Rodrigo Leão da Silveira

Segurança de Sistemas T2 AES e modos de operação

O segundo trabalho da disciplina de Segurança de Sistemas consiste na implementação de um programa capaz de cifrar e decifrar dados utilizando a cifra de bloco AES, podendo ser escolhido dentre duas opções, CBC e CTR. O programa gerado deverá ser capaz de cifrar e decifrar corretamente os 6 exemplos propostos no enunciado do trabalho.

AES

Advanced Encryption Standard (AES), é um método de criptografia de blocos com chave simétrica, estabelecida pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) em 2001 para substituir seu antecessor, o DES. É um algoritmo de chave simétrica, ou seja, utiliza a mesma chave para cifrar ou decifra uma mensagem, a chave pode variar entre os tamanhos de 128 bits, 192 bits ou 256 bits, e o tamanho do bloco é sempre de 128 bits.

Modos de Operação

Algoritmos de criptografia geralmente trabalham em cima de bloco de tamanho fixo, geralmente 128 bits, porém, as mensagens a serem cifradas não necessariamente terão este mesmo tamanho, ou pior, não terão um tamanhão múltiplo do tamanho de bloco esperado pelo algoritmo, Para resolver esta situação é utilizado a cifragem em blocos, que consistem em encadear blocos de 128 bits da mensagem até que toda ela seja cifrada e só possa ser decifrada se, e somente se todos os blocos forem decifrados. A cifragem em blocos possui diferentes modos de operação. A maioria dos modos de operação necessitam de um bloco falso de iniciação (IV) que não precisa ser secreto, mas que nunca deve ser utilizado com a mesma chave para não fornecer pistas e possibilitar que um atacante possa encontrar a chave através da análise dos dados cifrados. A seguir será explicado os modos de operação solicitados no trabalho (CBC e CTR).

CBC

Cipher Block Chaining (CBC) é um modo de criptografia utiliza o bloco cifrado anterior para gerar o novo bloco cifrado, através de um xor, por este motivo é necessário a utilização de um vetor de inicialização para iniciar a criptografia. Tem como característica a necessidade de se decifrar todos os blocos para se obter a mensagem original.

Como o modo de operação CBC necessita que os blocos a serem cifrados sejam múltiplos do tamanho de bloco do algoritmo, é necessário utilizar alguma técnica de *padding* para completar o tamanho do bloco, para o trabalho será utilizado o padrão PKCS5, que consiste na inserção de N bytes de valor N ao final do bloco, onde N é o número de bytes necessário para completar o bloco.

01
02 02
03 03 03
etc.

CTR

Counter Mode (CTR) é um modo de criptografia que utiliza um contador somado ao IV, onde eles são cifrados e após submetido a um xor com o texto simples. Tem como características a possibilidade do acesso aleatório ao um bloco e a paralelização no processo de cifragem e decifragem dos blocos, visto que os blocos não necessitam do bloco anterior para serem decifrados, apenas do contador utilização para cifrar ele. O contador pode ser uma função qualquer que demora muito tempo para repetir seus

valores, geralmente um contador resolve este problema, além de possibilitar a decifragem de um bloco qualquer sabendo apenas a posição dele na cadeia de blocos da mensagem cifrada.

Desenvolvimento

A implementação do presente trabalho foi realizada na linguagem de programação Java, utilizando o *Visual Studio Code* como IDE em uma máquina *Windows*. É utilizada a classe *Cipher* do *package javax.crypto*. Os casos de testes foram escritos em um arquivo no formato *Json* que posteriormente é mapeado para uma classe Tarefa que contém as propriedades necessárias para executar o processo de cifra/decifrar no modo de operação correto. Após o usuário escolher ou informar via parâmetro qual tarefa ele quer executar, é instanciada uma classe AES com os parâmetros modo e a chave. É feito um parse da chave em string para um *array* de *bytes* através da classe *DatatypeConverter* do *package javax.xml.bind*. Através da informação contida nos campos *ciphertext* e *plaintext* da classe tarefa é executado o método de cifrar ou decifra. Em ambos os métodos, é extraído o IV nos primeiros 16 bytes da mensagem. No método de decifra o IV é removido da mensagem a ser decifrada.

Resultados

Após a execução dos testes informados no trabalho obteve-se os seguintes resultados:

1. Basic CBC mode encryption needs padding.
2. Our implementation uses rand. IV
3. CTR mode lets you build a stream cipher from a block cipher.
4. Always avoid the two time pad!
5. 7A5A59C3C41CE0E086345B9220C1F029DFB9C2D8927D650232F6E4250DFC0CF1BB290946C6F3D33B5B62ACF93409BC45AB70AA1B962C00A8B0BB
6. 60D73DBEF0DAD0461D175BDA54EF8C9C5A41351E46AEA0BD348E61B8328DB8C351D342237E185ABEB0FD5A3CE13AE562BDD2F7A82F101388DCFD28730EFBF240219733B7D485E6ACB579AB0F520F008A295D6744A0DB0364925CE86B371186DDD339E08167DDE06592BC8125CF7B245B5A0671AFC15960F0E7ED1104D8131E34

Pelo resultado dos testes de 1 a 4 serem frases legíveis e condizentes com o contexto da disciplina, e que quando parâmetros errados eram escolhidos para a decifragem da mensagem o resultado obtido eram sequencias de caracteres sem lógica nenhuma, a implementação da decifragem está correta. E, como a implementação da cifragem é estritamente parecida com a da decifragem, acredita-se que ela também esteja correta.