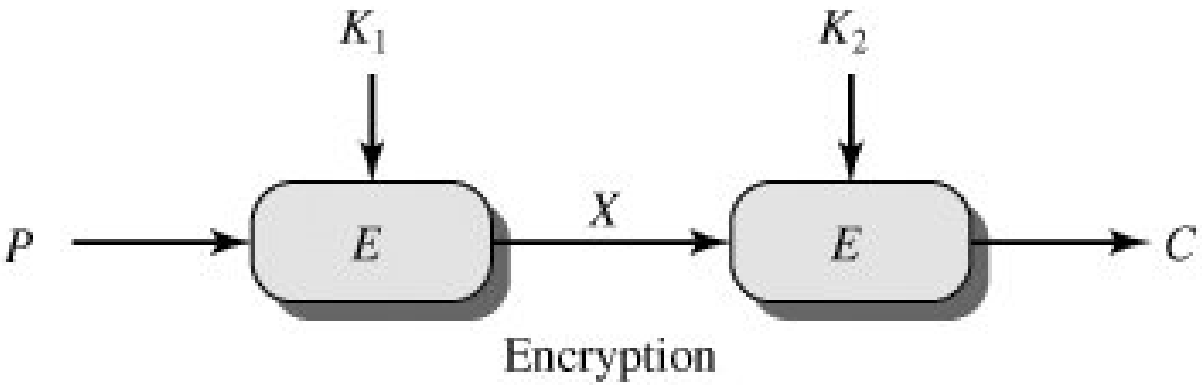


- DES, apesar de ser resistente a criptoánalise linear a diferencial ainda é relativamente fraco contra ataques de força bruta.
- Apesar de um domínio de chaves de 2^{56} o DES foi provado ser inseguro em 1998.
- Ataque com menos de 3 dias para decifrar uma chave através de uma máquina decifradora de DES com custo de 250 mil dólares.

DES Triplo (3-DES)

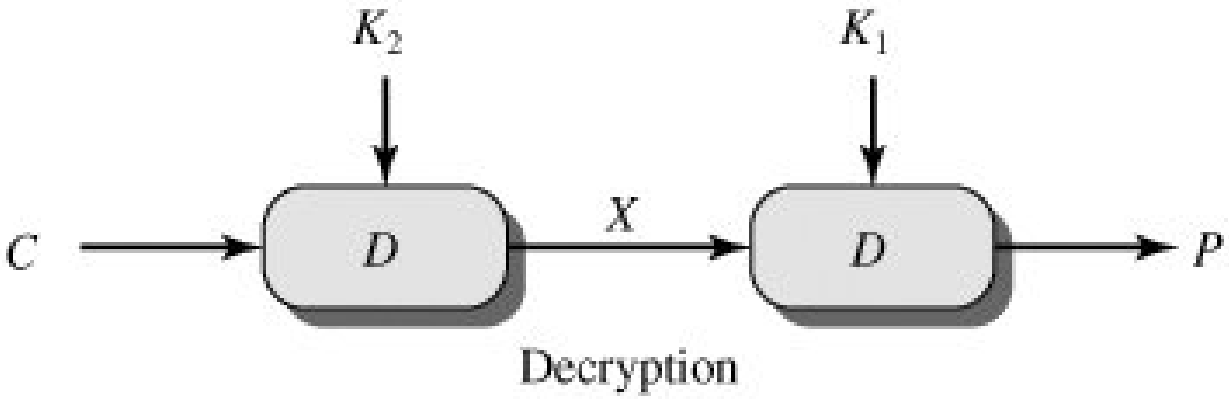
- Em alternativa ao DES foi proposto o *DES duplo*, que consiste em dois estágios do DES com duas chaves K1 e K2 aumentando o tamanho de chave = 112 bits.

