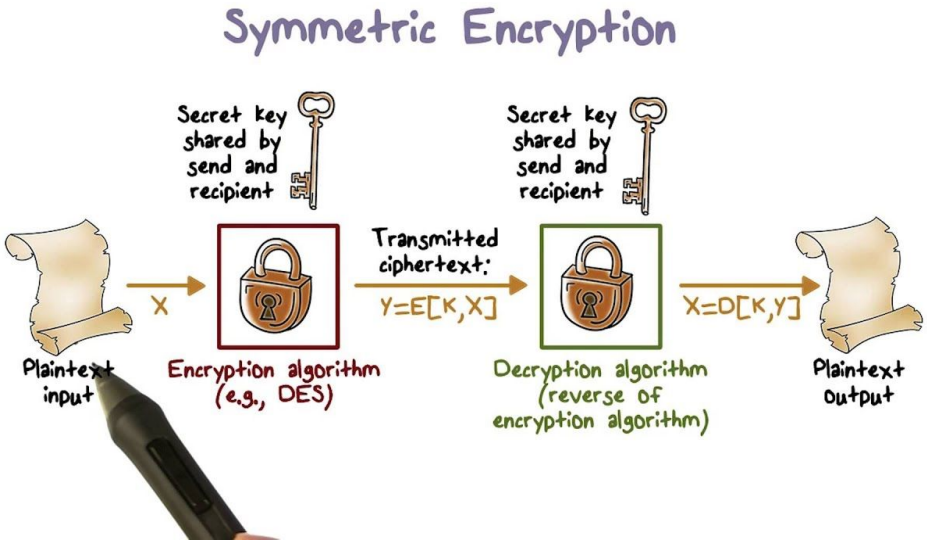
INE5429-07208
Segurança em Computação
Criptografia Básica

Prof. Jean Everson Martina

Cifragem – Técnicas Clássicas

- Modelo de Cifragem Simétrica
- Técnicas de Substituição
- Técnicas de Transposição
- Maquinas de Rotores
- Esteganografia

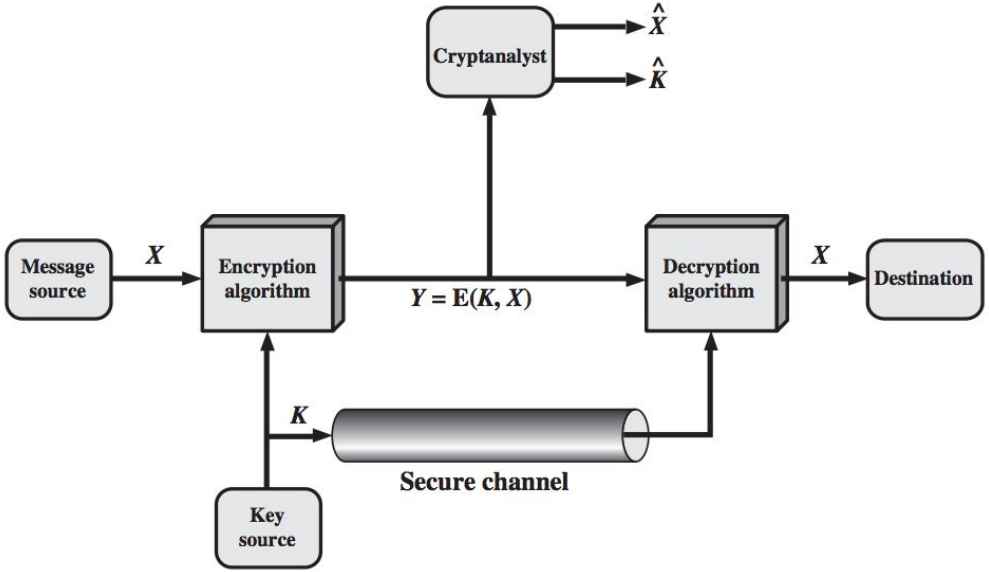
Modelo de Cifragem Simétrica



- Texto Claro
- Algoritmo de Cifração
- Chave Secreta
- Texto Cifrado
- Algoritmo de Decifração

Criptografia x Criptoanálise

- Criptografia
  - Operações no texto claro para texto cifrado
  - Numero de Chaves
  - A forma como o texto claro é processado
- Criptoanálise
  - Ataque na natureza do algoritmo
  - Características do texto (claro e cifrado)
  - Força Bruta



Incondicionalmente x Computacionalmente Seguro

Found this super secure lock keeping $5000 of laptops safe at work

- Incondicional
  - Texto cifrado não contém informação suficiente para determinar o texto claro
- Computacional
  - Custo de quebrar excede o valor do ativo
  - O tempo requerido é maior que a vida útil do ativo

