COL759: Introduction to Cryptography

Tutorial-1

Question 3

We have modified the logic of the Playfair cipher since it has become a difficult question. We are skipping commas, spaces, and full stops to generate the ciphertext. For each word, if the length of the word is odd then we are appending 'X' to the plaintext before generating the ciphertext. All the remaining rules are the same.

Ciphertext is the same for everyone.
New Ciphertext can be found in the second sheet in the following link: Sheet Link.

Further reducing its difficulty we are revealing some parts of the key as below.

_	_	_	D	_
_	_	_	S	_
_	_	_	E	_
_	_	_	P	_
V	W	X	Y	Z

Example using the modified Playfair Cipher logic:
Assume the plaintext `HI INDIA`:

- Break into digraphs: `HI`, `IN`, `DI`, `AX`
- Encrypt using the Playfair matrix.

So, `HI INDIA` might be encrypted to `GY YTUIBH`.
Note: The example doesn't follow the original key mapping as given above.