Network Security (NS) MTech(CLIS) Jan-Jun 2024 Lab Assignment-4.

Deadline: Solve Early Earn More

NOTE: Start Assignment-4 only after successful completion of Assignment-3. In Assignment-3, you have computed the MAC signature of a data file F using a k-byte secret key α and stored the output as a binary file named σ (Sigma).

Q.1. Write a function which takes two matrices **A** and **B** of dimensions $(p \times q)$ and $(q \times r)$ respectively, and produces the result $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ of dimension $(p \times r)$. **NOTE THAT** the multiplication is in GF(256), i.e., all the elements of both the matrices **A** and **B** are binary strings of 1-byte size, all the multiplications and additions used in producing the elements of **C** are field operations in GF(256) (byte -multiplication and byte-addition), and thus all the elements of the result matrix **C** are also binary strings of 1-byte size. Use the same irreducible polynomial (100011011) which you used in Assignment-2 and Assignment-3 as the modulus.

Place the definition of the function in 'MyCryptoLib.h' which you created in the previous assignment. Test the function by giving the input matrix **A** from terminal (keyboard) and the other input matrix **B** from an input file.

Q.2. Using the above matrix multiplication function perform the following three experiments:-

Experiment-1:

Take a data file \mathbf{F} as input from the user. Suppose file \mathbf{F} contains a total n number of blocks, each consisting of m sectors of 1-bytes. So, the data file \mathbf{F} can be treated as a matrix of size $(n \times m)$ as shown below:-

<i>s</i> ₁₁	<i>s</i> ₁₂		S_{1m}
s ₂₁	s ₂₂		s_{2m}
	-		
		-	
•	•	•	•
S_{n1}	S_{n2}		S_{nm}

Matrix F (n x m) (Data File F)

Now, from the user, take an n-byte long binary string V. Hence, the string V can be viewed as a matrix of size $(1 \times n)$ as shown below:-

Now, calling the matrix multiplication function, compute the result $\mu = V \times F$. Note that the result μ will be a matrix of size $(1 \times m)$ as shown below:

μ_1	μ_2		μ_m
---------	---------	--	---------

Result Matrix μ (1 x m)

where, for all $1 \le j \le m$,

$$\mu_j = (v_1. s_{1j} + v_2. s_{2j} + ... + v_n. s_{nj}) = \sum_{i=1}^{n} (v_i. s_{ij})$$

Print the string μ on the monitor in HEX format.

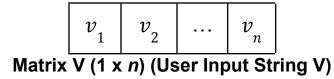
Experiment-2:

Now, use the signature file σ (Sigma) as matrix **T**. Note that, $\sigma = MACSIG(F, \alpha)$ which you have already created in Assignment-3. The signature file σ can be treated as a matrix of size $(n \times k)$ as shown below:-

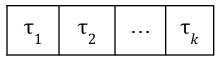
$= MAC_{\alpha_1}(b_1)$	$= MAC_{\alpha_2}(b_1)$	 $= MAC_{\alpha_k}(b_1)$
$\sigma_{21} = MAC_{\alpha_1}(b_2)$	$\sigma_{22} = MAC_{\alpha_2}(b_2)$	 $\sigma_{2k} = MAC_{\alpha_k}(b_2)$
$\sigma_{n1} = MAC_{\alpha_1}(b_n)$	$\sigma_{n2} = MAC_{\alpha_2}(b_n)$	 $\sigma_{nk} = MAC_{\alpha_k}(b_n)$

Matrix T ($n \times k$) (Tag File σ)

From the user, take the same n-byte string V which you used in Experiment-1. Hence, the string V can be viewed as a matrix of size $(1 \times n)$ as shown below:-



Now, calling the matrix multiplication function, compute the result $\tau = \mathbf{V} \times \mathbf{T}$. Note that the result τ will be a matrix of size $(1 \times k)$ as shown below:-



Result Matrix τ (1 x k)

where, for all $1 \le l \le k$,

$$\tau_l = (v_1. \sigma_{1l} + v_2. \sigma_{2l} + ... + v_n. \sigma_{nl}) = \sum_{i=1}^{n} (v_i. \sigma_{il})$$

Print the string $\boldsymbol{\tau}$ on the monitor in HEX format.

Experiment-3:

Check that:-

$$\tau == MACSIG(\mu, \alpha)$$

END