1. $n_1 = 11$ $n_2 = 13$ $n_3 = 17$ $n_4 = 19$

$n = n_1 n_2 n_3 n_4 = 46189$

$N_1 = n_2 n_3 n_4 = 4199$

$N_2 = n_1 n_3 n_4 = 3553$.

$N_3 = n_1 n_2 n_4 = 2717$

$N_4 = n_1 n_2 n_3 = 2431$

$y_1 = 4199^{-1} \pmod{11} = 8^{-1} \pmod{11} = 7 \pmod{11}$ $(m = 5)$

$y_2 = 3553^{-1} \pmod{13} = 4^{-1} \pmod{13} = 10 \pmod{13}$ $(m = 3)$

$y_3 = 2717^{-1} \pmod{17} = 14^{-1} \pmod{17} = 11 \pmod{17}$ $(m = 9)$

$y_4 = 2431^{-1} \pmod{19} = 18^{-1} \bmod (19) = 18 \pmod{19}$ $(m = 17)$

$a \cdot a^{-1} = 1 \pmod n$

EEA: $a \cdot a^{-1} + ny = 1$

$a a^{-1} = 1 - ny.$ $(n \in \mathbb{Z})$

Discrete Mathematics: Homework 4

(Deadline: 8:00am, March 18, 2022)

$w_1 = y_1 N_1 \pmod n = 29393 \pmod n$

$w_2 = 35530 \pmod n$

$w_3 = 29987 \pmod n$

$w_4 = 43758 \pmod n$

$\Rightarrow x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod n$

$= [29393 a_1 + 35530 a_2 + 29987 a_3 + 43758 a_4]_{46189}$

1. (20 points) Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.

$$\begin{cases} x \equiv a_1 (\text{mod } 11); \\ x \equiv a_2 (\text{mod } 13); \\ x \equiv a_3 (\text{mod } 17); \\ x \equiv a_4 (\text{mod } 19). \end{cases}$$

2. (20 points) See the following figure. The RSA public keys of Alice, Bob and Charlie are $pk_1 = (N_1, 3), pk_2 = (N_2, 3)$ and $pk_3 = (N_3, 3)$, respectively. David wants to send a private message m to Alice, Bob and Charlie, where m is an integer and $0 < m < N_i$ for $i = 1, 2, 3$. In order to keep m secret from an eavesdropper Eve, David encrypts m as $c_1 = m^3 \bmod N_1$, $c_2 = m^3 \bmod N_2$ and $c_3 = m^3 \bmod N_3$; and then sends c_1 to Alice, c_2 to Bob and c_3 to Charlie.

2. $\begin{cases} c_1 = m^3 \bmod N_1 \\ c_2 = m^3 \bmod N_2 \\ c_3 = m^3 \bmod N_3 \end{cases}$

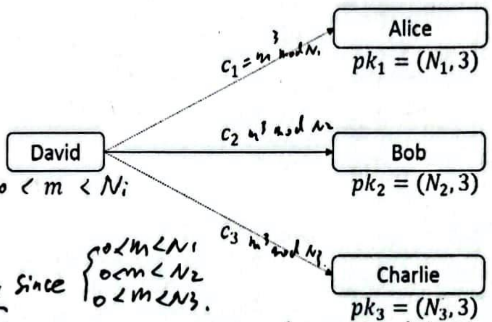
$\Rightarrow \begin{cases} m^3 = c_1 \pmod{N_1} \\ m^3 = c_2 \pmod{N_2} \\ m^3 = c_3 \pmod{N_3} \end{cases}$

$n = (N_1 N_2 N_3)$.

CRT:

$m^3 = b = c_1 N_2 N_3 \cdot [[N_2 \cdot N_3]^{-1} \bmod N_1]$
$+ c_2 N_1 N_3 \cdot [[N_1 \cdot N_3]^{-1} \bmod N_2]$
$+ c_3 N_1 N_2 \cdot [[N_1 \cdot N_2]^{-1} \bmod N_3]$.

3.



$c_1 = m^3 \bmod N_1$

c_2 $m^3 \bmod N_2$

c_3 $m^3 \bmod N_3$

$0 < m < N_i$

$m^3 = b$ exists and can be solved uniquely since $\begin{cases} 0 < m < N_1 \\ 0 < m < N_2 \\ 0 < m < N_3. \end{cases}$

$m^3 \equiv b \pmod{N_1 N_2 N_3}$ $\rightarrow$ when $0 < m^3 < N_1 N_2 N_3$. m exist and unique. it's the solution.

