Name:

Math 424: Exam 2

Make sure to show all your work as clearly as possible, except that you may omit brute force computations. Justify any answers that do not result from standard algorithms. Only 4-function calculators are allowed.

You may use any result from the chapters covered in the text or from lecture. You may not use the results of homework or in-class problems.

1. Short questions.

   (a) (10 pts) Compute $3^{494} \pmod{71}$.

   Solution: Clearly 71 is not divisible by $2, 3, 5$, or 7. As $\sqrt{71} < \sqrt{81} = 9$, we conclude that 71 is prime. By Fermat's Little Theorem, $3^{70} \equiv 1 \pmod{71}$. As $494 = 7 \cdot 70 + 4$, we get that $3^{494} \equiv (3^{70})^7 \cdot 3^4 \equiv 81 \pmod{71}$, so the answer is 10.

   (b) (10 pts) Compute $\varphi(187)$.

   Solution: We have $187 = 11 \cdot 17$, so

   $$\varphi(187) = 187 \cdot \left(1 - \frac{1}{11}\right) \cdot \left(1 - \frac{1}{17}\right) = 160.$$

   (c) (10 pts) Solve $x^2 \equiv 63 \pmod{67}$.

   Solution: Clearly 67 is not divisible by $2, 3, 5$, or 7, and all other primes exceed $\sqrt{67}$. Therefore 67 is prime. But also $67 \equiv 3 \mod 4$. One can therefore solve this problem by computing $\pm(63)^{(67+1)/4}$ and checking our answer.

   However, there is a shortcut: observe that $63 \equiv -4 \pmod{67}$. Since $67 \equiv 3 \pmod{4}$, either 4 or -4 is a square mod 67, but not both. As $4 \equiv 2^2 \pmod{67}$, we know that -4 cannot be a square mod 67. Therefore there are no solutions.

   (d) (10 pts) Let $n = 720259$; it is an RSA modulus. Consider the function that for $m \in \mathbb{Z}$ with $\gcd(m, n) = 1$ is given by $h(m) = m^2 \pmod{n}$. Show that h is *not* strongly collision resistant. Be completely explicit!

   Solution: For example, $h(1) = h(-1) = 1$.

2. (20 pts) Bob uses RSA with public key $(n, e) = (1219, 229)$. He receives a ciphertext $c = 4$. What was the original message?

   Solution: We first have to factor 1219. Brute force yields $1219 = 23 \cdot 53$. Thus $\varphi(1219) = 1144$. Now we want to find the inverse of 229 mod 1144. We can apply the Extended Euclidean algorithm, but in the first step we see that

   $$1144 - 4 \cdot 229 = 228$$

   so that $5 \cdot 229 - 1144 = 1$. Therefore $5 \cdot 229 \equiv 1 \pmod{1144}$, so the decryption exponent is 5.

   Lastly, we compute $4^5 \pmod{1219}$ which is 1024.

3. (15 pts) Give an example of a pair of integers $a, n \in \mathbb{N}$ such that

   - $n \geq 21$ and is odd,
   - $\gcd(a, n) = 1$,
   - the Jacobi symbol $(\frac{a}{n}) = +1$, and
   - $x^2 \equiv a \pmod{n}$ has no solutions.

   Justify that your answer works.

   Solution: There are many solutions. One solution is given by $n = 21$, $a = 20$. As $21 \equiv 1 \pmod 4$, we get
   $$\left(\frac{20}{21}\right) = \left(\frac{-1}{21}\right) = +1.$$
   But $3 \equiv 3 \pmod 4$, so -1 is not a perfect square mod 3. Therefore $x^2 \equiv -1 \equiv 20 \pmod{21}$ can have no solutions.

4. Bob has a 3-bit PRNG (output consists of 3 bits) whose first bit is always 0. Eve plays the CI game against Bob with the associated OTP cryptosystem.

   (a) (5 pts) Give an *explicit* description of an optimal strategy that Eve should follow.

   Solution: Eve picks $m_0 = 000$ and $m_1 = 100$; the last two bits are irrelevant, we just want the first bits to be different. Let c be the ciphertext in the CI game. If the first bit of c is t, then she guesses that c is the encryption of m_t.

   (b) (10 pts) Compute Eve's probability of winning the CI game with the above strategy.

   Solution: It is 100%. Let r be the output of the PRNG with input the secret key. Since the first bit of r is 0, the first bit of $r \oplus m_0$ is 0, and the first bit of $r \oplus m_1$ is 1. Thus the first bit of the ciphertext tells Eve which message was chosen.

5. (15 pts) The following Python function takes as input integers h, y with $h \geq 2$ and $\gcd(h, y) = 1$:

```python
def mat(h, y):
    i, m = 1, y
    while i < h-1:
        m = (m*y)%h
        i = i + 1
    if m != 1:
        return 1
    return 0
```

   What can you conclude on output 1, and same for output 0? Prove your answer.

   Solution: If the output is 1, then h is composite. If the output is 0, then we can conclude nothing. The reason is that the function outputs 0 if and only if $m^{h-1} \equiv 1 \pmod h$. Thus if h is prime, the output will always be 0 by Fermat's Little Theorem. The contrapositive of this statement is that if the output is 1, then h is composite.

   If h is composite, 0 is still a possible output though; for instance, if $y = 1$, then we will always get an output of 0.