#### YALE UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE

CPSC 467: Cryptography and Computer Security

Professor M. J. Fischer

Handout #4 September 15, 2020

# **Homework Assignment 3**

Due on Tuesday, September 22, 2020

### Goal

The goal of this problem set is to get some hands-on experience at cryptanalysis for monoalphabetic substitution ciphers.

## What to do

- (a) Solve the two cryptograms<sup>1</sup> in Figures 1 and 2, *by hand*. I know there are cryptogram solvers on the internet. Don't use them. The point of this assignment is for you to get a feeling for things that are so easy that they can even be done by hand.
- (b) For each cryptogram, write the plaintext letters on the line above the corresponding ciphertext letters. Also, fill in as much of the substitution table at the top as needed. The top row represents plaintext letters. The boxes underneath should be filled in with the corresponding ciphertext letters.
- (c) Describe what you did to find the solution.

# How to submit

There are two ways to record your solutions:

- (a) Print out the puzzles, write in the solutions by hand, scan the solution sheets to PDF, and submit the PDF to Canvas as usual.
- (b) Download the assignment PDF, use a PDF annotation tool to fill in your answers, save the annotated version, and submit it as usual.

If you take the first option, be sure to use a proper scanning tool to create a legible PDF. If you have access to a scanner, great! If not, you can use the CamScanner on your smart phone or tablet. It's free if you don't mind the ads and the watermark that it puts on the scan. (I don't mind.)

For the second option, Adobe Acrobat and the osx Preview.app both offer good annotation tools. Canvas also has annotation tools, so perhaps your paper never needs to leave Canvas.

<sup>&</sup>lt;sup>1</sup>Created by Puzzlemaker at DiscoveryEducation.com

	А	В	С	D	E	F	G	н	I	J	к	L	м	Ν	0	P	Q	R	s	Т	U	۷	w	×	У	Ζ		
	•	•	_										_						_						z	;		
			T	н	Л	1 >	< 1	N	K		X I	N	٢	, ,	ĸ	ν	в	ĸ		þ	ĸ	v	в	ĸ	Ζ			
I	н	Ν	×	N	-	к	×	N	-	I	Н	s	R	l		Z	В	1	4	p	R	1	u'	В	В	N	-	
P R																											N	
P	R		v –	в	R	-		R	p	R	۷	В	R	z		-	I	н	к	I		s	Z		I	۷		
<u>z к</u> ,	4	В		1	p	R		/ 1	в				<u>ч</u>	×	N	_	к	×	N	-		v	С	N		I	н	s
R L	z	-	В	N	-	0	V		R	۷	I		P	R	٧	В	- •	-	Q	U	I	-	I	н	N	×	N	
к×	N	-	<	F	z	۷	-	U	R	p	R	V		R	_	U	R		R			3	R	z		<u>с</u> н	N	-
V	R	Ν	Z		В	N	-	(		v	R		I	Ŀ		2	v	в	-	3 1	1	0		v'	R	I		
P F	2	v	в	•		У	×	٧	С	-	0	٧	R									z	У	N	F	0	•	
					_	y									1	2		2	0 0	) 2								

Figure 1: Puzzle 1



Figure 2: Puzzle 2