Advanced Encryption Standard

30/05/2016

Gabriel Sousa

Sumário

Introdução

- Variante do algoritmo *Rijndael*
- Algoritmo de criptografia de chave simétrica
- Ciframento em blocos fixos de 128, 192 e 256 bits
- Padrão de criptografia adotado pelo governo dos EUA
- Primeiro (e único) algoritmo de criptografia de domínio publico aprovado pela NSA

Introdução

- Variante do algoritmo *Rijndael*
- Algoritmo de criptografia de chave simétrica
- Ciframento em blocos fixos de 128, 192 e 256 bits
- Padrão de criptografia adotado pelo governo dos EUA
- Primeiro (e único) algoritmo de criptografia de domínio publico aprovado pela NSA

Introdução

- Variante do algoritmo *Rijndael*
- Algoritmo de criptografia de chave simétrica
- Ciframento em blocos fixos de 128, 192 e 256 bits
- Padrão de criptografia adotado pelo governo dos EUA
- Primeiro (e único) algoritmo de criptografia de domínio publico aprovado pela NSA

Introdução

- Variante do algoritmo *Rijndael*
- Algoritmo de criptografia de chave simétrica
- Ciframento em blocos fixos de 128, 192 e 256 bits
- Padrão de criptografia adotado pelo governo dos EUA
- Primeiro (e único) algoritmo de criptografia de domínio publico aprovado pela NSA

Introdução

- Variante do algoritmo *Rijndael*
- Algoritmo de criptografia de chave simétrica
- Ciframento em blocos fixos de 128, 192 e 256 bits
- Padrão de criptografia adotado pelo governo dos EUA
- Primeiro (e único) algoritmo de criptografia de domínio publico aprovado pela NSA

Criptografia de chave simétrica

- A mensagem é criptografada e descriptografada com a mesma chave
- Se a chave for descoberta o sigilo estará comprometido
  - Como se comunicar com um número indeterminado de indivíduos?
  - Quantidade de chaves necessárias é $O(n^2)$
  - Como seria feito o acordo sobre as chaves?

Criptografia de chave simétrica

- A mensagem é criptografada e descriptografada com a mesma chave
- Se a chave for descoberta o sigilo estará comprometido
  - Como se comunicar com um número indeterminado de indivíduos?
  - Quantidade de chaves necessárias é $O(n^2)$
  - Como seria feito o acordo sobre as chaves?

Criptografia de chave simétrica

- A mensagem é criptografada e descriptografada com a mesma chave
- Se a chave for descoberta o sigilo estará comprometido
  - Como se comunicar com um número indeterminado de indivíduos?
  - Quantidade de chaves necessárias é $O(n^2)$
  - Como seria feito o acordo sobre as chaves?

Criptografia de chave simétrica

- A mensagem é criptografada e descriptografada com a mesma chave
- Se a chave for descoberta o sigilo estará comprometido
  - Como se comunicar com um número indeterminado de indivíduos?
  - Quantidade de chaves necessárias é $O(n^2)$
  - Como seria feito o acordo sobre as chaves?

Criptografia de chave simétrica

- A mensagem é criptografada e descriptografada com a mesma chave
- Se a chave for descoberta o sigilo estará comprometido
  - Como se comunicar com um número indeterminado de indivíduos?
  - Quantidade de chaves necessárias é $O(n^2)$
  - Como seria feito o acordo sobre as chaves?

Criptografia de chave simétrica

- Por que utilizar esse tipo de criptografia
  - Muito mais veloz que criptografia com chaves assimétricas
- Geralmente utilizado em conjunto com chave assimétricas
  - Inicialização da comunicação feita por outro tipo de criptografia
  - Troca das chaves simétricas utilizando criptografia de chave assimétrica

Criptografia de chave simétrica

- Por que utilizar esse tipo de criptografia
  - Muito mais veloz que criptografia com chaves assimétricas
- Geralmente utilizado em conjunto com chave assimétricas
  - Inicialização da comunicação feita por outro tipo de criptografia
  - Troca das chaves simétricas utilizando criptografia de chave assimétrica

Criptografia de chave simétrica

- Por que utilizar esse tipo de criptografia
  - Muito mais veloz que criptografia com chaves assimétricas
- Geralmente utilizado em conjunto com chave assimétricas
  - Inicialização da comunicação feita por outro tipo de criptografia
  - Troca das chaves simétricas utilizando criptografia de chave assimétrica