Técnicas de Substituição

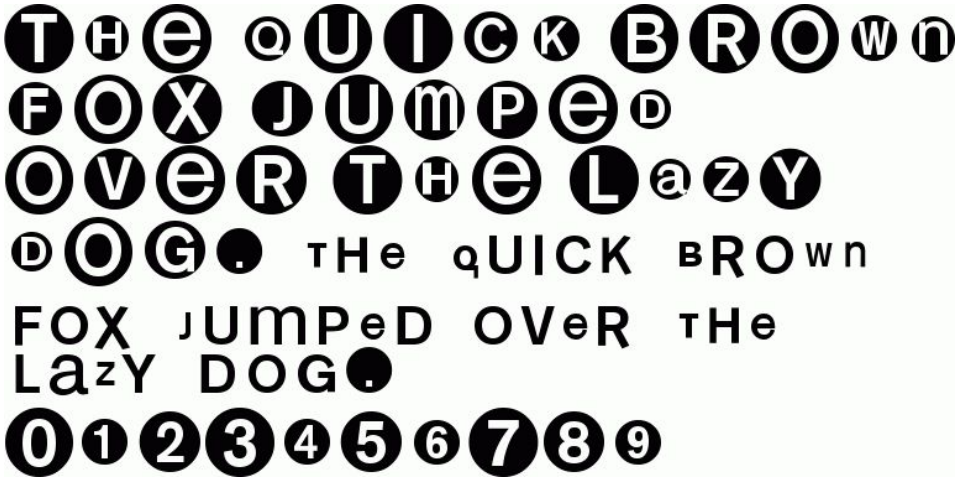
- Cifrador de Cesar
- Cifradores Mono-alfabéticos
- Playfair
- Cifradores Poli-alfabéticos
- Cifrador de Veginère
- Cifrador de Vernam
- One-time pad

Cifrador de Cesar

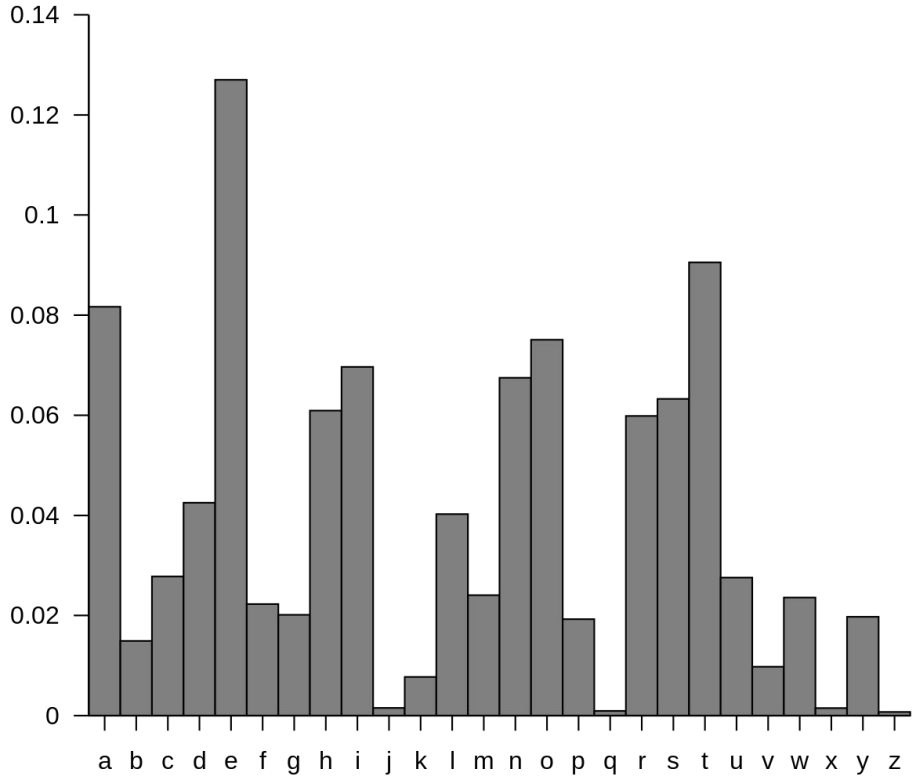
- Claro: Me encontre depois da aula
- Cifrado: PHHQF RQWUH GHSRL VGDDX OD
- C = E(p + 3) mod 26
- Criptoanálise:
  - Força Bruta
  - 25 chaves para tentar

Cifradores Mono-alfabéticos

- Mapeia de um alfabeto para outro alfabeto
- Troca de uma letra por outra letra qualquer
- Espaço de Chaves:
  - 26! = 4 x 10 ^ 26
  - Maior que DES
- Criptoanálise:
  - Análise de freqüência
  - Analise de duplas, triplas



Freqüência Relativa das Letras



Playfair

- Cifra pares de letras
- Pares na mesma linha → Direita
- Pares na mesma coluna → Abaixo
- Esconde digramas
- Análises de freqüência muito mais difícil

