German University in Cairo
Faculty of Media Engineering and Technology
Mervat Abu-Elkheir
Mohamed Abdelrazik
Ahmad Helmy

CSEN1001: Computer and Network Security

Spring Term 2019

Tutorial 2

Mono Alphabetic Substitution Ciphers

- Mono-alphabetic substitution cipher was first used by Hebrew scholars.
- Spartan military, other Greek states, 7th–1st century BC used scytales to perform transposition ciphers.
- A transposition cipher is one that includes shifting one or more character according to a system.
- Other Examples:
  - Caesar Cipher http://www.braingle.com/brainteasers/codes/caesar.php
  - Playfair Cipher http://rumkin.com/tools/cipher/playfair.php

A Scytale

Problem 1

Decrypt the following scytale **transposition cipher**. Consider the whitespaces as normal characters.

ys boetourhn veude se

Answer

A scytale cipher works by wrapping a tape of paper around a rod and writing the letters in sequence on the wrapped tape, resulting in a regular displacement of the letters on the unfolded tape.

In the absence of any knowledge about the diameter of the rod or the number of letters across, one will have to try all possible combinations. Start with two letters down, we get:

y	space	o	t	u					
s	b	e	o						

We can see that even if we continue we will get no useful words. Let's try three letters down. We get:

y	b	t							
s	o	o							
space	e	u							

Also here, we have no useful word to start the sentence. Trying 4 letters down, we get:

y	o	u	space	d	e				
s	e	r	v	e					
space	t	h	e	space					
b	o	n	u	s					

The result is:

you deserve the bonus

Problem 2

Romans are known to have used a simple substitution cipher called **Caesar cipher**. Each letter in the message is replaced by a letter some fixed number of positions down the alphabet.
Example: three positions.
Plain: 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
Cipher: 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
The following cipher texts have been encrypted using Caesar cipher, find out the original text:

m xlmro, xlivijsvi m ibmwx

Answer

Ceasar Cipher is broken either with brute force or frequency analysis.
Using Frequency Analysis, the letter 'm' is repeated, and single letter words are scarce in English; examples are 'a' and 'I'.
To decipher the rest of the text, we find the shift needed to turn 'm' to 'a' and 'm' to 'I', whichever produces a meaningful sentence is the correct shift.
Fours shifts backwards are needed to turn 'm' to 'I', continuing to shift each of the letters of the cipher text 4 shifts backwards produces the decrypted text:

I think, therefore I exist

Polyalphabetic Substitution Ciphers

- A polyalphabetic cipher is one that involves substituting each character by more than one substitution.
- The Vigenère cipher is a well-known is a simple example.
- Using Rotor Machines to make it more complex for example: The Enigma Machine.
- How it works? http://www.telegraph.co.uk/culture/film/11229586/Imitation-Game-how-did-the-Enigma-machine-work.html