Criptografia de chave simétrica

- Por que utilizar esse tipo de criptografia
  - Muito mais veloz que criptografia com chaves assimétricas
- Geralmente utilizado em conjunto com chave assimétricas
  - Inicialização da comunicação feita por outro tipo de criptografia
  - Troca das chaves simétricas utilizando criptografia de chave assimétrica

Criptografia de chave simétrica

- Por que utilizar esse tipo de criptografia
  - Muito mais veloz que criptografia com chaves assimétricas
- Geralmente utilizado em conjunto com chave assimétricas
  - Inicialização da comunicação feita por outro tipo de criptografia
  - Troca das chaves simétricas utilizando criptografia de chave assimétrica

Cifra de blocos

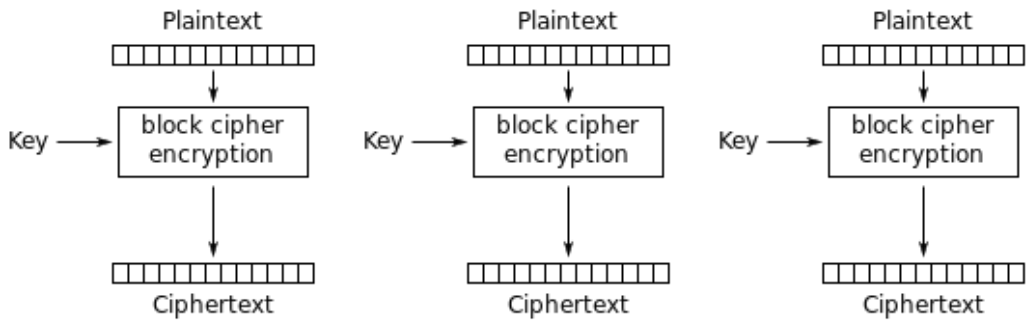
A mensagem é dividida em blocos de mesmo tamanho.

O Algoritmo

Animação explicando o processo de criptografia AES:
Rijndael Animation

Modos de operação

- O algoritmo só opera em blocos de 128 bits
- O que fazer quando a mensagem tem mais de 128 bits?
  - Dividir a mensagem em blocos deste tamanho e aplicar o algoritmo em cada bloco separadamente (*Electronic Codebook* - ECB)

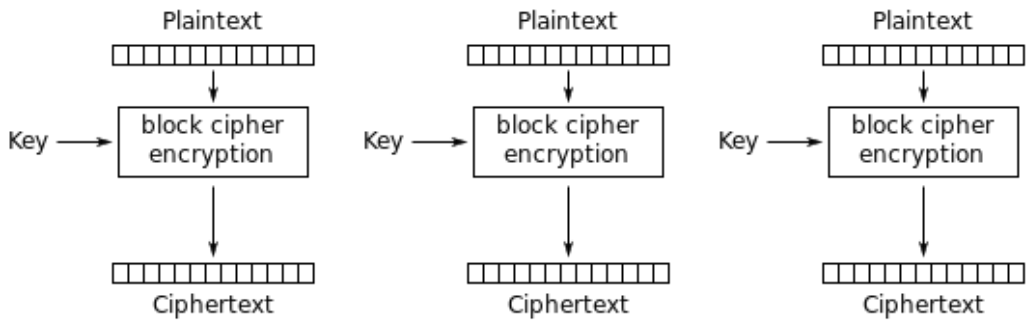


Electronic Codebook (ECB) mode encryption

- Tão simples assim?

Modos de operação

- O algoritmo só opera em blocos de 128 bits
- O que fazer quando a mensagem tem mais de 128 bits?
  - Dividir a mensagem em blocos deste tamanho e aplicar o algoritmo em cada bloco separadamente (*Electronic Codebook* - ECB)