S	E	G	U	R
O	A	B	C	D
F	H	I/J	K	L
M	N	P	Q	T
V	W	X	Y	Z

Cifradores Poli-Alfabéticos

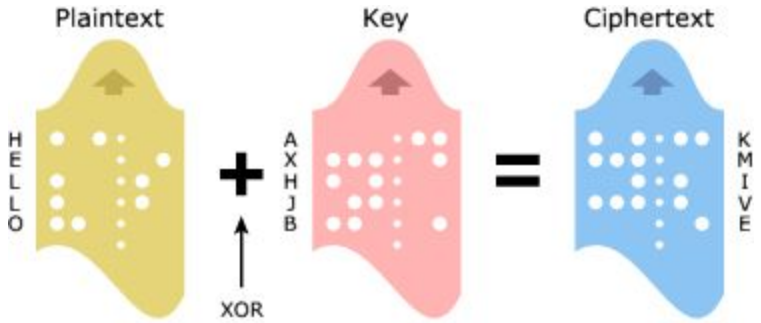
- Usam um conjunto de substituições mono-alfabéticas
- Uma chave determina como a transformação é dada
- Ofusca as informações de freqüência
- Nem toda a estrutura é perdida

Cifrador de Veginère

- Chave: segurosegurosegu
- Claro: aulanosabadoebom
- Cifrado: SYRUECJEHUUWFUG
- Ataque:
- Determinar o tamanho da chave
- Distância da repetição no texto cifrado

Cifrador de Vernam

- Transformação do texto em bits
- Transformação da chave em bits
- Ou-Exclusivo bit a bit
- Ci = Pi ⊕Ki
- Ataque:
  - Tamanho da chave exige repetição
  - Texto claro conhecido



One-Time Pad

- Chave de igual tamanho ao texto claro
- Incondicionalmente seguro
- Cifrador Veginère
- Cifrador de Vernam

Decrypt by hacker 1:

```
Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
Plaintext:  mr mustard with the candlestick in the hall
```

Decrypt by hacker 2:

```
Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
Key:        pftgpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
Plaintext:  miss scarlet with the knife in the library
```

Técnicas de Transposição

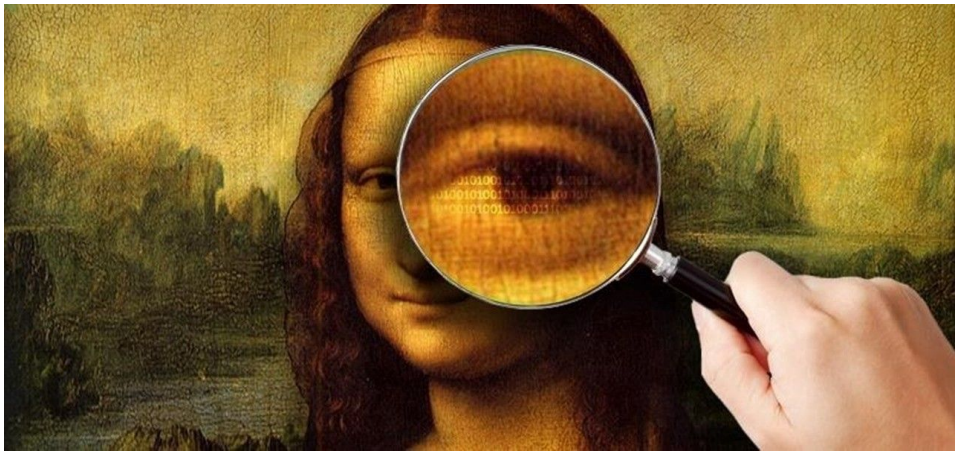
- Permutação no texto claro
- C i t g a i e a i
- R p o r f a f c l
- Matriz escrita em linha e recuperada em colunas
  - Chave pode ser a ordem das colunas
- Varias permutações confundem a Criptoanálise

Maquinas de Rotores

- Enigma
  - Criptoanálise: Trabalho de Turing
- Sistema eletro-mecânico
- Conjunto de cilindros independentes
- Cada cilindro um cifrador mono-alfabético
- Chave:
  - Ordem dos Rotores, posição inicial, posição do alfabeto, ligação do teclado, retroalimentação

Esteganografia

- Mensagem escondida em mídia portadora
- Objetivo: Repúdio do Envio
- Técnicas clássicas:
  - Marcação de caracteres
  - Tinta invisível
- Técnicas Modernas
  - Imagens
  - Audio
  - Cabeçalhos de Rede



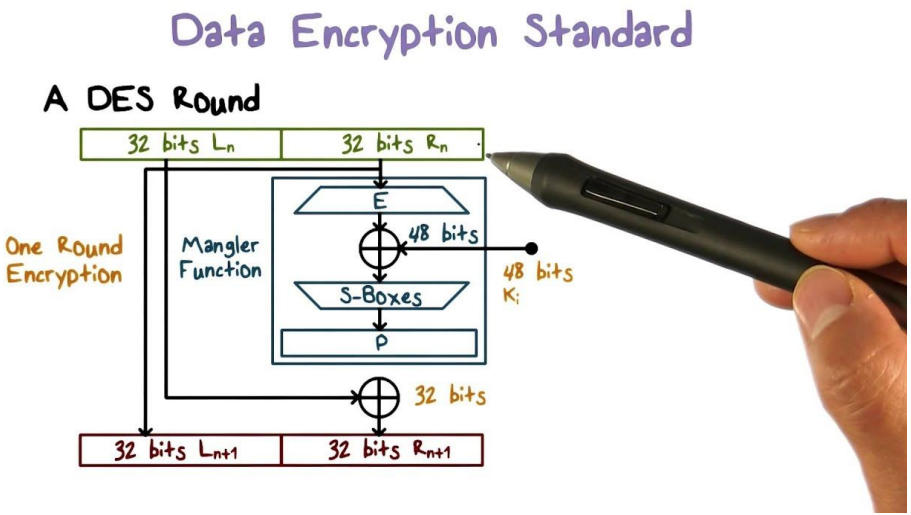
Cifradores Simétricos

- Mesma chave para cifra e decifrar
- 2 categorias:
  - Bloco
  - Stream
- Criptoanálise:
  - Diferencial
  - Linear

