CS 5158/6058 Data Security and Privacy, Spring 2018
Homework 1

Instructor: Dr. Boyang Wang

Due Date: 01/25/2018 (Thursday), 11:59pm.
Format: Please submit a pdf of your homework in Blackboard.
Total Points: 6 points

Problem 1 (1 point). Given a ciphertext `JSSXFEPP` encrypted by Shift Cipher, compute the key of shift cipher and the original message using brute-force attacks. In this problem, we assume the original message "makes sense" and is human-readable. The message space includes all the lower case characters, i.e., $\mathcal{M} = \{\mathtt{a}, \mathtt{b}, ..., \mathtt{z}\}$, key space is $\mathcal{K} = \{0, 1, ..., 25\}$ and ciphertext space is $\mathcal{C} = \{\mathtt{A}, \mathtt{B}, ..., \mathtt{Z}\}$.

Problem 2 (1 point). Given an encryption key (i.e., a permutation) of Substitution Cipher presented below, compute the ciphertext of a message `universityofcincinnati`.

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

If the message space of Substitution Cipher has a number of 50 unique characters/symbols, what is the size of the key space? In other words, how many permutations in total?

Problem 3 (1 point). Assume the key of Vigenere Cipher is `cats`, what is the ciphertext of a message `datasecurity` encrypted by this key using Vigenere Cipher? What is the size of the key space for Vigenere Cipher if each key is a string of 4 characters? For easy calculation, a mapping table between characters (a, ..., z) and integers (0, ..., 25) is listed below.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Problem 4 (1 point). Assume we have a sequence of 100 characters, the frequency distribution of different characters is listed below, compute the (approximated) index of coincidence (IC) of this sequence.

char	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
frequency	1	1	1	1	1	1	1	1	1	1	5	5	5	5	5	5	5	5	10	10	10	10	10	0	0	0

Problem 5 (1 point). An adversary analyzes a sequence of (ciphertext) characters, which is encrypted by Vigenere Cipher, using Kasishi's method. In addition, it knows the key length is at least 2. If it can find a sub-string with a length of 4 repeated twice in the sequence, and the distance between the two repeated sub-strings is 12, what are the possible key length of this Vigenere cipher?

Problem 6 (1 point). Assume an attacker knows the index of coincidence in plaintext is $\mathrm{IC}_{plain} = 0.090$. Given a long sequence of (ciphertext) characters, e.g.,

$$c_1c_2c_3c_4c_5c_6c_7c_8c_9.....$$

which is encrypted by Vigenere Cipher, explain how to calculate/estimate the key length by using the index of coincidence.