MATH 1025: Introduction to Cryptography

Homework 1

welcome to the class[1]

Problem 1.

(a) [10 **pts**] A shift cipher maps a to e. Decode the message "aipp hsri!"

(b) [10 **pts**] Encode the message that you obtained in (a) using the simple substitution cipher

$$\begin{aligned} &a \longleftrightarrow z,\\ &b \longleftrightarrow y,\\ &c \longleftrightarrow x,\\ &\dots\\ &m \longleftrightarrow n. \end{aligned}$$

(c) [10 **pts**] Is the cipher in (b) a shift cipher? Justify your answer.

[1] This cipher appeared in The Return of Sherlock Holmes by Sir Arthur Conan Doyle, "The Adventure of the Dancing Men".

Problem 2. Use Euclid's algorithm and a calculator to compute

(a) [10 **pts**] $\gcd(2834, 90)$.

(b) [10 **pts**] $\gcd(238792, 7843)$.

Problem 3 [10 **pts**] Use extended Euclid's algorithm to find x and y, such that $2834x + 90y = 2$.

Problem 4. Let a and b be positive integers.

(a) [10 **pts**] Suppose that there are integers x and y satisfying $ax + by = 1$. Prove that $\gcd(a, b) = 1$.

(b) [10 **pts**] Suppose that there are integers x and y satisfying $ax + by = 12$. Is it necessarily true that $\gcd(a, b) = 12$? If so, give a proof, if not, give a specific counterexample, and describe possible values of $\gcd(a, b)$.

Problem 5.

(a) [10 **pts**] Without using a calculator or long division, find out if 43279 is divisible by 7.[2]

(b) [10 **pts**] For which value(s) of digit $a \in \{0, 1, 2, \ldots, 9\}$ is the number $\overline{42a7321}$ divisible by 7? Justify your answer.

[2] **Hint:** $43279 = 4 \cdot 10^4 + 3 \cdot 10^3 + 2 \cdot 10^2 + 7 \cdot 10 + 9 \equiv ? \pmod 7$.