Confusão x Difusão

- Confusão:
  - Complexidade da relação texto cifrado x chave
  - Protege a chave
- Difusão:
  - Dissipação da estrutura estatística
  - 1 dígito de entrada afeta n dígitos de saída
  - Dissimula freqüência do texto claro

DES – Data Encryption Standard



- FIPS Pub 46
- IBM Lucifer [1971]
- Baseado em rede de Feistel
- Chave de 56 bits (64 com paridade)
- Permutações
- Caixas S
- Ótima implementação em Hardware

DES - Força Criptográfica

- 256 = 7.2 x 1016
- 1977 → US$ 20 Milhões = 10 horas
- 1998 → US$ 250mil = 70 horas
- Hoje → US$ 1mil = segundos
- Não foram descobertas até hoje falhas nas caixas S
- Suscetível a ataques de tempo

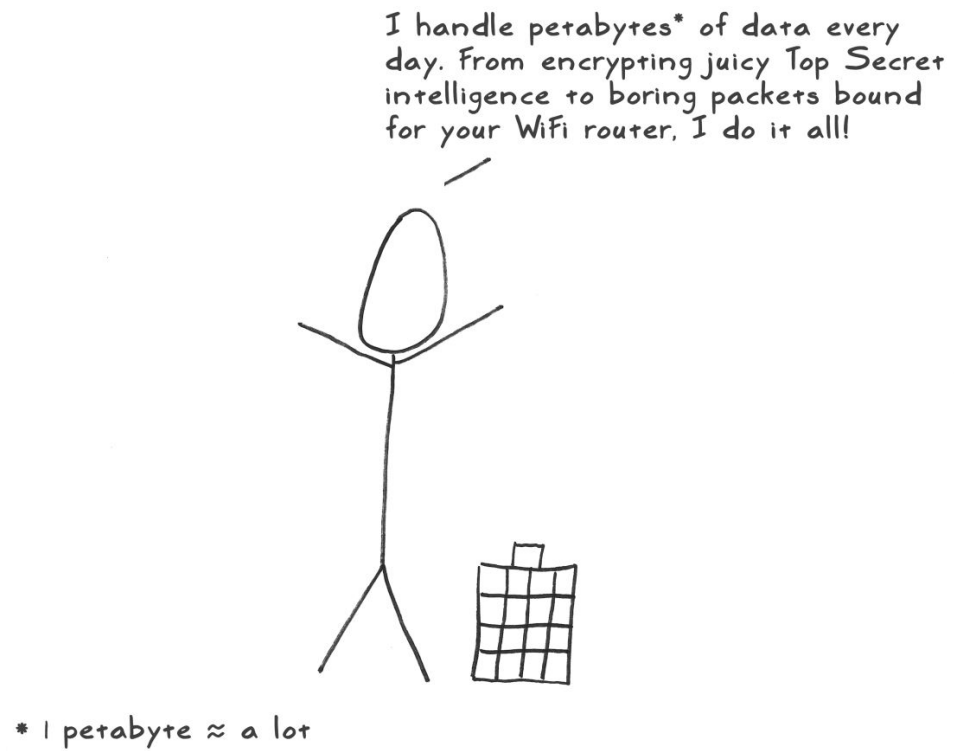
AES – Advanced Encryption Standard

- Cifrador de bloco para substituir o DES
- Competição em 2001, Chamada em 1997
- 21 algoritmos, 15 candidatos, 5 finalistas, Rijndael vencedor
- Suporte a 128, 192 e 256 bits
- Não usa Feistel
- Rounds:
  - Substituição de byte, permutação, operação sobre corpo finito, e XOR com a chave