- **Cifragem DES duplo: C = E(K2, E(K1,P));**



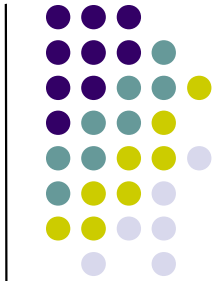
DES Triplo (3-DES)

- **Decifragem DES duplo: P =D(K1, D(K2,C));**



(a) Double encryption

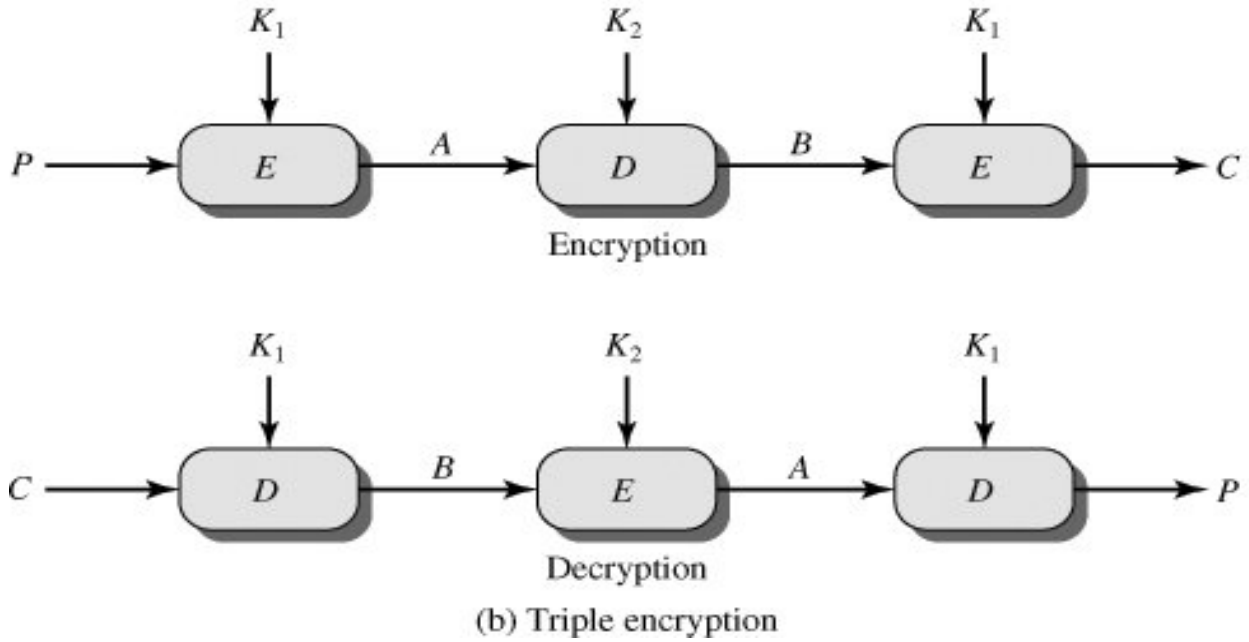
DES Triplo (3-DES)



- Apesar de ser melhor que o DES, o DES duplo pode ser atacado por um modelo que reduz o problema da descoberta da chave com esforço muito próximo ao DES normal.
- Ataque *meet-in-the-middle* baseia-se nas seguintes observações:
  - **Sendo: C=E(K2,E(K1,P))**
  - **então X = E(K1,P) = D(K2,C)**
- Dado um par conhecido (P,C) podemos proceder com o ataque de texto conhecido gerando todos os valores possíveis de E(P,K1) e todos os valores possíveis de D(C,K2). Comparamos os resultados com um novo par (P,C).

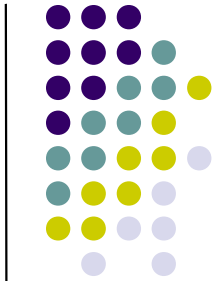
DES Triplo (3-DES)

- DES Triplo com duas chaves :
  - Chave de 112 bits, melhor desempenho, boa segurança apesar dos trabalhos demonstrarem vulnerabilidades.