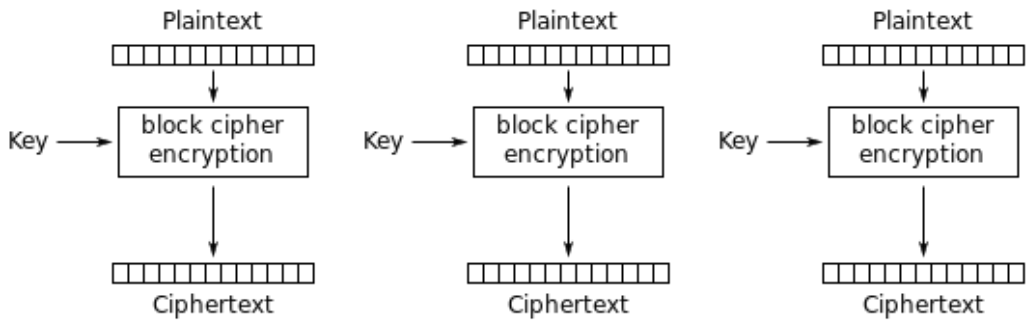


Electronic Codebook (ECB) mode encryption

- Tão simples assim?

Modos de operação

- O algoritmo só opera em blocos de 128 bits
- O que fazer quando a mensagem tem mais de 128 bits?
  - Dividir a mensagem em blocos deste tamanho e aplicar o algoritmo em cada bloco separadamente (*Electronic Codebook* - ECB)

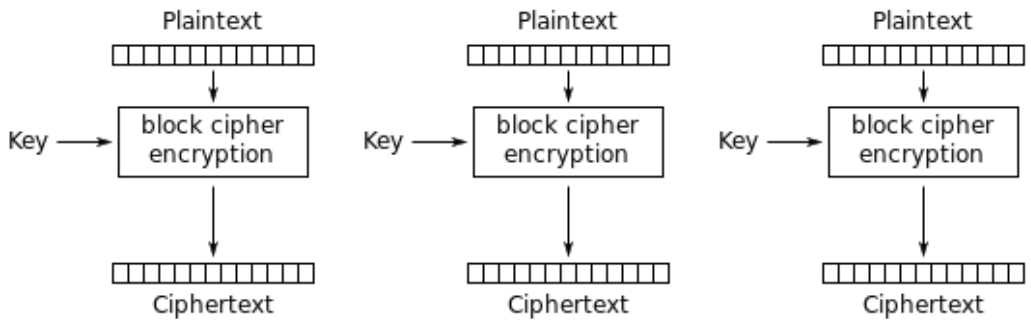


Electronic Codebook (ECB) mode encryption

- Tão simples assim?

Modos de operação

- O algoritmo só opera em blocos de 128 bits
- O que fazer quando a mensagem tem mais de 128 bits?
  - Dividir a mensagem em blocos deste tamanho e aplicar o algoritmo em cada bloco separadamente (*Electronic Codebook* - ECB)



Electronic Codebook (ECB) mode encryption

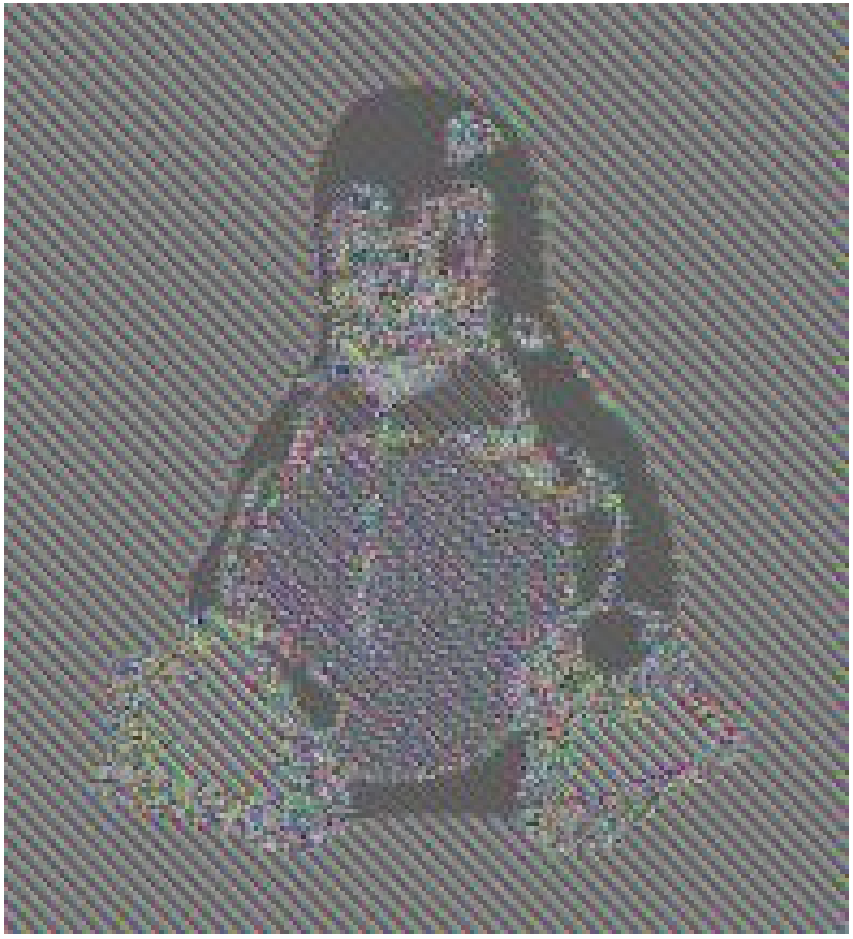
- Tão simples assim?