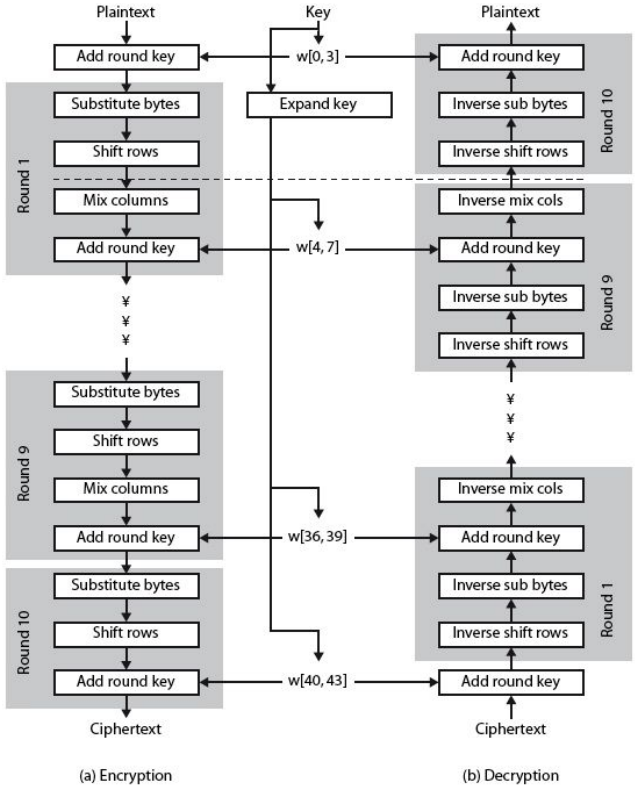
AES - Cifrador

- Tamanho de bloco sempre 128 bits
- Tamanho de Chave Variável (128,192,256)
- Rijndael
  - Resistência a ataques conhecidos
  - Velocidade e tamanho em variadas plataformas
  - Simplicidade

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Number of rounds	10	12	14
Expanded key size (words/byte)	44/176	52/208	60/240



AES – Cifragem e Decifragem



- Chave é expandida por matriz
- Quatro estágios por rodada:
  - Byte Sub: Caixa S GF (28)
  - ShiftRows: Permutação
  - MixColumns: Substituição GF (28)
  - AddRoundKey:XOR com chave de rodada
- XOR da chave + 9 rodadas cheias + 3 passos da ultima rodada

AES - Estrutura

- Chave só entra em AddRoundKey
- AddRoundKey é um cifrador de Vernam
- Cada estágio é facilmente reversível
  - Chave + confusão, difusão e não linearidade
- Reversibilidade por XOR
- Decifragem usa chave na ordem invertida
- Estágio final adiciona a chave para proteger as operações anteriores

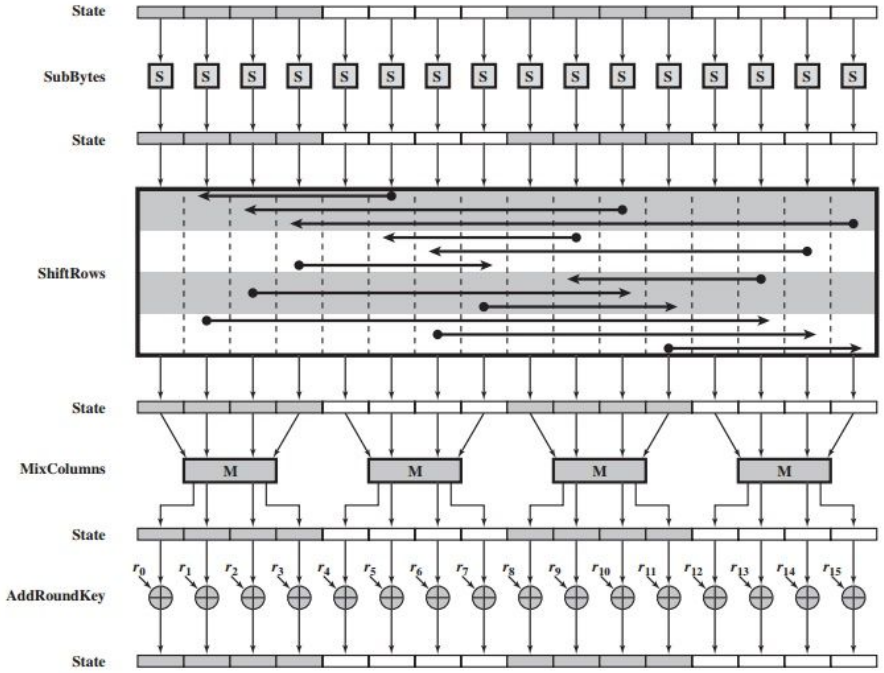
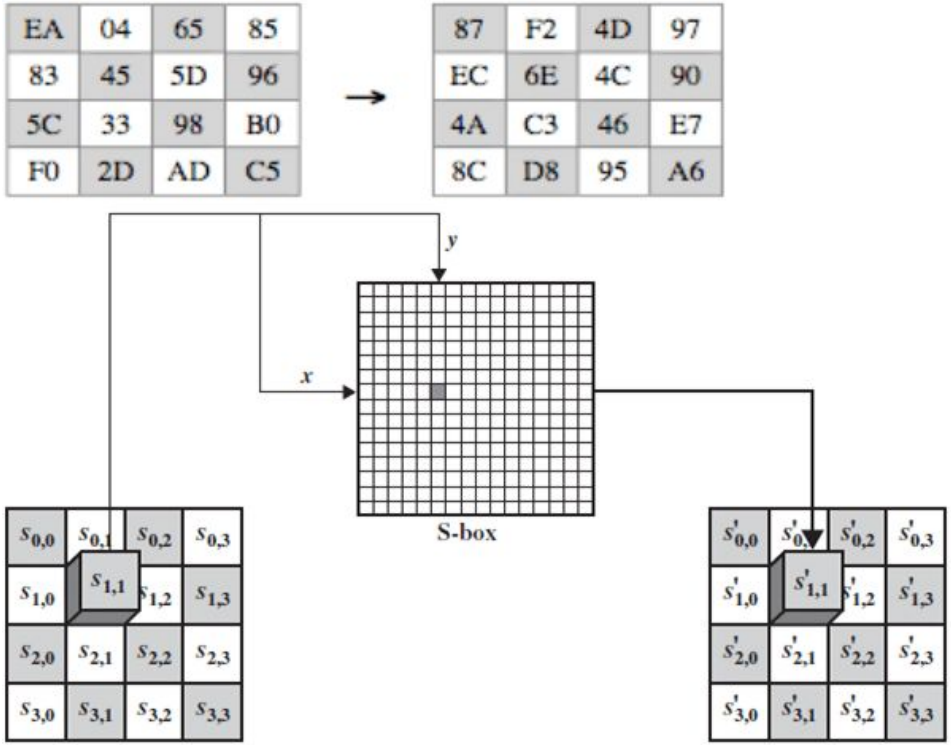


