

M360 Mathematics of Information Security

exercise sheet # 4

Exercise # 1

(2 points)

Suppose you have a language with only 3 letters a, b, c, and they occur with frequencies .7, .2, .1, respectively. The following ciphertext was encrypted by the Vigenère method (shifts are mod 3 instead of mod 26, of course):

CAAABBCACBCABACAABCCCACA.

Show that it is likely that the key length is 2, and determine the most probable key.

Exercise # 2

(2 points)

Ernie, Bert and the Cookie Monster want to measure the length of Sesame Street. Each of them does it his own way. Ernie relates: “I made a chalk mark at the beginning of the street and then again every 7 feet. There were 2 feet between the last mark and the end of the street” Bert tells you: “Every 11 feet there are lamp posts in the street. The first is 5 foot from the beginning and the last one exactly at the end of the street” Finally Cookie Monster says: “starting at the beginning of Sesame Street, I put down a cookie every 13 feet. I ran out of cookies 22 feet from the end.” All three agree that the length does not exceed 1000 feet. How many feet is Sesame Street long?

Exercise # 3

(2 points)

a) Let p be prime. Suppose a and b are integers such that $ab \equiv 0 \pmod{p}$. Show that either $a \equiv 0$ or $b \equiv 0 \pmod{p}$.

b) Show that if a, b, n are integers with $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Exercise # 4

(2 points)

Let $p \geq 3$ be prime. Show that the only solution to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. Hint: Apply part a) of the previous exercise to $(x+1)(x-1)$.

Exercise # 5

(2 points)

Suppose $x \equiv 3 \pmod{7}$ and $x \equiv 3 \pmod{10}$. What is x congruent to mod 70?

due to Friday, 10/7/05.