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 x q) and (q x r) respectively, and produces the result **C** = **A** x **B** of dimension (p x 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:-

<u>**Experiment-1:**</u>

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

s_{11}	s_{12}	$\cdots$	s_{1m}
s_{21}	s_{22}	$\cdots$	s_{2m}
$\vdots$	$\vdots$	$\vdots$	$\vdots$
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 x *n*) as shown below:-

v_1	v_2	$\cdots$	v_n

Matrix V (1 x *n*) (User Input String V)

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

μ_1	μ_2	$\cdots$	μ_m

Result Matrix μ (1 x *m*)

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

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

Print the string μ on the monitor in HEX format.

<u>Experiment-2:</u>

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

$\sigma_{11} = MAC_{\alpha_1}(b_1)$	$\sigma_{12} = MAC_{\alpha_2}(b_1)$	$\cdots$	$\sigma_{1k} = MAC_{\alpha_k}(b_1)$
$\sigma_{21} = MAC_{\alpha_1}(b_2)$	$\sigma_{22} = MAC_{\alpha_2}(b_2)$	$\cdots$	$\sigma_{2k} = MAC_{\alpha_k}(b_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\sigma_{n1} = MAC_{\alpha_1}(b_n)$	$\sigma_{n2} = MAC_{\alpha_2}(b_n)$	$\cdots$	$\sigma_{nk} = MAC_{\alpha_k}(b_n)$

Matrix T (*n* x *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 x *n*) as shown below:-

v_1	v_2	$\cdots$	v_n

Matrix V (1 x *n*) (User Input String V)

Now, calling the matrix multiplication function, compute the result τ = **V** x **T**. Note that the result τ will be a matrix of size (1 x *k*) as shown below:-

τ_1	τ_2	$\cdots$	τ_k

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 τ on the monitor in HEX format.

Experiment-3:

Check that:-

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

END