Suppose that N_1, N_2, N_3 are pairwise relatively prime. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.

3. (20 points) Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

4. (20 points) Let $(G, \cdot)$ be a multiplicative (Abelian) group of order m. Show that $o(a) | m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

5. (20 points) Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where

$a^q = 1 \pmod{}$

p=179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227998859,

$q = (p - 1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where

A=1129835751630026189475896666667354281816845178451448750969029100664347239526230
166033932125012141273999088232234924787259712660427548927981777812675128216074705
452830594726890347313130276198642286884664382583275520454375902037906355067286037
74799021127049872571983254506993921153718739796769296097404717448108;

B=1117727678052102394963651916915168810433949881962970620138536466745747434010427
364473288861564296291926916015263983660880127367494546266862814675792056750844619
894945132946240660741372479130373300404872753469132533457334297677819009771026871
85378411660147190296412313303321533586102552123457499563789255321369.

In particular, $\log_g A, \log_g B \le 10^4$. Find the output of Alice and Bob.

3. $x * y = xy - x - y + 2$

closure: $\forall a, b \in G$ $a>1$, $b>1$

$a * b = ab - a - b + 2 = a(b-1) - (b-1) + 1$

$= (a-1)(b-1) + 1 > 1$

$\Rightarrow a * b \in G$

Associative: $\forall a, b \in G$

$a * (b * c) = a * (bc - b - c + 2) = a(bc - b - c + 2) - a - (bc - b - c + 2) + 2$

$= (ab - a - b + 2) \cdot c - (ab - a - b + 2) - c + 2$

$= (a * b) * c$.

Identity:

$\exists e = 2 \in G$. $\forall a \in G$.

$a * 2 = 2a - a - 2 + 2 = a$

$2 * a = 2a - 2 - a + 2 = a = a * 2$.

Inverse: $\forall a \in G$, $\exists b = \frac{a}{a-1} > 1$, $b \in G$.

$a * b = \frac{a^2}{a-1} - a - \frac{a}{a-1} + 2 = 2$

$b * a = \frac{a^2}{a-1} - \frac{a}{a-1} - a + 2 = 2 = a * b \in G$.

Commutative:

$\forall a, b \in G$

$a * b = ab - a - b + 2$

$b * a = ba - b - a + 2 = ab - a - b + 2 = a * b$.

$\Rightarrow (G, *)$ Abelian Group.

4. $(G, \cdot)$ is a multiplicative Abelian group of order m.
Apply Euler's theorem: $a^m = 1$

For any $a \in G$, $a^m = 1$

$\forall a \in G$ $a^{o(a)} = 1$

Use division algorithm.

$\exists q, r \in \mathbb{Z}$: $m = q \cdot o(a) + r$. $0 \le r < o(a)$.

$a^m = a^{q \cdot o(a) + r} = (a^{o(a)})^q \cdot a^r = a^r = a^r = 1$ $(a^m = 1)$.

1^q

$\Rightarrow a^r = 1$, $0 \le r < o(a)$

$o(a)$ is the least integer value $a^{o(a)} = 1$.

$\Rightarrow r = 0$.

$\Rightarrow m = q \cdot o(a)$

$o(a) \mid m$. for any $a \in G$.

5.

```python
def Diffie_Hellman():
    A = 112983575163002618947589666667
    B = 111772767805210239496365191691
    p = 179769313486231590772930519078
    q = (p-1)/2
    a = 1
    b = 1
    while True:
        if (3**a)%p == A: break
        else: a+=1
    while True:
        if (3**b)%p == B: break
        else: b+=1
    print("Alice:", A**b%p)
    print("Bob:", B**a%p)
Diffie_Hellman()
```

```
>>> Diffie_Hellman()
Alice: 1082811278345346238104170780205614986659639207224390394098745967277926067531952266309908038877090398254625052499242035020002
076243274206123001706208026653029057500457776843481258274843650075907186383731879368899673093247226552949922258154109141050722107 2
504595310501935245754077299550897831569910724739835012 8
Bob: 1082811278345346238104170780205614986659639207224390394098745967277926067531952266309908038877090398254625052499242035020020 7
6243274206123001706208026653029057500457776843481258274843650075907186383731879368899673093247226552949922258154109141050722107250
4595310501935245754077299550897831569910724739835012 8
```