Assignment1

Due: Sunday Feb 9, 11:59PM

- Answer the questions below, showing all relevant work and the methods used to obtain your results.
- Submit your answers on SLATE by the due date specified.
- Answers may only be submitted in Jupyter/Python notebook (.html) format, and/or PDF (.pdf) format.
- If you are submitting handwritten answers, scan them and submit them as a single PDF file (the college printers have a scan/email feature for this).
- This is an individual assignment. Assignments copied in whole or in part will receive a grade of ZER0.

Question1: (6 marks) **Decrypt**

An affine cipher, $f(M) = (aM + b) \mod p$, uses a block size of 10-digits and was used to encrypt a message. The ciphertext is:

06140752101027545539

The parameters of this cipher are:

- $p = 2625242353$
- $a = \phi(k)$ where k is the smallest integer such that $\phi(k) = \phi(k+1) = \phi(k+2)$
- b is the integer solution to: $3866629434 \equiv 12^b \mod 9876543211$

a) Explain a method to compute the key,$\{a, b\}$, and decrypt the ciphertext.

b) Implement your method using a Jupyter/Python notebook.

Question2: (6 marks) **RSA: full proof**

In class we proved that an RSA message block, M, can always be recovered by computing $C^d \mod n$ because of Euler's theorem which states that $M^{\phi(n)} \equiv 1 \mod n$, when $GCD(n, M) = 1$.

There are some (very rare!) cases when $GCD(n, M) \neq 1$ which must be proved to guarantee that any ciphertext, C, can be decrypted even when it came from a message block with $GCD(n, M) \neq 1$. To do this we compute $C^d \mod p$ and $C^d \mod q$ in order to obtain a pair of modular equations:

$$C^d \equiv x \mod p$$
$$C^d \equiv y \mod q$$

The Chinese Remainder Theorem states that the solution to these two equations is unique $\mod (n) = \mod (pq)$

a) Find the value of both x and y and simplify them as much as possible.

b) Determine the unique solution and prove that RSA works for all possible message blocks.

Question3: (6 marks) Choose one of the following (**A** or **B**):

A: Proving the EEA

Let the elements in the columns (R,S,T) of the EEA be:

R	S	T
r_0	s_0	t_0
r_1	s_1	t_1
$\vdots$	$\vdots$	$\vdots$
r_{i-1}	s_{i-1}	t_{i-1}
r_i	s_i	t_i
$\vdots$	$\vdots$	$\vdots$

Where $r_0 = N$, $r_1 = a$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$ and for $i \geq 2$:

$$r_i = r_{i-2} - q_i r_{i-1}$$
$$s_i = s_{i-2} - q_i s_{i-1}$$
$$t_i = t_{i-2} - q_i t_{i-1}$$

The quotient is $q_i = \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor$ (this is "R[-2] // R[-1]" in python...)

a) Show that if N and a are positive integers such that $a < N$, then $N = qa - r$ for some integers q and r, where $0 \leq r < a$.

b) Prove, using mathematical induction, that the remainder, r_i, in the ith row is equal to $N(s_i) + a(t_i)$ for every $i \geq 0$.

- Show the BASIS STEP (show that r_0 and r_1 are true...)
- Show the INDUCTIVE HYPOTHESIS (assume for some integer $i \geq 2$ that r_{i-1}=.... and r_{i-2}=... are true)
- Show the INDUCTIVE STEP.

c) Let t_k be in the last row. Prove that if $GCD(N, a) = 1$, then:

$$t_k \equiv a^{-1} \mod N$$

B: Proving Fermat's Little Theorem

Let p be a prime and $a \in \mathbb{Z}^+$ such that $a < p$.

a) Show that $C(p, r) \mod p = 0$ for $1 \leq r \leq (p-1)$.
   $C(n, r)$ is the binomial coefficient: $C(n, r) = nCr = \binom{n}{r}$

b) Show that $(k+1)^p \equiv k^p + 1^p \mod p$ using the Binomial Theorem.

c) Use the results from a) and b) to prove that $a^p \equiv a \mod p$ using mathematical induction.

   - Show the BASIS STEP (show that for $a = 1$...)
   - Show the INDUCTIVE HYPOTHESIS (assume that when $a = k$...)
   - Show the INDUCTIVE STEP.

d) Use the result from c) to prove Fermat's Little Theorem:

$$a^{p-1} \equiv 1 \mod p$$

Overall assignment organization and formatting: (2 marks)

- scans of handwritten solutions are clear/ordered and are submitted as a single PDF file.
- Jupyter/Python notebooks are organized and include comments to explain the code.