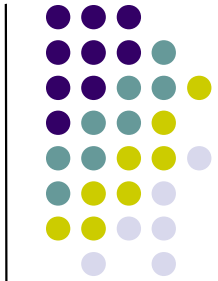
(b) Triple encryption

DES Triplo (3-DES)



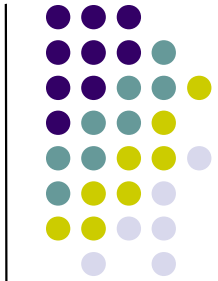
- Finalmente o DES triplo com 3 Chaves:
  - **C=E(k3,D(k2,E(k1,P)))**
- **Desconfiança na segurança do DES triplo usando 2 chaves apenas.**
- Torna-se compatível com DES quando utilizamos k3=k2 ou K2=k1.

AES – Advanced Encryption Standard



- 3DES possui grande resistência a diversos ataques sendo inclusive aos ataques de força bruta, o grande problema do seu sucessor DES.
- A grande desvantagem do 3DES é o tamanho de chave de 168 bits que em conjunto com o modelo de cifra de Feistel o torna muito lento em software.
- Por este motivo, em 1997 o NIST abriu um concurso para propostas de um novo padrão de segurança o Advanced Encryption Standard. Esse novo algoritmo deveria ser tão forte quanto o 3DES porém com eficiência e chaves maiores.

