COL759: Introduction to Cryptography

Tutorial-1 [5 Marks]

Question 1

For this question, you are given a ciphertext and need to find the corresponding key and plaintext using a substitution cipher. In this cipher, each lowercase letter is substituted with a different letter according to a key that is a permutation of all 26 letters of the alphabet. While encrypting, we skip all commas, and all other characters remain unchanged. Since each student's ciphertext is different, we have created a file where you can find your ciphertext based on your entry number. For this question the ciphertext is Ciphertext 1.
Please access your file here: Sheet Link.

Note: You simply need to copy the cell against your Entry No and ciphertext for analyzing.

Example of Substitution Cipher:
Assume a key where each letter of the alphabet is substituted by another letter. For example:

- Plaintext alphabet: `abcdefghijklmnopqrstuvwxyz`
- Key (cipher alphabet): `mnbvcxzlkjhgfdsapoiuytrewq`

To encrypt the plaintext: `hello, how are you.`

- `h` is substituted with `l`
- `e` is substituted with `c`
- `l` is substituted with `g`
- `l` is substituted with `g`
- `o` is substituted with `s`

So, `hello, how are you` becomes `lcggs lsr moc wsy.`

Question 2

Similarly, for this question, you are provided with a ciphertext and need to determine the key and plaintext using a substitution cipher. Each lowercase letter is substituted with a different letter according to a key that is a permutation of all 26 letters of the alphabet. While encrypting, we skip all characters apart from the alphabets. Since each student's ciphertext is unique, you can find your ciphertext under Ciphertext 2: Sheet Link.

Example of Substitution Cipher:
Assuming a different key for substitution:

- Plaintext alphabet: `abcdefghijklmnopqrstuvwxyz`
- Key (cipher alphabet): `mnbvcxzlkjhgfdsapoiuytrewq`

To encrypt the plaintext `hello, how are you.`

- `h` is substituted with `l`
- `e` is substituted with `c`
- `l` is substituted with `g`
- `l` is substituted with `g`
- `o` is substituted with `s`

So, `hello, how are you` becomes `lcggslsrmocwsy`

Question 3

For this question, you are provided with a ciphertext and need to determine the key and plaintext using a Playfair cipher. The Playfair cipher encrypts pairs of letters (digraphs) rather than single letters, using a keyword to generate a 5x5 matrix of letters. The encryption process depends on the position of the letters in this matrix.

The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I. While encrypting we are only considering the alphabets and skipping the rest of the characters.

To encrypt using the Playfair cipher:

- Construct the Playfair matrix using the keyword. For example, with the keyword `KEYWORD`:

K	E	Y	W	O
R	D	A	B	C
F	G	H	I	L
M	N	P	Q	S
T	U	V	X	Z

- Break the plaintext into digraphs (pairs of letters). If a digraph consists of the same letter twice, insert a filler letter (e.g., `x`).
- Encrypt each digraph based on their positions in the matrix:
  - If both letters are in the same row, replace them with the letters immediately to their right (wrap around if necessary).
  - If both letters are in the same column, replace them with the letters immediately below them (wrap around if necessary).
  - If the letters form a rectangle, replace them with the letters on the same row but at the opposite corners of the rectangle.

Since each student's ciphertext is unique, you can find your specific ciphertext file here: Ciphertext 3: Sheet Link.
Example of Playfair Cipher:
Assume the plaintext `HELLO`:

- Break into digraphs: `HE`, `LL`, `OX`
- Encrypt using the Playfair matrix:
  - `HE` becomes `GY`
  - `LL` (Since both are same character replace second L with X, so it becomes LX) becomes `IZ`
  - `OX` (O is in row 1, column 5 and X is in row 5, column 4) becomes `WZ`

So, `HELLO` might be encrypted to `GYIZWZ`.

Submission

- **You need to submit a report in pdf format that contains your plain_text, key, and cipher_text for all three questions on Moodle.**
- **Mention briefly your approach for finding the plaintext and key in the report**
- **Deadline: 11th August 11:59PM**