Homework 4

Graded

Student

Kevin Vuong

View or edit group

Total Points

24 / 25 pts

Question 1

Question #1

5 / 5 pts

- ✔ **– 0 pts** Correct
- **– 0.5 pts** No python code

Question 2

Question #2

5 / 5 pts

- ✔ **– 0 pts** Correct
- **– 0.5 pts** #2 partially incorrect
- **– 1 pt** #2 incorrect
- **– 0.5 pts** No python code

Question 3

Question #3

4.5 / 5 pts

- **– 0 pts** Correct
- ✔ **– 0.5 pts** #3 incorrect

Used incorrect b

Question 4

Question #4

9.5 / 10 pts

- **– 0 pts** Correct
- ✔ **– 0.5 pts** #4b c2 incorrect
- **– 0.5 pts** #4c m' incorrect
- **– 0.5 pts** #4d partially incorrect
- **– 1 pt** No Python code

Questions assigned to the following page: 3, 1, and 2

Homework 4

Instructions: Solutions must be typed using LaTeX. All work should be uploaded to Gradescope by 11:59PM on Friday, February 16, 2024. If you use Python, include a link to your Google Colab file in your PDF and be sure that your permissions are updated to allow anyone with the link to run your code.

1. (5 pts) Use Pollard's $p-1$ Algorithm to factor $n = 220459$. Verify your answer in Python.

   1. Starting with $\gcd(2^{9!}-1, n)$...

$$
\begin{aligned}
2^{2!} - 1 &\equiv 3 (\text{mod } 220459) & \gcd(2^{2!}-1, 220459) &= 1 \\
2^{3!} - 1 &\equiv 63 (\text{mod } 220459) & \gcd(2^{3!}-1, 220459) &= 1 \\
2^{4!} - 1 &\equiv 22331 (\text{mod } 220459) & \gcd(2^{4!}-1, 220459) &= 1 \\
2^{5!} - 1 &\equiv 85053 (\text{mod } 220459) & \gcd(2^{5!}-1, 220459) &= 1 \\
2^{6!} - 1 &\equiv 4045 (\text{mod } 220459) & \gcd(2^{6!}-1, 220459) &= 1 \\
2^{7!} - 1 &\equiv 43102 (\text{mod } 220459) & \gcd(2^{7!}-1, 220459) &= 1 \\
2^{8!} - 1 &\equiv 179600 (\text{mod } 220459) & \gcd(2^{8!}-1, 220459) &= 449
\end{aligned}
$$

so

$$
\begin{aligned}
p &= 449 \\
\implies q &= 220459/449 = 491
\end{aligned}
$$

Thus, $220459 = 449 * 491$ We verify our answer HERE

2. (5 pts) Use Shanks' Baby Step, Giant Step Algorithm to solve $11^x = 21$ in $\mathbb{F}_{71}$. Verify your answer in Python. (Hint: $|11| = 70$. When verifying, you can either implement the Algorithm or use something like the discrete log Python example in class.)

See that $n = 1 + \lfloor\sqrt{70}\rfloor = 9$. Then, we create the lists

$$L_1 = 11^i (\text{mod } 71) \text{ for } i = 0, 1, 2, ..., 9$$

$$L_1 = \begin{bmatrix} 1 & 11 & 50 & 53 & 15 & 23 & 40 & 14 & 12 \end{bmatrix}$$

$$L_2 = 21 * 11^{-i9} (\text{mod } 71), \text{ for } i = 0, 1, 2, ..., 9$$

$$L_2 = \begin{bmatrix} 21 & 5 & 35 & 32 & 11 & 6 & 42 & 10 & 70 \end{bmatrix}$$

We have a match at position 1 in L_1 and at positon 4 in L_2 (Since we index from 0)

Then

$$
\begin{aligned}
11^1 &\equiv 21 * 11^{-9*4} (\text{mod } 71) \\
\implies 11^{37} &\equiv 21 (\text{mod } 71) \\
\implies x &= 37
\end{aligned}
$$

We verify this answer HERE

3. (5 pts) Alice and Bob agree on $p = 1373$ and $g = 2$ for a key exchange. Bob chooses exponent $b = 871$, and Alice computes $A \equiv 974 (\text{mod}\, p)$. What is the key that they obtain using Diffie-Hellman?

We know $A \equiv 974 (\text{mod } 1373)$. Then, going from bob's perspective, Secret S is:

$$
\begin{aligned}
&A^b (\text{mod } p) \\
&\equiv 974^{981} (\text{mod } 1373) \\
&= 214
\end{aligned}
$$

Thus, the secret key is 214.

Question assigned to the following page: 4

4. (10 pts) Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the ElGamal public key cryptosystem.
   (a) Alice chooses $a = 947$ as her private key. What is the value of her public key, A?
   (b) Bob chooses $b = 716$ as his private key, so his public key is
   $$B \equiv 2^{716} \equiv 469 (\mathrm{mod}\, 1373)$$
   Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?
   (c) Alice decides to choose a new private key $a = 299$ with associated public key $A \equiv 2^{299} \equiv 34 (\mathrm{mod}\, 1373)$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.
   (d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 (\mathrm{mod}\, 1373)$ and using the value of b to decrypt the message.

(a)
$$\begin{aligned} A &\equiv g^a (\text{mod } p) \\ \implies A &\equiv 2^9 47 (\text{mod } 1373) \\ \implies A &\equiv 177 (\text{mod } 1373) \end{aligned}$$

(b)
$$\begin{aligned} c_1 &\equiv g^k (\text{mod } p) \\ \implies c_1 &\equiv 2^{777} (\text{mod } 1373) \\ \implies c_1 &\equiv 719 \end{aligned}$$

$$\begin{aligned} c_2 &\equiv m B^k (\text{mod } p) \\ \implies c_2 &\equiv 583 * 469^{877} (\text{mod } 1373) \\ \implies c_2 &\equiv 623 (\text{mod } 1373) \end{aligned}$$

(c)

$$\begin{aligned} m' &\equiv (c_1^a)^{-1} * c_2 (\text{mod } p) \\ \implies m' &\equiv (c_1^2 99)^{-1} * 1325 (\text{mod } 1373) \\ \implies m' &= m = 332 \end{aligned}$$

Thus, the message is 332

(d) $g = 2, h = 893. N = 1372$ So $n = 1 + \lfloor \sqrt{N} \rfloor = 1 + 37 = 38$ We now create our 2 lists. They can be found HERE since they don't they fit onto the LateX page reasonably.

We find match for $2^i = 893 * 2^{-j38}$ When
$$i = 29, j = 5.$$

This is at the matching value 452.

Then
$$\begin{aligned} 2^2 9 &= 893 * 2^{-5*38} \\ \implies 2^{219} &= 893 (\text{mod } 1373) \\ \implies b &= 219 \end{aligned}$$

Now we can decrypt the message
$$\begin{aligned} m' &\equiv (c_1^b)^{-1} * c_2 (\text{mod } 1373) \\ \implies m' &\equiv (693^{219})^{-1} * 793 (\text{mod } 1373) \\ \implies m' &= 365 \end{aligned}$$

Thus, 365 is our message