Modos de operação - ECB

Observe a imagem do Tux a ser criptografada no modo ECB

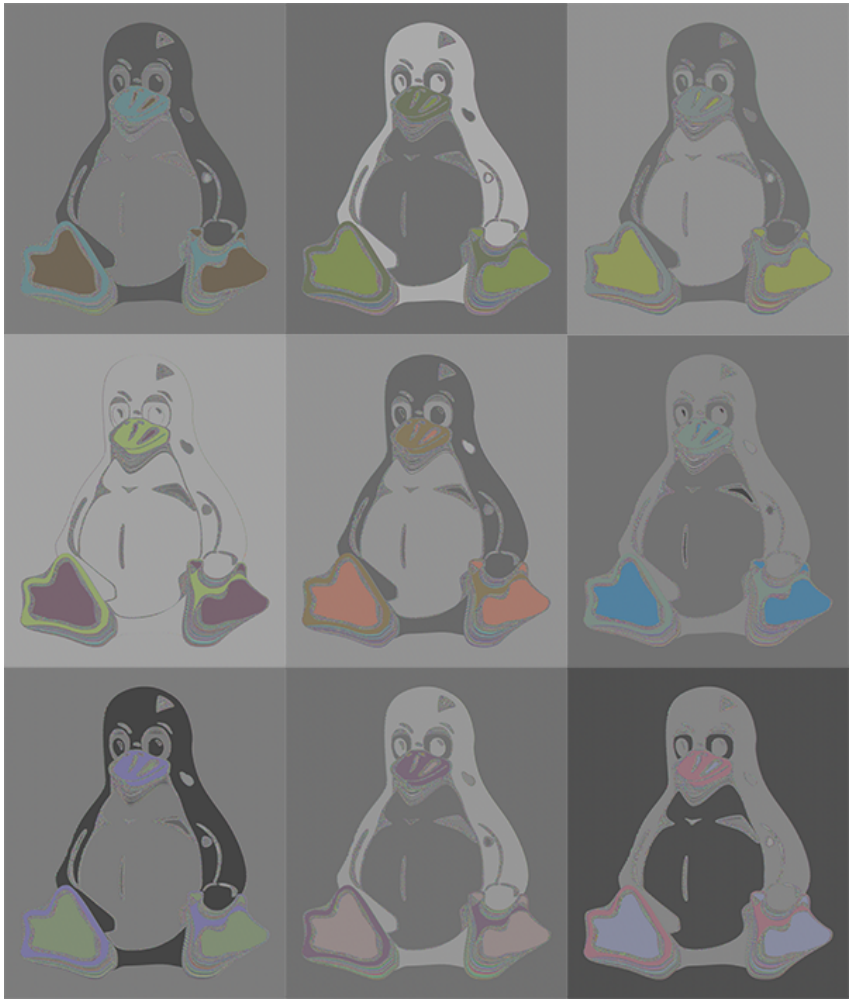
Modos de operação - ECB

Esse modo de operação fez o algoritmo se comportar basicamente como um “filtro”



Modos de operação - ECB

Mudando a chave de criptografia temos outros "filtros"

