CS60065: Cryptography and Network Security Total: 70 *points*

Assignment 1

Instructor: *Monosij Maitra* Due: *Aug 12, 2024*

Note: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

A. [Modular Arithmetic : $3 \times 3 = 9$ points.]

1. Show that $(5^{2n} + 7)$ is divisible by $8, \forall n \in \mathbb{N}$.[†]
2. Find the remainder when $6 \cdot 7^{32} + 7 \cdot 9^{45}$ is divided by 4.[†]
3. Prove that there exists infinitely many $n \in \mathbb{N}$ such that $4n^2 + 1$ is divisible by 65.

[†] Use modular arithmetic rules to solve these. Solutions obtained in other ways will fetch zero credits.

B. [GCD and Euclid's Algorithm : $5 + 2 + (3 \times 3) = 16$ points.]

Define $\mathsf{GCD}(\alpha, \beta)$ as the greatest common divisor of $\alpha, \beta \in \mathbb{Z}$.

1. Let $a = -85652$ and $b = 16261$. Compute $\mathsf{GCD}(a, b)$ demonstrably using the *Euclidean division algorithm*. Use the *Extended Euclidean algorithm* to demonstrably express $\mathsf{GCD}(a, b)$ (computed above) as an integer linear combination of a and b. Find an infinite set $S = \{(x, y) \in \mathbb{Z}^2 \mid ax+by = \mathsf{GCD}(a, b)\}$ of such integer linear combinations. Let $p \in \mathbb{P}$ be the smallest possible prime number greater than $\mathsf{GCD}(a, b)$. Demonstrate how to compute $(\mathsf{GCD}(a, b))^{-1} \pmod p$.
[1+1+2+1=5 points]
2. Define a function $\mathsf{gcd}^+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $\mathsf{gcd}(\cdot, \cdot)$ computes $\mathsf{GCD}(a, b)$ with $a, b \in \mathbb{N}$. Prove or disprove if $\mathsf{gcd}^+(\cdot, \cdot)$ is injective and/or surjective.
3. Let $a, b \in \mathbb{Z}$ be such that $\mathsf{GCD}(a, b) = d \in \mathbb{N}$.
   (a) Prove that $\mathsf{GCD}(a^2, b^2) = d^2$.
   (b) Prove that $\mathsf{GCD}(a + b, a - b)$ is either 1 or 2, if $d = 1$.
   (c) Prove that $\mathsf{GCD}(3a + 2b, 2a + 5b)$ is either 1 or 11, if $d = 1$.

C. [Algebraic Structures : $3 \times 5 = 15$ points.]

1. Let $S \neq \emptyset$ be a finite set of cardinality $n \in \mathbb{N}$. A *binary operation* $\star$ on S is defined by a function $\star : S \times S \to S$. How many different binary operations can be defined on S? How many of these binary operations are commutative? Argue your answers formally.
2. Let $\mathcal{P}(X)$ denote the power set of a set X. Consider the operation Δ (symmetric difference) on $\mathcal{P}(X)$ defined as $A \Delta B = (A \setminus B) \cup (B \setminus A)$ for any $A, B \in \mathcal{P}(X)$. Prove formally that $(\mathcal{P}(X), \Delta)$ is a commutative group.
3. **[Euler's Theorem.]** Recall $\phi : \mathbb{N} \to \mathbb{N}$ denotes Euler's totient function. For any $m \in \mathbb{N}$, prove that for all $a \in \mathbb{Z}_m^*$, $a^{\phi(m)} \equiv 1 \pmod m$.

D. [Symmetric Key Encryption+Classical Ciphers : 30 points.]

1. In class, we discussed different adversarial attack models for encryption schemes. Explain them briefly with their significance and state the weakest and strongest ones among these. Which attack models among these require randomized encryption algorithms and why?
[5 points]

2. Recall the (mono-alphabetic) Substitution cipher discussed in class using a permutation as a key. The following ciphertext is computed under such an encryption scheme from an English text:

$c =$ `iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnbhcc hwwhbsqvqbre hwq vhlq`

Do a frequency analysis on c to find the underlying plaintext using the following frequency table.

Letter	Frequency	Letter	Frequency
a	0.0817	n	0.0675
b	0.0150	o	0.0751
c	0.0278	p	0.0193
d	0.0425	q	0.0010
e	0.1270	r	0.0599
f	0.0223	s	0.0633
g	0.0202	t	0.0906
h	0.0609	u	0.0276
i	0.0697	v	0.0098
j	0.0015	w	0.0236
k	0.0077	x	0.0015
l	0.0403	y	0.0197
m	0.0241	z	0.0007

[5 points]

3. Define $[n] = \{1, 2, 3, \ldots, n\}$ for $n \in \mathbb{N}$. Consider the permutation $\sigma : [6] \to [6]$ defined as follows:

x	1	2	3	4	5	6
$\sigma(x)$	5	3	4	1	6	2

Find out the inverse permutation $\sigma(\cdot)^{-1}$. Next, consider the following plaintext m:

$m =$ `it is true that this proposition is not true`

Discard all white-space in the text above. Compute the 6×6 permutation matrices K_σ and its inverse $\mathsf{K}_{\sigma^{-1}}$ associated with $\sigma(\cdot)$ and $\sigma(\cdot)^{-1}$ respectively. Encrypt m as done in Hill cipher and output the ciphertext. Verify its correctness by decrypting the ciphertext back to m.

[2+4+2+2=10 points]

4. Recall $(\mathsf{GL}_t(\mathbb{Z}_p), \boxtimes)$ describes the group of all $t \times t$ invertible matrices w.r.t. matrix multiplication $\boxtimes$ over $\mathbb{Z}_p$ for some prime $p \in \mathbb{P}$. Compute the order of $\mathsf{GL}_t(\mathbb{Z}_p)$. Consider a Hill cipher with plaintext and ciphertext spaces as $(\mathbb{Z}_{26})^*$ and key space as $\mathsf{GL}_2(\mathbb{Z}_{26})$. Find the number of valid keys or matrices with an *even* determinant because one or both rows are even. (A row of any matrix is "even" if both entries in the row are even integers.) Generalize your answer when the plaintext and ciphertext spaces are $(\mathbb{Z}_p)^*$ and key space is $\mathsf{GL}_2(\mathbb{Z}_p)$ for any prime $p \in \mathbb{P}$.

[2+3+3+2=10 points]