International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Lab Assignment 2: A Practical Application: Error Detection used in Computer Communications for Data Link Layer Security

Hard Deadline: **February 12, 2021 (23:55 P.M.)**

Total Marks: 100

Note:- *It is strongly recommended that no student is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Please upload in code along with a README file in the course moodle portal through a ZIP file (RollNumber-Lab2.zip).*

Problem Description

Definition 1 (Linear Transformation)**.** *Let V and W be vector spaces over the same field F. A mapping $T : V \to W$ is called a linear transformation from V into W, if it preserves addition and scalar multiplication, that is,*

(i) $T(u + v) = T(u) + T(v)$

(ii) $T(\alpha u) = \alpha T(u), \forall u, v \in V, \alpha \in F.$

Example 1 (Linear Transformation)**.** *Let $M_{2\times3}(C)$ be the space of all 2×3 matrices with complex entries. Define $T : M_{2\times3}(C) \to M_{3\times2}(C)$ be a mapping (transformation) by $T(A) = A^t$, where A^t is the transposition of the matrix A.*

Let $A, B \in M_{2\times3}(C)$ and $\alpha \in C$. Then, T is a linear transformation, because
(i) $T(A + B) = (A + B)^t = A^t + B^t = T(A) + T(B)$
(ii) $T(\alpha A) = (\alpha A)^t = \alpha A^t = \alpha T(A)$.

Note that if V and W be vector spaces over the same field F, and a linear transformation $T : V \to W$ is invertible, then $T^{-1} : W \to V$ is also a linear transformation.

Consider a variant of secure data link security protocol as described in Figure 1. Also, consider a secret cipher matrix, A, which is known to only transmitter and receiver, where $A = \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}_{3\times3}$ such that its inverse A^{-1} exists.

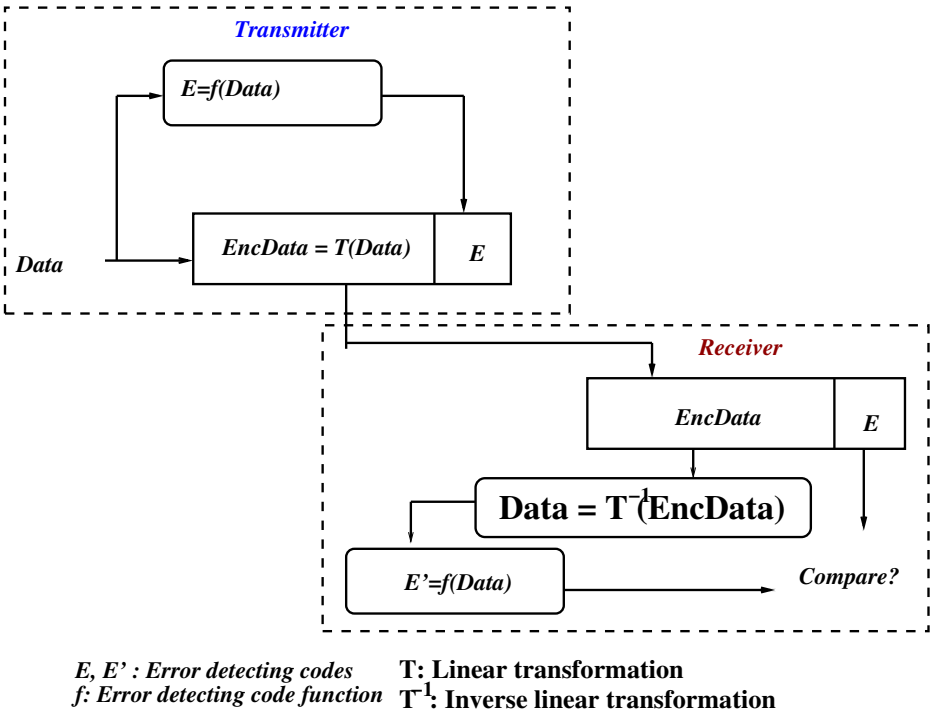

Figure 1: Error detection

Table 1: Encoding Rule

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z		Blank space
15	16	17	18	19	20	21	22	23	24	25	26		27

Let us map each character to its equivalent numeric value as shown in Table 1.

Let the message (Data) be (for example) $Data =$ PENGUINS ARE ONE TO ONE

The $Data$ is then transformed into the numerical equivalent as: 16, 5, 14, 7, 21, 9, 14, 19, 27, 1, 18, 5, 27, 15, 14, 5, 27, 20, 15, 27, 15, 14, 5

We compute error detecting code on $Data$ as $E = f(Data)$ using public error detecting code function f, say **cyclic redundancy check (CRC)**.

We separate the plaintext $Data$ into 3×1 vectors until the whole plaintext is used. We augment the above vectors into a plaintext matrix, say $p = \begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix}_{3\times 8}$

Consider a linear transformation $T : \mathcal{P} \to \mathcal{C}$, where $\mathcal{P}$ and $\mathcal{C}$ are the vector spaces representing the plaintext space and ciphertext space, respectively, defined by $T(p) = Ap$. Thus, $p = A^{-1}.T(p)$. Hence, inverse linear transformation $T^{-1} : \mathcal{C} \to \mathcal{P}$ is defined.

Now, calculate $EncData = T(Data) = A.p$

$$= \begin{bmatrix} -119 & -120 & -207 & -77 & -182 & -176 & -186 & -165 \\ 19 & 30 & 46 & 23 & 29 & 47 & 42 & 32 \\ 135 & 127 & 221 & 78 & 209 & 181 & 201 & 179 \end{bmatrix}_{3\times 8}$$

The transmitter sends the message $\{EncData, E\}$ to the receiver.

The receiver separates the $EncData$ from the error detecting code (E), and applies the inverse linear transformation $T^{-1} : \mathcal{C} \rightarrow \mathcal{P}$ on $EncData$ using the inverse cipher matrix $A^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}_{3\times 3}$ as follows: $p = T^{-1}(EncData) = A^{-1}.EncData$

$= \begin{bmatrix} 16 & 7 & 14 & 1 & 27 & 5 & 15 & 14 \\ 5 & 21 & 19 & 18 & 15 & 27 & 27 & 5 \\ 14 & 9 & 27 & 5 & 14 & 20 & 15 & 27 \end{bmatrix}_{3\times 8} \rightarrow$

$\begin{bmatrix} P & G & N & A & & E & O & N \\ E & U & S & R & O & & & E \\ N & I & & E & N & T & O & \end{bmatrix}$

Thus, the $Data$ = "PENGUINS ARE ONE TO ONE". We recompute the error detecting code $E' = f(Data)$. Check if $E' = E$? If so, no error is detected during the communication by the receiver.

Implement the above the scheme using a client-server programming model by assuming the transmitter as the client and receiver as the server. Your implementation should allow variable plaintext message as input. You can fix the cipher matrix as pre-fixed for simplicity.

All the best!