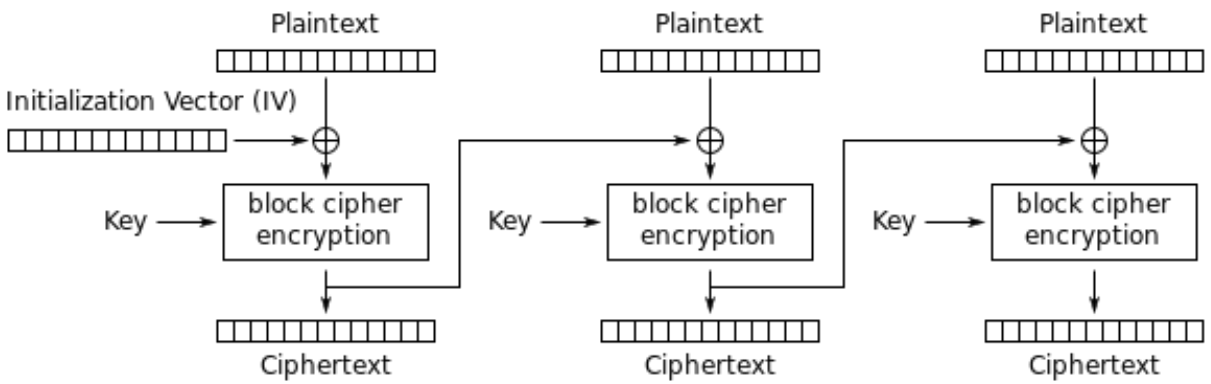


Modos de operação - ECB

Utilidade para esse modo?

Modos de operação - CBC

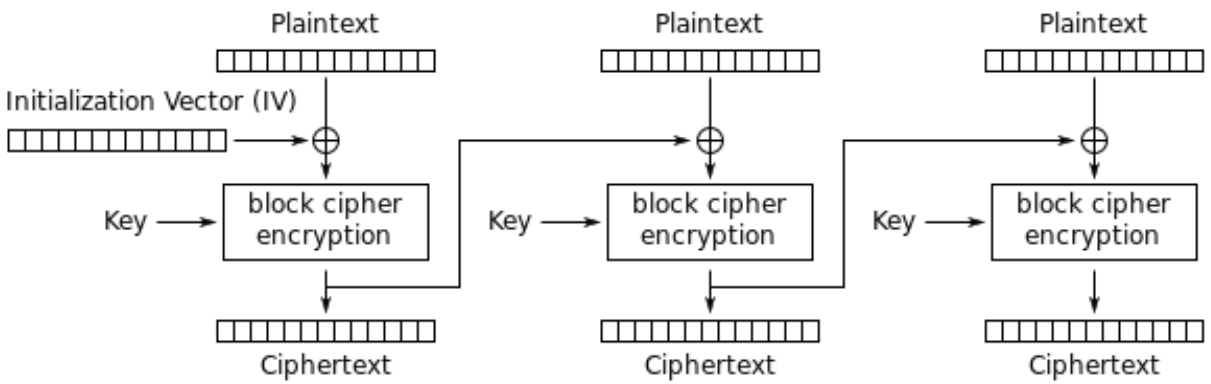
- Filme *O jogo da imitação* - Não era preciso processar toda a mensagem para obter a chave alemã, provavelmente eles estavam usando o modo ECB
- Um modo de dificultar a obtenção da chave é obrigar o atacante a processar todos os blocos da mensagem
- Tornar a encriptação de um bloco dependente do bloco anterior (*Cipher Block Chaining* - CBC)



Cipher Block Chaining (CBC) mode encryption

Modos de operação - CBC

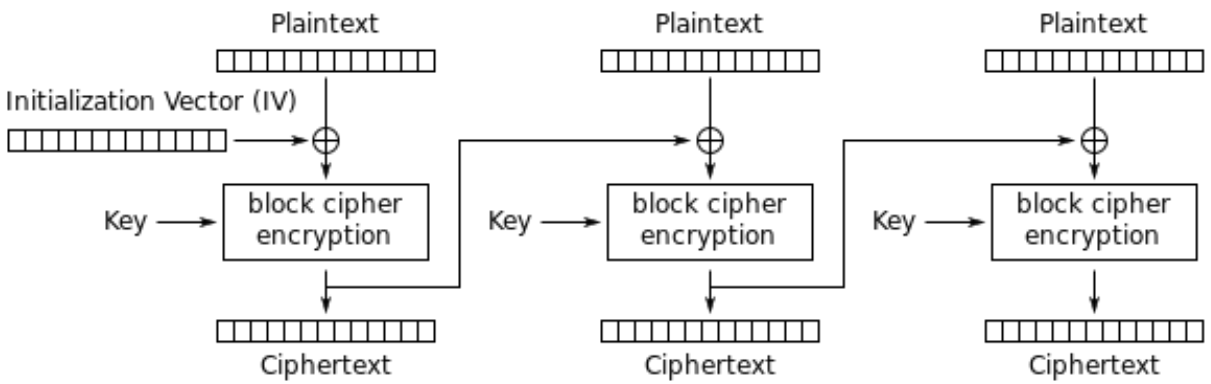
- Filme *O jogo da imitação* - Não era preciso processar toda a mensagem para obter a chave alemã, provavelmente eles estavam usando o modo ECB
- Um modo de dificultar a obtenção da chave é obrigar o atacante a processar todos os blocos da mensagem
- Tornar a encriptação de um bloco dependente do bloco anterior (*Cipher Block Chaining* - CBC)