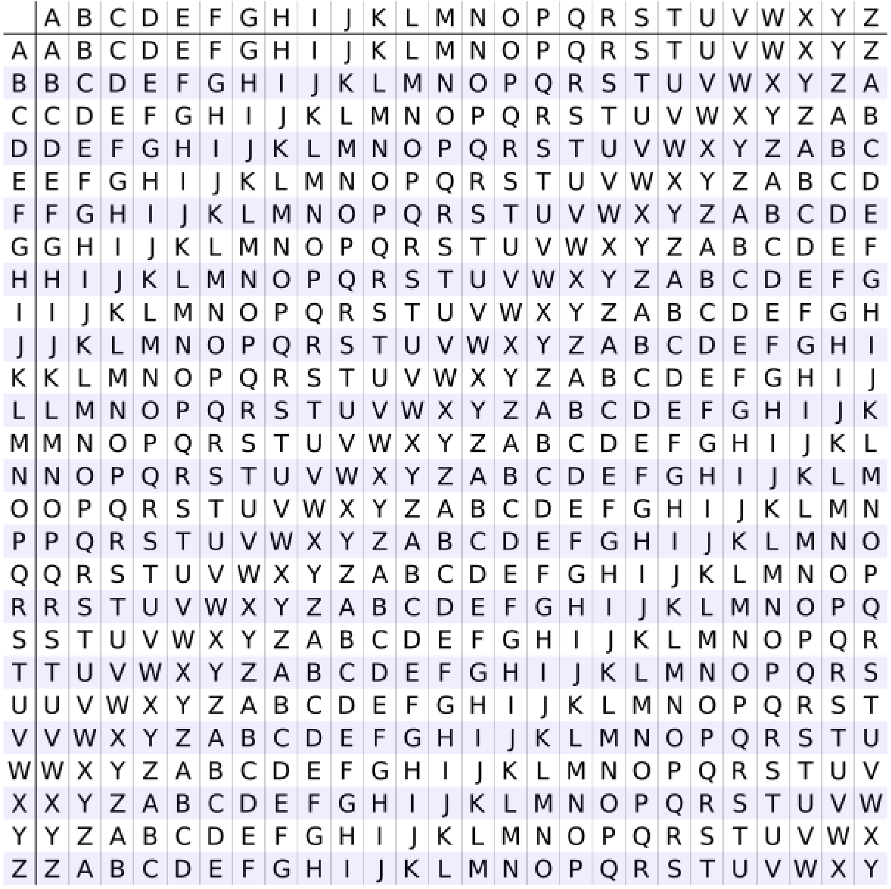
Problem 3

The Vigenère cipher is a method of encrypting alphabetic text. It is a form of poly-alphabetic substitution.

a) Encrypt “Attack Now” using Vigenère cipher, with the keyword “Play” using tabula recta below.

b) Perform an examination to find the length of the key that was used to produce the following Vigenère cipher text:

io ygx wewq ss tswmw nzl eytluonnr. Vs wewq ss hzo aj acw ysamdi yo mw eytluojd.



	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

Answer

a) Plain text: “a t t a c k n o w”
Key : “p l a y p l a y p”
Result : “p e t y r v n m l”

b) A brute force attack or a Kasiski examination is used to break the Vigenère cipher. The "Kasiski examination involves looking for strings of characters that are repeated in the ciphertext. The strings should be three characters long or more for the examination to be successful. Then, the distances between consecutive occurrences of the strings are likely to be multiples of the length of the keyword. Thus finding more repeated strings narrows down the possible lengths of the keyword, since we can take the greatest common divisor of all the distances."

More info here: http://en.wikipedia.org/wiki/Kasiski_examination

First, we find repetitions of sequences in the cipher:

io ygx wewq ss tswmw nzl eytluonnr. vs wewq ss hzo aj acw ysamdi yo mw eytluojd.

The distances between repetitions are 25 characters and 35 characters respectively.
Using prime factorization:
$25 = 5 \times 5$
$35 = 5 \times 7$
Therefore the gcd = 5
This indicates a key length of 5.

Problem 4

The Vigenère autokey cipher is a modification over the traditional Vigenère cipher, where the key that is used for encryption is generated from a passphrase plus the plaintext itself. For example, to encrypt the phrase "*Ilovesecurity*" using the passphrase "*frog*", the encryption key becomes "*frogIlovesecu"*. A two-stage encryption algorithm is built using a Vigenère autokey cipher followed by a transposition cipher. The passphrase for the Vigenère autokey cipher is "goal" and the key for the transposition cipher is 3 5 4 1 2. Decrypt the following ciphertext to obtain the plaintext.

LFTWUXNQVKSOUWASRHTBCZZJJ

(*Hint*: Rearrange the ciphertext into a 5×5 matrix according to the transposition key 3 5 4 1 2, and then produce the ciphertext before transposition. Proceed to decrypt the resulting ciphertext following the Vigenère autokey scheme explained above.)

Answer

Ciphertext transposition encryption

3	5	4	1	2
S	C	S	L	X
O	Z	R	F	N
U	Z	H	T	Q
W	J	T	W	V
A	J	B	U	K

Decryption of transposition is SCSLXOZRFNUZHTQWJTWVAIJBUK

Decrypt the first 4 letters SCSL using the passphrase "goal" gives MOSA. Thus, we decrypt the next 4 letters XOZR using MOSA to get LAHR, and decrypt the next 4 letters FNUZ using LAHR to get UNNI, and so on.

We continue to get the phrase MOSALAHRUNNINGDOWNTHEWING

Or *Mo Salah Running Down The Wing*