Figure 5.4 AES Encryption Round

AES - ByteSub

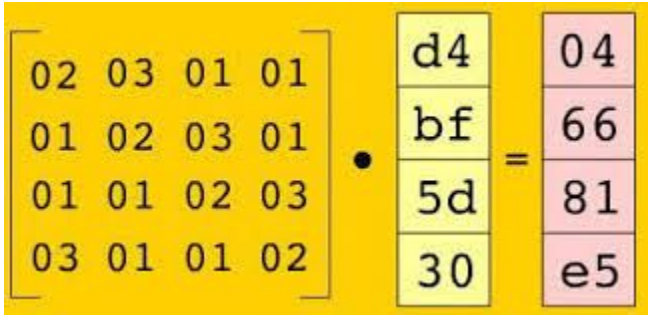


- Busca em Tabela
- Similar a uma Caixa S
- Resistente a todos os ataques cripto-analíticos conhecidos
- Criada com Base em aritmética num GF (28), com o polinômio irredutível x8 + x4 + x3 +x +1
- Funcionamento byte a byte

AES - ShiftRows

- Deslocamento horizontais de n-bytes por linha
    - 0 na primeira, 1 na segunda, 2 na terceira e 3 na quarta
- Direita gira para esquerda
- Inversa gira para a Direita
- Garante que 4 bytes de uma colunas são dispersos para outras colunas

AES – MixColumns

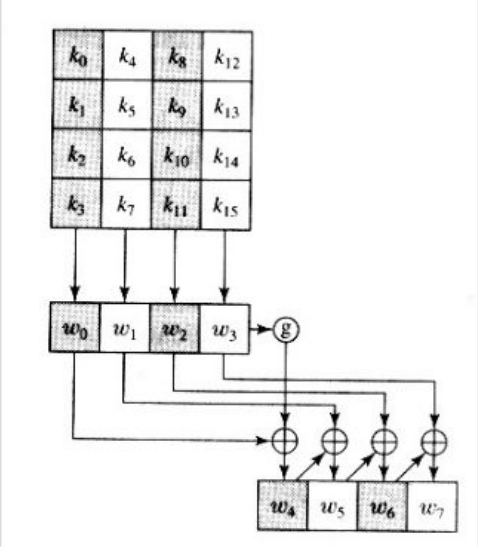


- Multiplicação de uma coluna do estado por uma matriz pré-determinada
- Matrix 4 x 4 é baseada numa inversão GF(28)
- Cada elemento na matriz produto é a soma dos elementos de uma linha e uma coluna, tudo em GF(28)
- Implementação prática baseada em XORs

AES - AddRoundKey

- XOR do estado com uma chave de 128 bits da rodada
- Cifrador de Vernam (que tem problemas)
- Simples, mas eficaz por causa dos outros passos e da expansão de chaves

AES – Expansão de Chaves



- Entram 16 bytes e saem 176 bytes
- Produz 4 bytes para cada sub chave
- A chave são os 4 primeiros bytes da chave expandida
- Cada byte posterior depende do byte anterior com XOR exceto o ultimo
- G é uma função complexa(rotação, substituição usando caixa S e XOR com uma constante de rodada

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

AES – Cifrador Inverso

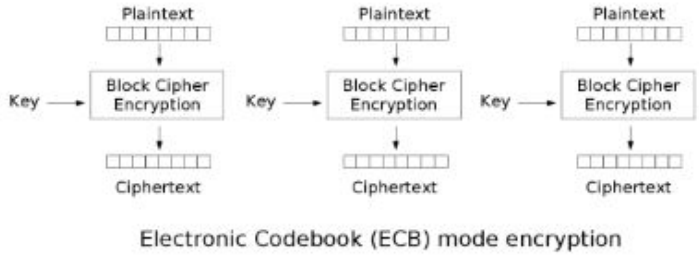
- Troca-se:
  - ShiftRows → InvShift Rows
  - SubBytes → InvSubBytes
  - MixColumns → InvMixColums
  - AddRoundKey usa as chaves em ordem invertida
- Em termos de implementação é o mesmo algoritmo, com matrizes de valores diferentes