Cipher Block Chaining (CBC) mode encryption

Modos de operação - CBC

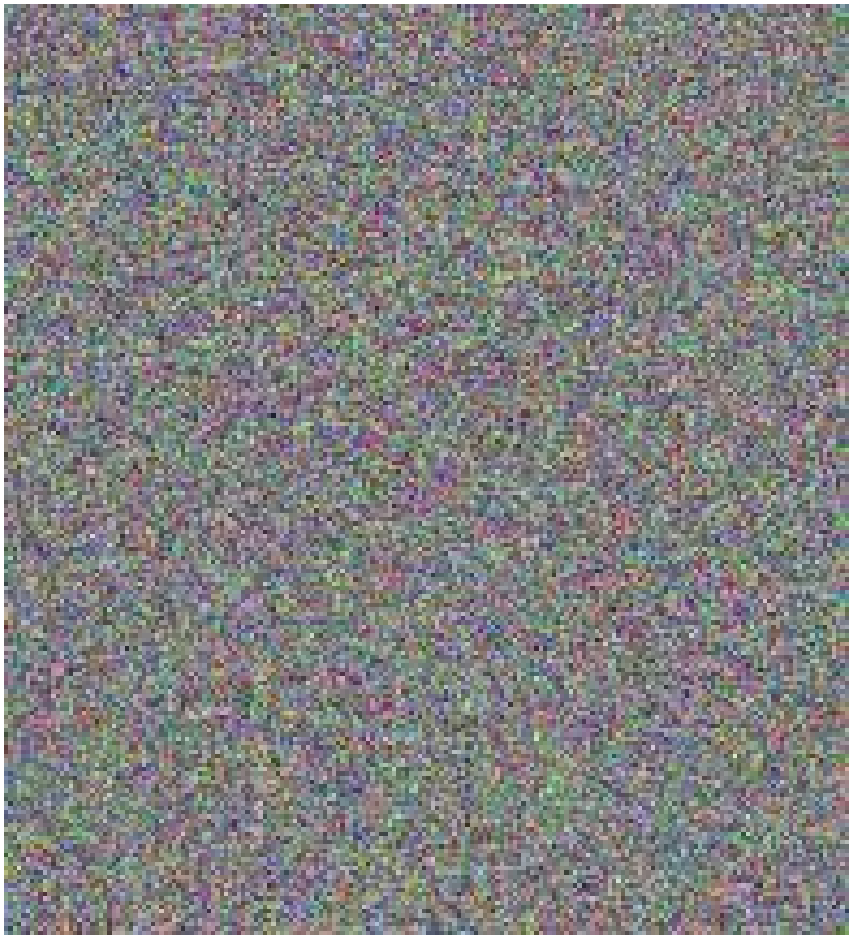
- Filme *O jogo da imitação* - Não era preciso processar toda a mensagem para obter a chave alemã, provavelmente eles estavam usando o modo ECB
- Um modo de dificultar a obtenção da chave é obrigar o atacante a processar todos os blocos da mensagem
- Tornar a encriptação de um bloco dependente do bloco anterior (*Cipher Block Chaining* - CBC)



Cipher Block Chaining (CBC) mode encryption

Modos de operação - CBC

O Tux mais seguro com este modo



Referências

- Wikipedia - Advanced Encryption Standard
- Avi Kak - Lecture 8: AES: The Advanced Encryption Standard
- Wikipedia - Block cipher mode of operation