MATH 75: MATHEMATICAL CRYPTOGRAPHY
HOMEWORK #2

Problems

Problem 1. The following ciphertext was generated using a simple substitution algorithm:

```
53ddc305))6*;4826)4d.)4d);806*;48c8p60))85;;]8*;:d*8c83
(88)5*c;46(;88*96*?;8)*d(;485);5*c2:*d(;4956*2(5*-4)8p8*
;4069285);)6c8)4dd;1(d9;48081;8:8d1;48c85;4)485c528806*81
(d9;48;(88;4(d?34;48)4d;161;:188;d?;
```

Decrypt the message. *[Warning: The resulting message is in English but may not make much sense on a first reading.]*

Problem 2. A disadvantage of the general substitution cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword `CIPHER`, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

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

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generated the sequence by reading down the columns:

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

This yields the sequence: `C A K S Y I B L T Z P D M U H F N V E G O W R J Q X`.

Such a system is used in the following ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
directcontactshavebeenmadewithpolitical

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
representativesofthevietconginmoscow
```

Determine the keyword.

Problem 3. Let $n \geq 3$. We say that $\sigma \in S_n$ *has a fixed point* if there exists $k \in \{1, \ldots, n\}$ such that $\sigma(k) = k$. Prove that the probability that a random $\sigma \in S_n$ has a fixed point

Date: Due Wednesday, 13 April 2016.

is $\geq 5/8$ and $\leq 2/3$. (Conclude that a random substitution cipher, realized as a random permutation in S_n, is likely to fix at least one symbol.)

Problem 4. Let $a, b \in \mathbb{Z}$.

(a) Let $\gcd(a, b) = g \neq 0$. Prove that $\gcd(a/g, b/g) = 1$.
(b) Prove that $\gcd(a + kb, b) = \gcd(a, b)$ for all $k \in \mathbb{Z}$.

Problem 5.

(a) Use the extended Euclidean algorithm to compute 367^{-1} in $(\mathbb{Z}/1001\mathbb{Z})^*$ and 1001^{-1} in $(\mathbb{Z}/367\mathbb{Z})^*$. [Do this by hand.]
(b) [Sage] Compute $314159265^{-1} \pmod{2718281828}$. [You may use a computer!]

Problem 6. Let $f_0 = f_1 = 1$ and $f_{i+1} = f_i + f_{i-1}$ for $i \geq 1$ denote the Fibonacci numbers.

(a) Use the Euclidean algorithm to show that $\gcd(f_i, f_{i-1}) = 1$ for all $i \geq 1$.
(b) Find $\gcd(11111111, 11111)$.
(c) Let $a = 111\cdots11$ be formed with f_i repeated 1s and let $b = 111\cdots11$ be formed with f_{i-1} repeated 1s. Find $\gcd(a, b)$. *[Hint: Compare your computations in parts (a) and (b).]*

Problem 7. Let $a, b \in \mathbb{Z}_{>0}$ with $a > b$.

(a) Show that $a - b$ can be computed in time $O(\log a)$.
(b) Suppose that the Euclidean algorithm is performed on $r_0 = a, r_1 = b$ with successive quotients q_i defined by $r_{i-1} = q_i r_i + r_{i+1}$. Show (by induction) that $a \geq q_1 \cdots q_t$, so that $\log a \geq \sum_i \log q_i$. Conclude that the Euclidean algorithm runs in time $O\big((\log a)(\log b)\big)$.