Modos de Operação

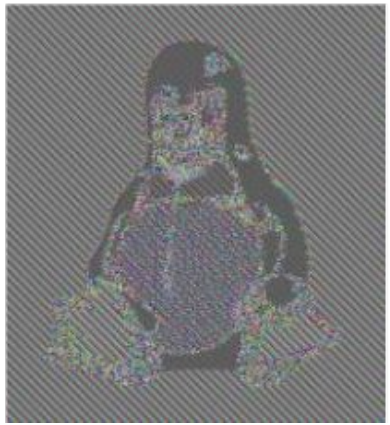
- Electronic Codebook -ECB
- Cipher Block Chaining - CBC
- Cipher Feedback - CFB
- Output Feedback - OFB
- Counter Mode - CTR

ECB

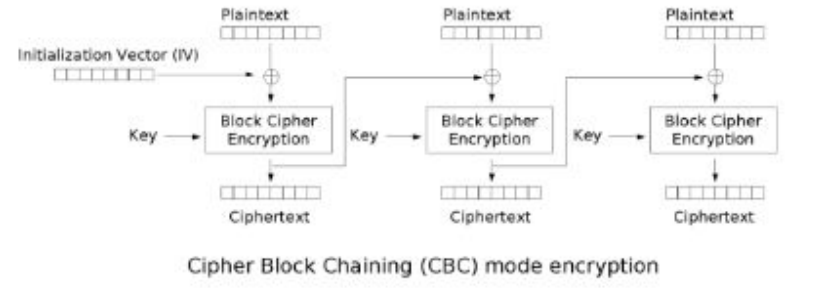
- Cada bloco é codificado de forma independente
- Segurança para transmissão de dados únicos



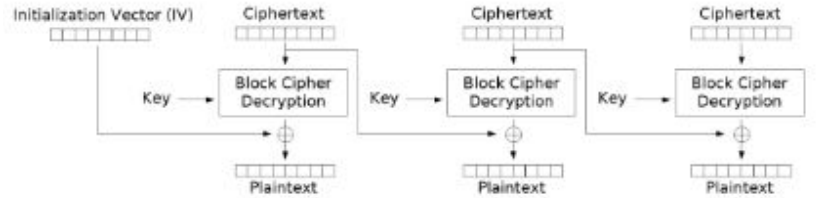
Electronic Codebook (ECB) mode encryption



CBC



Cipher Block Chaining (CBC) mode encryption

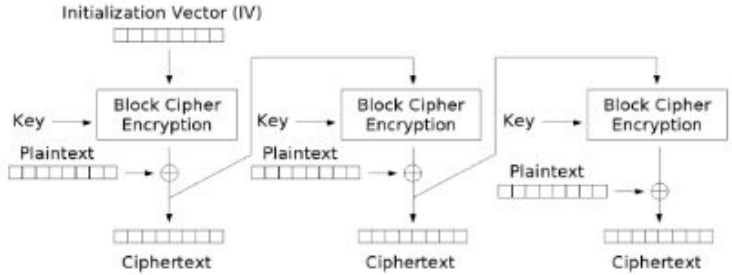


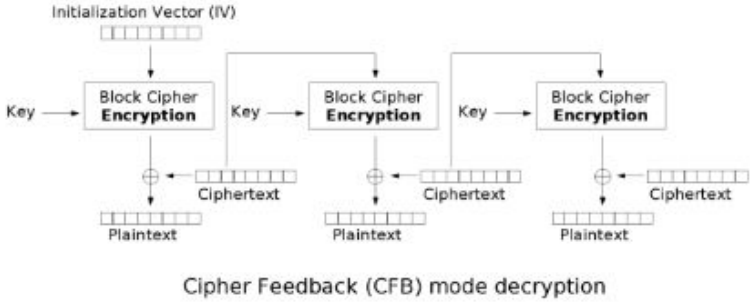
Cipher Block Chaining (CBC) mode decryption

- A entrada é XOR do próximo bloco de texto claro e o bloco anterior cifrado
- Uso para transmissão de dados e autenticação

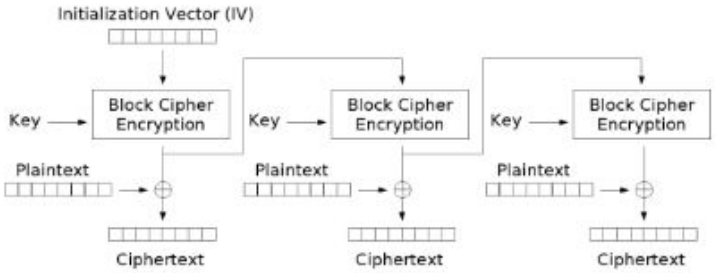
CFB

- O texto cifrado é XOR com o texto claro e retroalimentado no cifrador
- Uso para transmissão de dados e autenticação

