Exam 2 – Take home

Printed Name: Paul Beggs

Instructions: This is an individual, open-book, open-notes exam. You may not give help, receive help, or discuss this exam with anyone apart from me.

You may use a calculator or the computer to help with computations, just be sure to cite when you do so.

You may consult your textbook, your personal class notes, and your previous homework assignments while working on this exam. You may also consult anything posted on our Teams page. Only these resources are allowed.

You may NOT consult any other sources. No internet sources. No other textbooks. No notes or any other material from other students. No consulting with another student. No consulting with another professor.

As always, show work to get full credit (the correct answer may NOT be enough).
Write clearly! Double check your answers!

Honor Pledge: I have neither received nor given aid on this work, nor have I witnessed any such violation of the Honor Code.

Honor Pledge Signature:

Question	Points	Score
1	12	
2	12	
Total:	24	

1. Pirates hid a treasure somewhere on campus. They broke the location up into two pieces and encrypted them. An ElGamal Encryption scheme with the public key $p = 24691$, $g = 106$, and $A = 12375$ was used to encrypt the first part of a hidden message. Here is the resulting ciphertext: $c_1 = 3799$, $c_2 = 5973$. [12]

   (a) Use the Pohlig-Hellman algorithm to find the discrete logarithm problem to find the private key a such that $A = g^a \pmod{p}$.

   Solution. To use the Pohlig-Hellman algorithm, we need to find the order of the prime number $p = 24691$. Since it is prime, we calculate the order to be $\varphi(24691) = 24691 - 1 = 24690$. We can factor this number to $30 \cdot 823$. Let $x = a_0 + 30a_1$:

   $$(106^{a_0+30a_1})^{823} \equiv 12375^{823} \pmod{24691} \tag{1}$$
   $$(106^{823a_0+24690a_1}) \equiv 24143 \pmod{24691} \tag{2}$$
   $$(106^{823a_0} \cdot 106^{24690a_1}) \equiv 24143 \pmod{24691} \tag{3}$$
   $$(106^{823})^{a_0} \cdot (106^{24690})^{a_1} \equiv 24143 \pmod{24691} \tag{4}$$
   $$(1410)^{a_0} \equiv 24143 \pmod{24691}. \tag{5}$$

   For (1), we got the expression by substituting x for $a_0 + 30a_1$ for the exponent in $g^x \equiv \ldots$. From there, (2) — (4) is simple algebra. Then for (5), because 106^{a_1} is congruent to 1, $(106^{a_1})^{24690} = 1$. Additionally, we take $106^{823} \pmod{24691}$ to get 1410^{a_0}. Then, we do the same thing for the other side of the equation. Now, we can brute force this by setting $a_0 = \{0, 1, 2, 3, \ldots, 823\}$. We find that when $a_0 = 12$, $1410^{a_0} \equiv 24143 \pmod{24691}$. Seeing that we have a_0, we need to find b_0:

   $$(106^{b_0+823b_1})^{30} \equiv 12375^{30} \pmod{24691}$$
   $$15097^{b_0} \equiv 7229 \pmod{24691}.$$

   Thus, through brute force, we find that $b_0 = 171$. We can take our a_0 and b_0 to solve for x_1, x_2:

   $$x_1 = a_0 + 30a_1$$
   $$x_1 = 12 \pmod{30}$$

   and

   $$x_2 = b_0 + 823b_1$$
   $$x_2 = 171 \pmod{823}.$$

   At this point, we can solve the Chinese Remainder Theorem.

   1. Let $m = 30 \cdot 823 = 24690$.
   2. Compute $n_1 = \frac{24690}{30} = 823$ and $n_2 = \frac{24690}{823} = 30$.
   3. Compute $y_1 = 823^{-1} \pmod{30} \equiv 7$ and $y_2 = 30^{-1} \pmod{823} \equiv 631$.
   4. Compute $x = (12)(823)(7) + (171)(30)(631) \pmod{24690} \equiv 22392$.

   Therefore, $a = 22392$.

(b) Use the private key found in part (a) to decrypt the ciphertext (be sure to convert from ascii back to text).

Solution. to decrypt the message, we will compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. Substituting values, we get $(3799^{22392})^{-1} \cdot 5973 \pmod{24691} \equiv 7378$. Turning this from ascii into regular text, we get "`IN-`".

2. The pirates used an RSA Encryption scheme with public key $N = 57247159$ and $e = 11$ to encode the second part of the message. Here is the resulting cipher text: $c = 2772237$. [12]

(a) Use your knowledge of algorithms to factor N. Show all work.

Solution. If we use an method like factoring by difference of squares, we can set up a brute force algorithm to decrypt the factors of N. To compute this algorithmically, we will calculate values up to `i < limit` for which we add $N + i^2$. We square root this value, and take the integer value so we cut off the decimal. Then, we compare the squared value to the original. To do this in Python, we can look to the code below. From the algorithm we get $(p, q) = (421, 135979)$.

```
1   import math
2
3   def factor_using_diff(n, limit):
4       i = 1
5       while i < limit:
6           prod = n + i ** 2
7           sqrt_prod = int(math.sqrt(prod))
8
9           # Check if prod is a perfect square
10          if sqrt_prod ** 2 == prod:
11              factor1 = sqrt_prod - i
12              factor2 = sqrt_prod + i
13              return factor1, factor2  # Return the two factors
14          i += 1
15      return None  # If no factors are found within the limit
16
17  if __name__ == "__main__":
18      n = 57247159
19      limit = 100000
20      print(factor_using_diff(n, limit))
```

(b) Use the factors of N from part (b) to find the private decryption exponent d.

Solution. We can compute $d = e^{-1} \pmod{420 \cdot 135978} = 11^{-1} \pmod{57110760} \equiv 36343211$.

(c) Use the private key found in parts (a) and (b) to decrypt the ciphertext c and discover fully where the pirates hid their treasure.

Solution. To decrypt, we compute $m' = c^d \pmod{N} = 2772237^{36343211} \pmod{57247159} \equiv 667988$. Turning this from ascii into regular text, we get "`BOX`." Thus, from the first question, the full text is "`IN-BOX`."