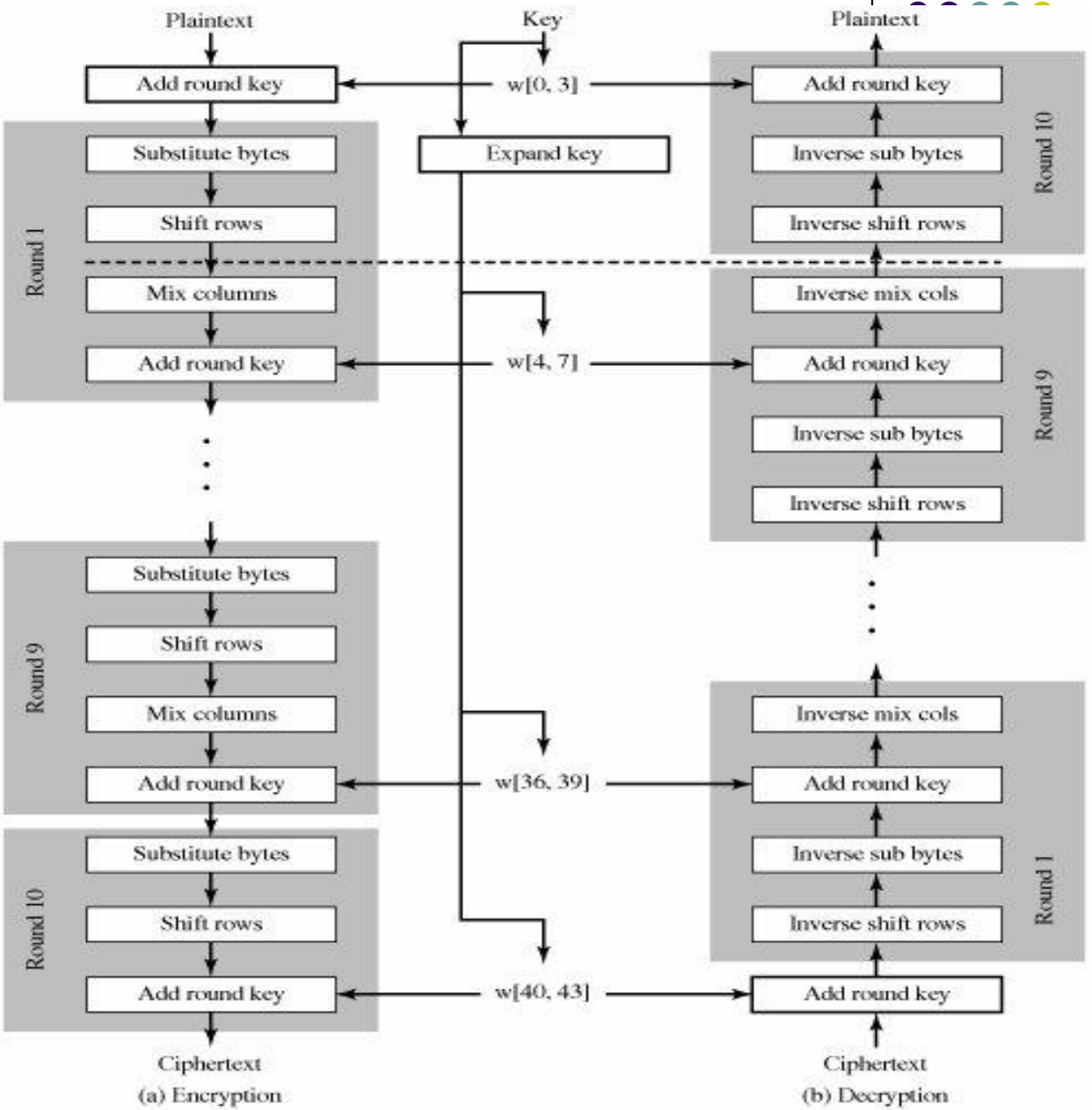
AES – Advanced Encryption Standard



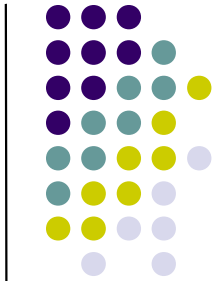
- Ao final do concurso (2001) o algoritmo escolhido foi o Rijndael desenvolvido pelos belgas Dr. Joan Daemen e Dr. Vicent Rijmen.
- Em resumo o novo AES usa um tamanho de blocos de 128 bits e chaves de tamanho 128,192 ou 256 bits.
- **Não usa a estrutura de Feistel** e a cada rodada inclui 4 funções:
  - Substituição de bytes
  - Permutação
  - Operações sobre um corpo finito
  - E operação XOR

AES

- Chave de Entrada é expandida em um vetor de 44 words.
- Sub Bytes
- ShiftRows
- MixCollumns
- AddRoundKey
- Modelo reversível porém com estruturas diferentes para cada modo E e D.



AES – Versão Simplificada

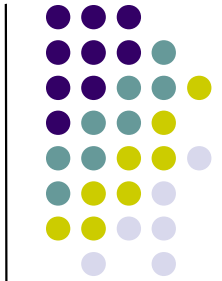


Atividade : Procure pela dissertação de mestrado abaixo, faça uma leitura do capítulo 3 sobre o modelo simplificado do AES. Escreva um resumo de como o S-AES proposto na dissertação funciona.

- MIERS, Charles Christian. UNIVERSIDADE FEDERAL DE SANTA CATARINA Programa de Pós-Graduação em Ciência da Computação. **Modelo simplificado do cifrador AES.** Florianópolis, 2002. 112 f. Dissertação (Mestrado) –

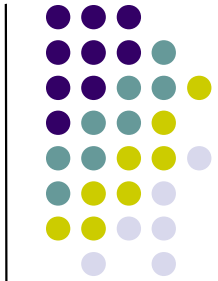
- Disponível em PDF no site da biblioteca da UFSC.

Cifras de Fluxo



- *Vimos que:*
  - Cifras de fluxo codificam um fluxo de dados por bit ou bytes de cada vez. Sua qualidade esta ligada ao tamanho da chave que deve, quanto maior a chave maior a dificuldade de revelar a mensagem.

Cifras de Fluxo

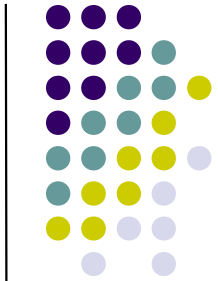


- **Exemplo**:

```
  11001100   plaintext
⊕ 01101100   key stream
  10100000   ciphertext

  10100000   ciphertext
⊕ 01101100   key stream
  11001100   plaintext
```

