MATH 173A, FINAL EXAM

2 August 2023

Name: ____________________________________

Student ID: ________________________________

Instructions: This 60 minute exam will be closed book, closed note, and proctored using Zoom proctoring (your webcam must be enabled). This exam must be hand-written on paper (not on a tablet). No checking cell phones during the exam. Do not type on the computer unless it is to ask the instructor a question through the Zoom chat. Your answers will be graded based on clarity as well as correctness; a correct answer will not receive full credit if the reasoning is difficult to follow. Good luck.

Question	Score	Maximum
0		1
1		6
2		6
3		4
4		3
5		10
6		5
7		5
Total		40

One point out of 40 on the final will be assigned for your pdf upload being organized and easy to read (for example, the question numbers should be clearly indicated and should be in consecutive order 1, 2, ...).

1. (6 points) Note that the different parts of this question use different numbers.

   a. Assume Bob's RSA modulus is $N = 35$. What numbers among $2, 3, 4, 5, 6, 7, 8, 9, 10$ may Bob choose as his encryption exponent? Explain your answer.

   b. What fast algorithm can Bob use to compute the secret decryption exponent d? Assume Bob's RSA modulus is $N = 55$ and his encryption exponent is $e = 17$. Compute Bob's secret decryption exponent d using that algorithm. Show your work. (Express your final answer d as a positive number.)

2. (6 points) Imagine Bob wants to generate a public RSA key $N = pq$ which is about 1000 bits, and he plans to find the primes p and q by testing randomly chosen numbers for primality.

   a. What is the *major flaw* with using the Fermat primality test for this purpose? (It should be a flaw which is not shared with the Miller-Rabin primality test.)

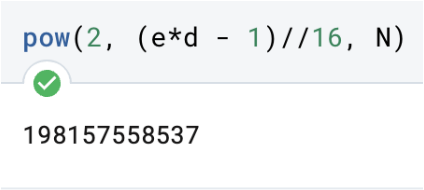
   b. Imagine there exists a public database of 10,000,000 primes of size suitable for RSA. One benefit of this database is that the numbers in it are guaranteed to be prime. What would be a disadvantage to using this database to select the primes? Explain in detail why using this database could be risky.

3. (4 points) Describe the main advantage of public key cryptography over private key cryptography.

4. (3 points) In the context of RSA, assume Bob has published an RSA key (N, e). Assume Bob agrees to make the following deal with Eve: Eve is allowed to choose three values x_1, x_2, x_3, and Bob will inform Eve of the values $x_1^e \bmod N$, $x_2^e \bmod N$, and $x_3^e \bmod N$ (in order, so Eve knows which value corresponds to which base). Would this arrangement enable Eve to efficiently factor N? Explain your answer.

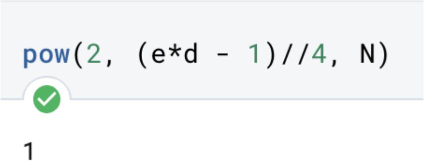
(Continued on the next page.)

5. (10 points) Assume $N = 563481825233$ is an RSA modulus and that e, d is an encryption-decryption pair relative to this modulus (as in Lab 5). Assume further that $ed - 1$ is divisible by 16, and that we make the following computations using Python.



```
pow(2, (e*d - 1)//16, N)
```

```
198157558537
```



```
pow(2, (e*d - 1)//4, N)
```

```
1
```

a. Assume `pow(2, (e*d - 1)//8, N)` is equal to 1. Can this information be used to factor N? Fully explain your answer. (This value of N is small enough that Python can factor it directly, without using e and d, but ignore that for this problem. You should not actually try to factor N.)

b. In the three computations above, does it make sense to replace the 2 appearing as the first `pow` argument with 3, so that `pow(2, ...)` becomes `pow(3, ...)`? Explain in about one sentence.

c. Assume $ed - 1$ is divisible by 5^4. In the three computations above, would it be useful to replace the denominators 16, 8, 4 with 5^4, 5^3, 5^2? Explain in about one sentence.

6. (5 points) Consider the following data, which relates to the Difference of Squares factorization method, with respect to $N = 46031$.

z	$z^2 \bmod 46031$
372	$3 \cdot 97$
480	$5 \cdot 7^2$
526	$2 \cdot 5 \cdot 7^2$
803	$3 \cdot 5^3$
885	$2 \cdot 349$
936	$11 \cdot 137$
984	$3 \cdot 5 \cdot 107$
1156	$3 \cdot 479$
1176	$2 \cdot 3 \cdot 11 \cdot 31$
1252	$2 \cdot 5^2 \cdot 7^2$

a. Find a non-trivial pair of numbers (A, B) with $A^2 \equiv B^2 \bmod 46031$. (For example, $(1, 46030)$ satisfies $1^2 \equiv 46030^2 \bmod 46031$, but it is a trivial pair.)

b. Using this pair, what GCD computation can now be performed in the hope that it yields a prime factor of 46031? (You do not need to make the GCD computations. If you didn't successfully find a pair in the previous part, just make up a pair to use for this part.)

(Continued on the next page.)

7. (5 points) Assume you learn that exactly one of the following numbers n is a Carmichael number and exactly one of the following numbers n is prime. Which is the Carmichael number? Justify your answer. (Using process of elimination is fine. Remembering which of these is a Carmichael number is not a valid justification.)

$n = 8321$

r	65	130	260	520	1040	2080	4160	8320	8321
$2^r \bmod n$	8192	8320	1	1	1	1	1	1	2
$3^r \bmod n$	2839	5193	7209	5036	7209	5036	7209	5036	6787
$4^r \bmod n$	8320	1	1	1	1	1	1	1	4
$5^r \bmod n$	6701	3285	7209	5036	7209	5036	7209	5036	217
$6^r \bmod n$	8214	3128	7209	5036	7209	5036	7209	5036	5253

$n = 14057$

r	1757	3514	7028	14056	14057
$2^r \bmod n$	926	14056	1	1	2
$3^r \bmod n$	692	926	14056	1	3
$4^r \bmod n$	14056	1	1	1	4
$5^r \bmod n$	5830	13131	14056	1	5
$6^r \bmod n$	8227	13131	14056	1	6

$n = 31621$

r	7905	15810	31620	31621
$2^r \bmod n$	31313	1	1	2
$3^r \bmod n$	31620	1	1	3
$4^r \bmod n$	1	1	1	4
$5^r \bmod n$	18745	2473	12876	1138
$6^r \bmod n$	308	1	1	6

$n = 41041$

r	2565	5130	10260	20520	41040	41041
$2^r \bmod n$	27994	27182	1	1	1	2
$3^r \bmod n$	24597	27028	24025	1	1	3
$4^r \bmod n$	27182	1	1	1	1	4
$5^r \bmod n$	38303	27182	1	1	1	5
$6^r \bmod n$	23561	155	24025	1	1	6