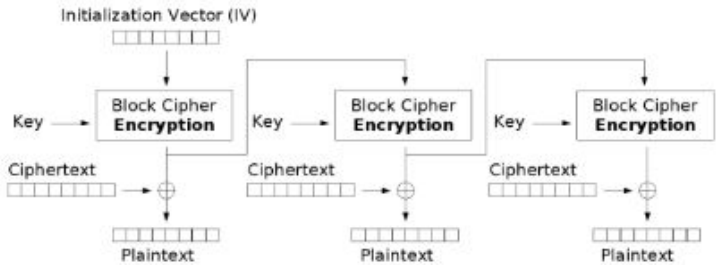




OFB



Output Feedback (OFB) mode encryption

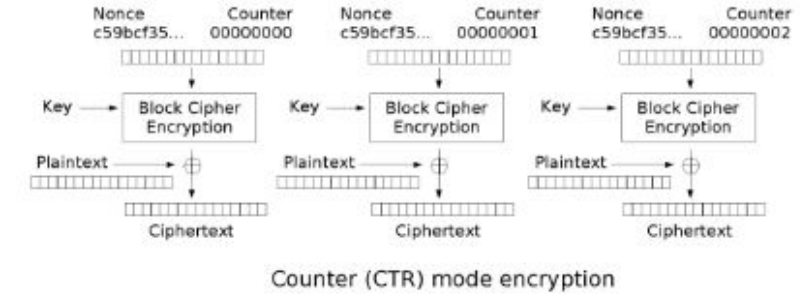


Output Feedback (OFB) mode decryption

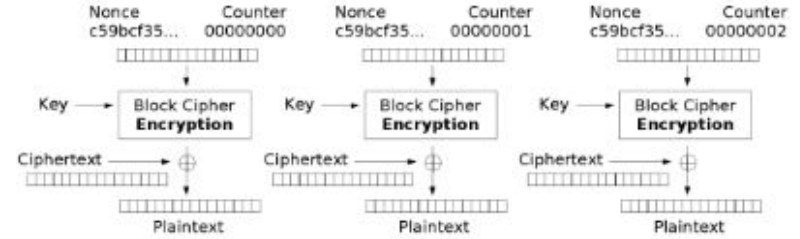
- Similar a CFB. A saída do cifrador é retroalimentada para gerar um stream de bits
- Usado em canais ruidosos

CTR

- Cada bloco é XORed com um contador cifrado
- Uso geral em transmissão de dados e em links de alta velocidade



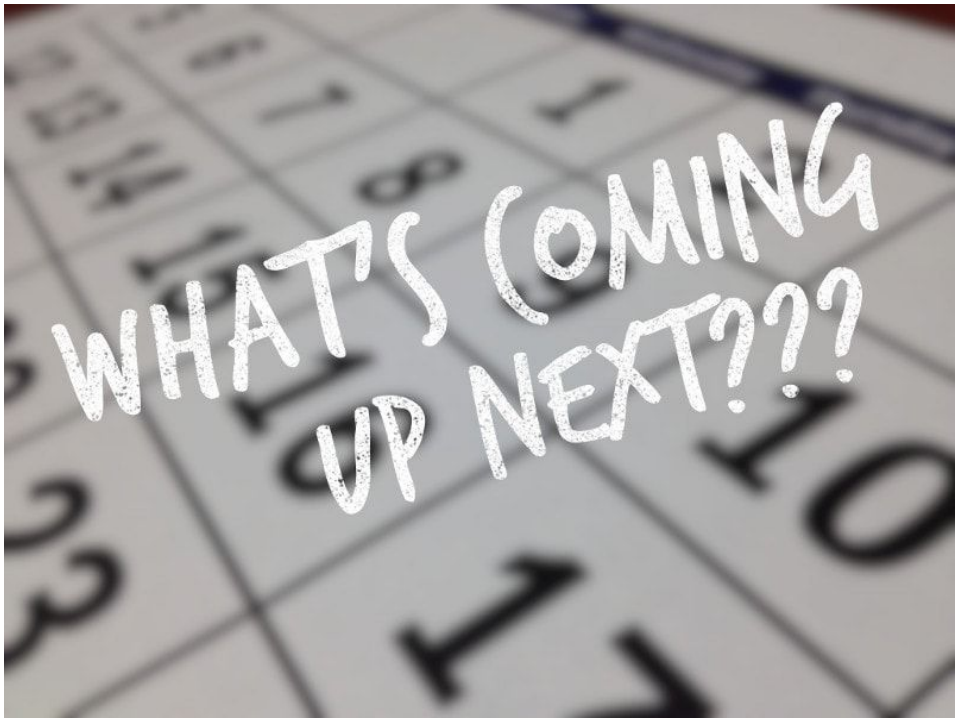
Counter (CTR) mode encryption



Counter (CTR) mode decryption

Próximas Aulas

- Prática:
  - Trabalho Individual I
    - Continuação
- Teórica:
  - Cripto Assimétrica e PRNGs



Perguntas?

jean.martina@ufsc.br