Cifras de Fluxo

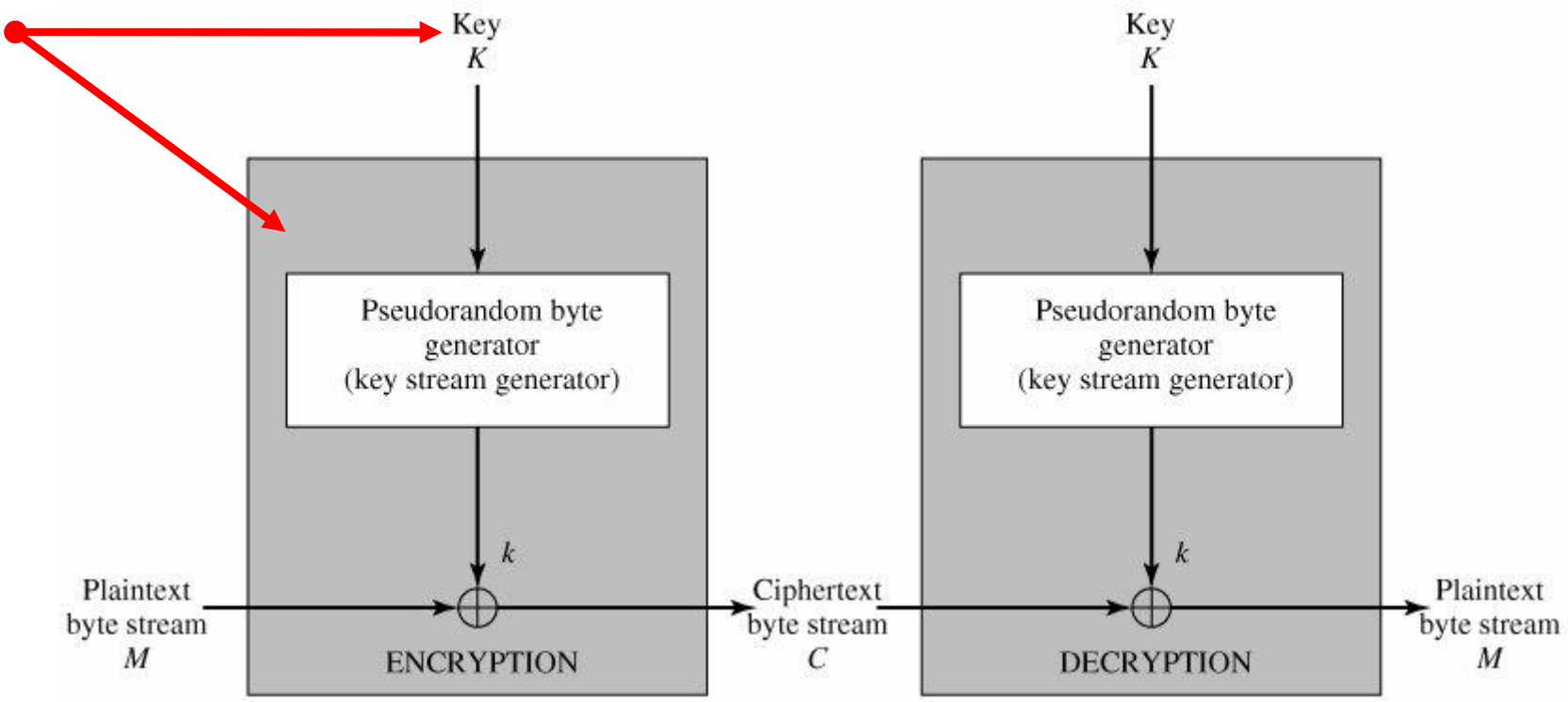


Características:

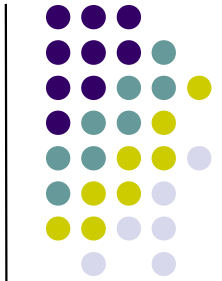
- Muito parecida com one-time-pad (números aleatórios genuínos).
- Cifras de fluxo usam números pseudo-aleatórios;
- Sequencia de criptografia deverá ter um período muito grande.
  - Fluxo determinístico de bits com repetição
  - Quanto maior o período melhor.
- Fluxo de chave deverá aproximar ao máximo do fluxo de números aleatórios.

Cifras de Fluxo

- Chave precisa ser suficientemente longa para evitar ataques de força bruta (128 bits).



