Introduction to Cryptography 2

Polyalphabetic Substitution Ciphers # 1

Yicheng Wang

White Hat Academy

2015-05-04

Review

Decipher this:

Zgyzhs rh vzhb

This is encrypted using a monoalphabetic substitution cipher.

Polyalphabetic Substitution Cipher

- As we've seen last time. Monoalphabetic substitution ciphers are not the most secure way of encrypting things.
- To get around this, people have invented polyalphabetic substitution cipher, this uses a different substitution system for each letter.
- Today we'll look at two basic polyalphabetic substitution ciphers: Tabula Recta and Vigenre Cipher.

Tabula Recta

- This cipher uses the table as illustrated on the next slide.
- It has 26 rows, each row a shift of the alphabet.
- With each letter we use a different row to encrypt it. For example, the tabula recta encryption of “hello” is “igopt.”

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

FIGURE : The Tabula Recta Table

```java
public class TabulaRecta {
    private char[][] board;
    private final String alphabet = "abcdefghijklmnopqrstuvwxyz";
    private char[] plainArray;

    private void genBoard() {
        board = new char[alphabet.length()][alphabet.length()];
        for (int i = 0 ; i < alphabet.length() ; i++) {
            for (int j = 0 ; j < alphabet.length() ; j++) {
                board[i][j] = alphabet.charAt((j + i) % 26);
            }
        }
    }
    public TabulaRecta(String s) {
        genBoard();
        plainArray = s.toCharArray();
    }
    public String encrypt() {
        StringBuilder cipherText = new StringBuilder();
        for (int i = 0 ; i < plainArray.length ; i++) {
            cipherText.append(board[(i + 1) % board.length][indexOf(board[0],
     plainArray[i])]);
        }
        return cipherText.toString();
    }
    public int indexOf(char[] arr, char el) {
        for (int i = 0 ; i < arr.length ; i++) {
            if (arr[i] == el) {
                return i;
            }
        }
        return -1;
    }
```

Vigenre Cipher

- Vigenre cipher is an improvement upon the old Tabula Recta cipher.
- It is developped by French cryptographer Blaise de Vigenre.
- It uses a key to determine which row to go to instead of going throw the entire alphabet from A to Z.
- For example, if the message is "APCSTESTTHURSDAY" and the key being "JAVA", we would first repeat the key until it matchs the length of the message, which would make the key "JAVAJAVAJAVAJAVA."
- Then, for each letter is encrypted using the tabula recta method on the row of the corresponding letter in the key.
- So "APCSTESTTHURSDAY" will encrypt to "JPXSCENTCHPRBDVY"

Breaking Vigenre

- The idea behind all polyalphabetic substitution ciphers is to disguise letter frequency to disrupt regular frequency analysis.
- If we have a crib, this makes our lives a lot easier. Because with the crib, the ciphertext and the encryption table, we can easily figure out the table and find the key, which in turn allows us to find the plaintext.
- Here's a contrieved exercise, we have intercepted the following encrypted message:

  mtltgbfoehviawsmhrin

- We know that the plaintext starts with the word "attack." and the key (hopefully) also has that length.
- Figure out the original message!

- However, we don't always know a crib, or the key length for that matter. Once we have the keylength, it is easy to figure out where the key repeats and Vigenere cipher breaks down to a series of interwoven Caesar shifts, each of which can be easily brute forced.
- The keylengths are determined by the Kasiski and Friedman tests. Which will be covered, eventually. (Mathy stuff ahead)