Segurança Computacional

Trabalho 2

Gabriel Nogueira - 18/0113330

1 Cifração e Decifração AES (chave 128 bits)

1.1 Geração da Chave de 128 bits

Para a geração de uma chave aleatória de 128 bits foram selecionados 16 bytes psedo-aleatórios por meio da função `getrandbits` do módulo `random` da linguagem python. Em seguida, esse valor foi convertido para o formato de string, para facilitar sua leitura do arquivo.

1.2 Cifração e decifração

Para cifrar uma mensagem, foi primeiro necessário dividi-la em blocos de 16 bytes (128 bits), para que pudessem ser processados um a um. Após divididos os blocos, cada bloco é tratado como uma matriz 4x4 de bytes, sendo assim, foram definidas as seguintes operações sobre os bytes da mensagem (M) e os bytes de uma chave(K_j):

- `add_key`: $M \oplus K_j$
- `sub_bytes`: cada byte de m_i é mapeado para um novo byte m_i'
- `shif_rows`: faz uma permutação em cada linha de M
- `mix_columns`: realiza uma transformação linear em cada coluna de M

Dessa forma, para criptografar um bloco (M), a partir da chave K_0 foi necessário realizar a operação $addkey(M, K_0)$, o que resulto na matriz de blocos denominada *state*

Em seguida, a chave foi expandida em outras 10 chaves. Para as primeiras 9 chaves foi realizada a seguinte composição de funções:

$$state = addkey(mixcolumns(shiftrows(sbox(state))), K_i)$$

e por ultimo foi realizada a seguinte operação para a chave K_{10}

$$state = addkey(shiftrows(subbytes(state))), K_{10})$$

Para a decifração foi realizado um procedimento análogo, invertendo as operações, e utilizando as chaves em ordem contraria

$$state = imixcolumns(addkey(isubbytes(ishiftrows(state)), K_i))$$

E por ultimo,

$$state = addkey(isubbytes(ishiftrows(state))), K_{10})$$

2 Geração de chaves e cifra RSA

Não foi possível completar o resto do relatório, mas tentei deixar o código o mais claro possível. Peço desculpas pelo inconveniente.

2.1 Geração de chaves

2.2 OEAP

2.3 Cifração/decifração assimétrica usando OEAP

3 Assinatura RSA

3.1 Assinatura da mensagem

3.2 Formatação do resultado

4 Verificação