CS 435: Introduction to Cryptography **2012 Fall**

Homework 1

Professor Somesh Jha **Due:** September 28

1. (Exercise 1.3) Consider an improved version of the Vigenère cipher, where instead of multiple shift ciphers, multiple mono-alphabetic substitution ciphers are used. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions i, $t+i$, $2t+i$, and so on are encrypted using the i-th permutation. Show how to break this version of the cipher.

2. (a) (Exercise 1.5) Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a known-plaintext attack. How much known plaintext is needed to completely recover the key for each of the ciphers?

   (b) (Exercise 1.6) Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext must be encrypted in order for the adversary to completely recover the key? Compare your solution to part (a).

3. Consider a variant of the monoalphabetic substitution cipher where the ciphertext alphabet is twice as large as the plaintext alphabet, and each plaintext character is encrypted to one of two possible ciphertext characters. More formally, the key k consists of a random permutation of

   $$\texttt{ABC}\ldots\texttt{YZ}\underline{\texttt{ABC}}\ldots\underline{\texttt{YZ}},$$

   i.e. the alphabet and an underlined duplicate. Putting the plaintext alphabet in correspondence with $\{0, 1, \ldots, 25\}$ (so that `a` corresponds to 0, `b` to 1, etc.), each plaintext character m_i is then independently and randomly encrypted to either the m_i-th character of k or the $(m_i + 26)$-th character of k. For example, if

   $$k = \underline{\texttt{NU}}\texttt{MYENB}\underline{\texttt{F}}\texttt{ICA}\underline{\texttt{D}}\texttt{J}\underline{\texttt{W}}\texttt{U}\underline{\texttt{YLG}}\texttt{DF}\underline{\texttt{IX}}\texttt{K}\underline{\texttt{Q}}\texttt{G}\underline{\texttt{O}}\texttt{V}\underline{\texttt{KT}}\texttt{Z}\underline{\texttt{V}}\texttt{PW}\underline{\texttt{SM}}\underline{\texttt{H}}\underline{\texttt{H}}\texttt{L}\underline{\texttt{E}}\texttt{T}\underline{\texttt{B}}\texttt{OAS}\underline{\texttt{R}}\texttt{X}\underline{\texttt{P}}\texttt{R}\underline{\texttt{CJZ}}\texttt{Q},$$

   then the encryption function can be visualized as

a	b	c	d	e	f	g	h	i	j	k	l	m
N	U	M	Y	E	N	B	F	I	C	A	D	J
V	K	T	Z	V	P	W	S	M	H	H	L	E

n	o	p	q	r	s	t	u	v	w	x	y	z
W	U	Y	L	G	D	F	I	X	K	Q	G	O
T	B	O	A	S	R	X	P	R	C	J	Z	Q

where `a` is encrypted to either `N` or `V`, each with probability 1/2, `b` to `U` or `K`, and so on.

Describe a ciphertext-only attack that recovers the plaintext.

(*Hint.* What would a graph of letter frequencies for ciphertext encrypted using the example k look like?)

4. Consider a variant of the Vigenère cipher where instead of a word or short phrase, the key instead consists of a book or some other English-language text that is much longer than the message to be encrypted. Using this cipher, the key is never repeated, so Kasiski's attack will fail.

   Now assume that Alice, using this cipher, sends Bob a ciphertext that reads

   `JLQJRYFQEKL`.

   The plaintext is known to be either `vegetarians` or `bacongrease`. Determine which plaintext Alice sent to Bob, and explain how you reached your answer.

   Note. Each ciphertext character c_i is equal to $m_i + k_i \pmod{26}$, where m_i is the i-th character of the paintext message and k_i is the i-th character of the key. In particular, the alphabet is indexed from 0, so `a` corresponds to 0, `b` corresponds to 1, and so on.

   (*Hint.* What possible values for the key are there?)