AES (Advanced Encryption Standard)

O processo de cifração em AES (Advanced Encryption Standard) envolve várias etapas fundamentais para garantir a segurança dos dados. Abaixo, vou detalhar cada uma dessas etapas:

1. Substituição de Bytes (SubBytes):

Nesta etapa, cada byte do bloco de dados é substituído por outro byte de acordo com uma tabela de substituição (chamada S-Box). Cada valor de byte é substituído por um valor correspondente na S-Box. A S-Box é projetada para introduzir não-linearidade no processo, aumentando a segurança da cifragem.

2. Permutação de Linhas (ShiftRows):

Os bytes no estado são reorganizados de acordo com um padrão específico. Cada linha da matriz de estado (bloco de dados) é deslocada ciclicamente para a esquerda. A primeira linha não é alterada, a segunda é deslocada uma posição para a esquerda, a terceira duas posições e a quarta três posições. Isso cria confusão nos dados, garantindo que cada byte afete múltiplos bytes no estado cifrado.

3. Difusão (MixColumns):

Nesta etapa, as colunas da matriz de estado são transformadas. Cada coluna é tratada como um polinômio, e a multiplicação é realizada em um corpo finito. Isso implica que cada byte na coluna é combinado com os outros bytes de uma maneira não linear. Essa etapa aumenta a difusão dos dados, garantindo que pequenas alterações nos dados de entrada resultem em grandes alterações no estado cifrado.

4. Adição da Chave de Rodada (AddRoundKey):

A chave de criptografia é expandida em várias subchaves de rodada usando um algoritmo chamado Key Expansion. Cada subchave

é, então, combinada com o estado atual usando uma operação de OU exclusivo (XOR). Cada rodada tem sua própria subchave, garantindo que cada parte dos dados seja influenciada por uma parte diferente da chave. Isso introduz a confusão e a difusão na cifragem.

5. Round Constant (Rcon)

A função Rcon na cifra AES é uma tabela de constantes usada durante a expansão da chave. Ela fornece valores constantes que são combinados com palavras-chave para criar subchaves exclusivas usadas em cada rodada do algoritmo. Essa diversificação de subchaves aumenta a segurança do AES, impedindo padrões previsíveis e possíveis ataques.

Estas quatro etapas (SubBytes, ShiftRows, MixColumns e AddRoundKey) são repetidas várias vezes (10, 12 ou 14 vezes para AES-128, AES-192 e AES-256, respectivamente) em uma estrutura chamada "rodadas". Após a última rodada, as etapas SubBytes, ShiftRows e MixColumns são aplicadas novamente, mas a etapa AddRoundKey não é aplicada na última rodada.

No final do processo de cifragem, o estado é convertido em uma sequência de bytes, que é o texto cifrado. O processo de decifragem é basicamente o inverso do processo de cifragem, onde as etapas são aplicadas em ordem reversa para obter o texto original a partir do texto cifrado. Essas etapas são cuidadosamente projetadas para garantir que o AES seja seguro e resistente a uma variedade de ataques criptográficos conhecidos.

Teste

O programa executa um teste onde são usados esses dados:

Key (128): E8E9EAEBEDEEEFF0F2F3F4F5F7F8F9FA

Plaintext: 014BAF2278A69D331D5180103643E99A

Ciphertext: 6743C3D1519AB4F2CD9A78AB09A511BD

O programa cifra/decifra o Plaintext com a Key, ao final confere se o Ciphertext gerado é igual ao Ciphertext esperado e se Plaintext recuperado e igual ao Plaintext original. Note que essa operação só será verdadeira usando 10 rodadas com entrada, pois o Ciphertext esperado é referente ao final do processo de cifração, quando se executa as 10 rodas padrões para o AES com chave de 128 bits.