

Problem Set # 2 (upload to Canvas by Friday, April 15, 10:10 am EDT)

Problems:

1. 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 generate 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 decoded ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMZSHZOWSFPAPPDTSVPQUZWMXUZHXS
directcontactshavebeenmadewithpolitical

EPYEPDPDZSZUFPOMBZWPFPZHMZJUDTMOHMQ
representativesofthevietcong inmoscow

Determine the keyword.

2. Let $n \geq 3$ and S_n be the symmetric group on $\{1, \dots, n\}$. We say that $\sigma \in S_n$ has a *fixed point* if there exists $k \in \{1, \dots, n\}$ such that $\sigma(k) = k$. Prove that the probability that a random $\sigma \in S_n$ has a fixed point is $\geq 5/8$ and $\leq 2/3$. Here, “probability” means that the number of those permutations with a fixed point divided by the number of all permutations. (Conclude that a random substitution cipher, realized as a random permutation in S_n , is likely to fix at least one symbol.)

3. 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 $k \in \mathbb{Z}$.

We stated this in lecture, but now you can check it carefully yourself!

4. Compute some inverses!

(a) Use the extended Euclidean algorithm to compute 367^{-1} in $(\mathbb{Z}/1001\mathbb{Z})^\times$ and 1001^{-1} in $(\mathbb{Z}/367\mathbb{Z})^\times$. [Do this by hand.]

(b) Compute 314159265^{-1} in $(\mathbb{Z}/2718281828\mathbb{Z})^\times$. [You may use a computer!]

5. 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 $i \geq 1$. (Again, we did this quickly in lecture, but now do it carefully!)

(b) Find $\gcd(11111111, 11111)$.

(c) Let $a = 111 \cdots 11$ be formed with f_i repeated 1s and let $b = 111 \cdots 11$ be formed with f_{i-1} repeated 1s. Find $\gcd(a, b)$.

[Hint: Compare your computations in parts (a) and (b).]