Math373 **Test 3** **Fri. Apr. 14, 2023**

Name: ____

Directions: Show all work. No credit for answers without work.

1. [**12 points**] Solve the following system of congruences.

$$3x \equiv 5 \pmod{7} \qquad x \equiv 6 \pmod{11} \qquad x \equiv 10 \pmod{23}$$

2. [**12 points**] Note that 73 is prime. Solve for x in $x^{49} \equiv 50 \pmod{73}$.

3. [**6 points**] True or False: Let $a, b, m_1, m_2 \in \mathbb{Z}$. If $m_1 \neq m_2$, then the system

$$x \equiv a \pmod{m_1} \qquad x \equiv b \pmod{m_2}$$

has a unique solution modulo M, where $M = m_1 m_2$. If True, then explain why, citing a theorem from class if appropriate. If False, then give a counter-example.

4. **[2 parts, 15 points each]** Bob generates an RSA key pair with $N = pq = 37 \cdot 131 = 4847$ and $e = 17$.

   (a) What is Bob's private key?

   (b) Alice wishes to encrypt and send Bob the message $m = 90$. What should he send?

5. [**6 points**] What is the main advantage of the Miller–Rabin primality test over the Fermat primality test? Be specific.

6. [**6 points**] Suppose we try to generate a roughly 1525-bit prime by selecting random numbers from the set $\{1, \dots, 2^{1525}\}$ until we happen to pick a prime number. On average, how many numbers will we need to pick before we find a prime?

7. [**6 points**] Alice claims to know the private key associated with public RSA key (N, e). To prove her claim, Alice offers to decrypt ciphertexts, so long as the corresponding plaintexts are random. So Bob may select a random $m_0 \in \mathbb{Z}_N$ and use Alice's public key to compute the corresponding ciphertext c_0, which he sends to Alice. Alice uses her private key to decrypt c_0 to recover m_0, and as long as m_0 looks random, she completes the challenge by sending m to Bob.

   Explain how Eve can exploit this system to decrypt a ciphertext c that she previously intercepted.

8. Samantha uses ElGamal digital signatures, and her private signing key is given by $(p, g, a) = (269, 18, 73)$. The following powers of g in $\mathbb{Z}_p$ may be helpful.

t	1	2	4	8	16	32	64	128	256
$g^t \pmod p$	18	55	66	52	14	196	218	180	120

(a) **[7 points]** What is Samantha's public verification key?

(b) **[15 points]** Samantha wishes to sign a document $D = 134$, and she picks random element $k = 37$. What is the signature D_{sig} corresponding to D?