Cifras de Fluxo



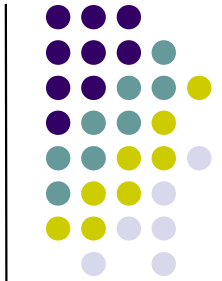
Vantagem:

- Quase sempre mais rápida em software do que a cifra de bloco
- Poucas linhas de código para implementar

Pode ser usado:

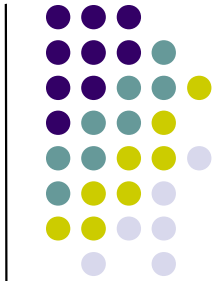
- Aplicações de criptografia sobre canais de comunicação.
- Necessário confrontar, desempenho e nível de confidencialidade desejado (valor da informação).

Algoritmo RC4



- "*Rivest Cipher 4*" é uma cifra de fluxo projetada em 1987 por Rivest para a RSA Security.
- Possui tamanho de chave variável
- Baseado em Permutação P-Aleatória
- Período de repetição muito grande na ordem de 10^{100}
- Era segredo até 1994.

Algoritmo RC4



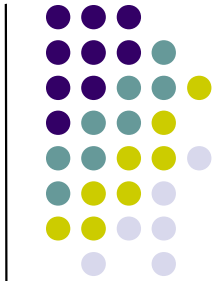
Onde é utilizado:

- Padrões SSL/TLS (SecurenSockets Layer/transport Layer Security) → HTTPS.
- WEP (Wired equivalence Privacy)
- WPA (Wifi Protected Access) -> WPA2 usa AES.

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	variable	0.9
RC4	variable	45

RC2: cifrador de bloco criado por Ron Rivest em 1987.

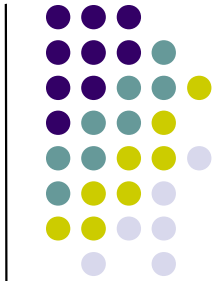
Algoritmo RC4



Como funciona:

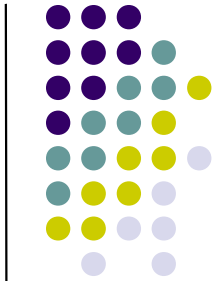
- Chave K variável de 1 a 256 bytes (8 a 2048 bits)
- S = vetor de estados de 256 posições (0 a 255) inicializado por permutação de posições definidas pela chave K.
- Para cifrar usamos um k gerado a partir de S , byte a byte.
- Para decifrar fazemos o mesmo processo.

Algoritmo RC4



- Inicialização de S:
- S é inicializado com os valores crescentes de sua posição 0 a 255. S[0]= 0 … S(2)=2 …
- Um vetor T auxiliar armazena os bytes da chave K, com repetição ou não, sendo K com tamanho=256 então T=K senão repete-se K para preencher cada posição de T.

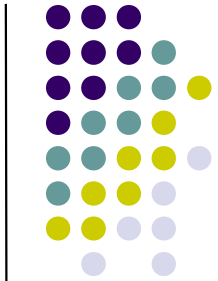
Algoritmo RC4



- Inicialização de S:
- Depois usa-se T para permutar S. de 0 a 255 para cada Si trocar Si por Sj onde j é ditado por T.

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j]);
```

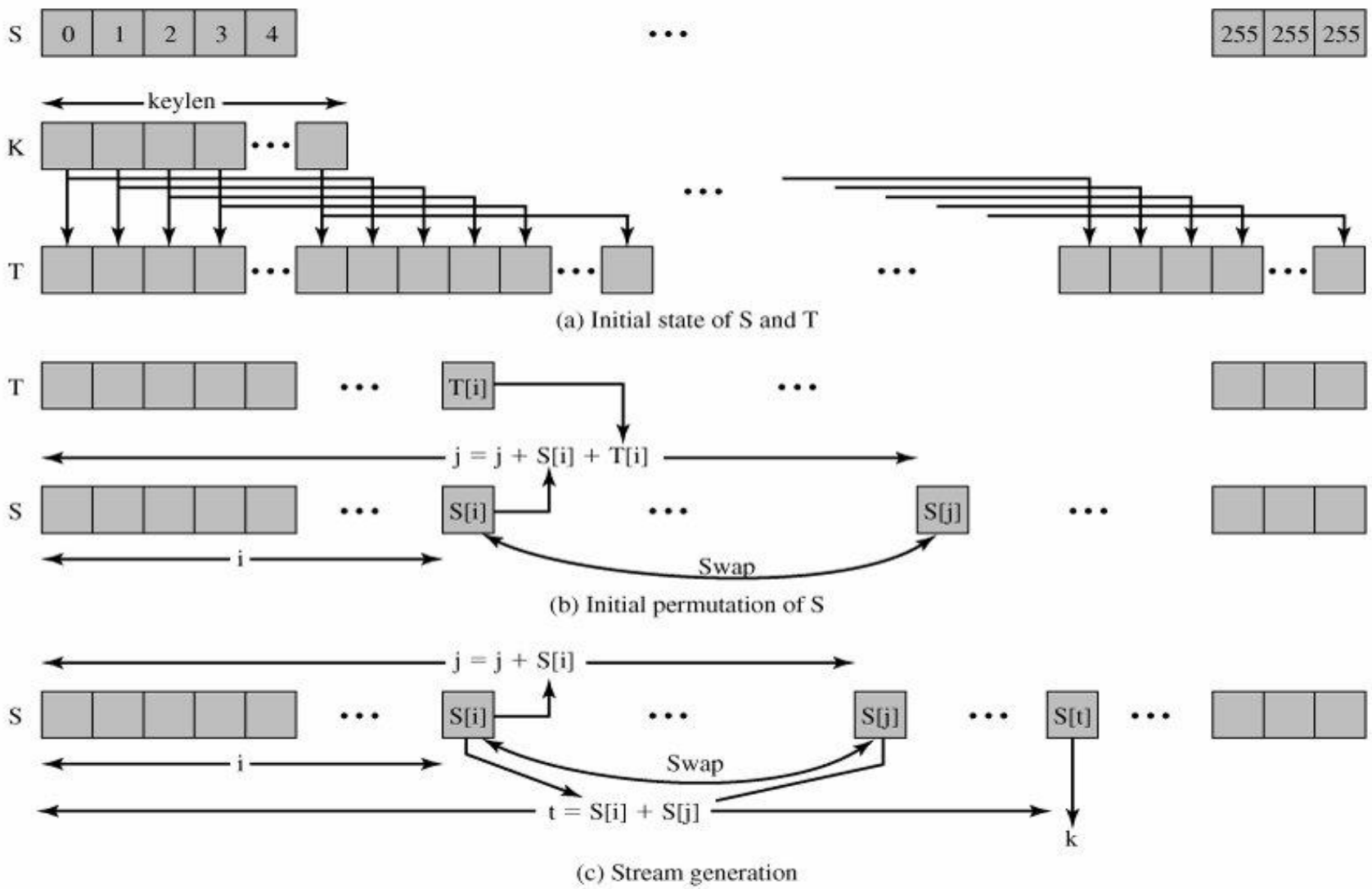
Algoritmo RC4: *Geração de Fluxo*



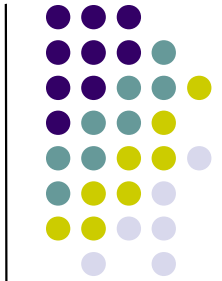
- Percorrer todos os elementos de S para cada Si trocar por outro elemento ditado por Si.
- Ao fim temos k que será XoRado com o próximo byte de texto plano.

```
/* Stream Generation */
i, j = 0;
while (true)
  i = (i + 1) mod 256;
  j = (j + S[i]) mod 256;
  Swap (S[i], S[j]);
  t = (S[i] + S[j]) mod 256;
  k = S[t];
```

Algoritmo RC4



Atividade Em Sala



Tarefa Prática

- Implementar o protótipo do Algoritmo RC4 para cifra qualquer texto usando uma chave de tamanho variável entre 1 a 256 bytes.