Problem 1 (5 pts x 2) Answer:
(a) First, note that $c_2$ is an integer, since $c_1b_1 \equiv 1 \mod b_2$. Now,
\[
\begin{align*}
x_1 &\equiv y_1^{c_1}(y_2^{c_2})^{-1} \mod n \\
&\equiv y_1^{c_1} \left(x^{b_1-1} \mod b_2\right)^{b_2} \mod n \\
&\equiv y_1^{c_1} \left(x^{c_1b_1-1}\right)^{-1} \mod n \\
&\equiv x^{b_1} (x^{c_1b_1})^{-1} \mod n \\
&\equiv x \mod n
\end{align*}
\]
(b) Given $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$, $y_2 = 14702$, we have
\[
c_1 = b_1^{-1} \mod b_2 = 2692 \\
c_2 = (c_1b_1 - 1)/b_2 = 15 \\
(y_2^{c_2})^{-1} \mod n = 5668
\]
Thus, the plaintext is $x = 15001$.

Problem 2 (5 pts x 3) Answer:
(a) First of all, $\gcd(x,pq) = 1$ implies that $\gcd(x,p) = 1$ and $\gcd(x,q) = 1$. Given that $p$ and $q$ are both odd primes, we have 2 as the common factor of $p-1$ and $q-1$. Thus, we get $\phi(n) = (p-1)(q-1) = 2u_1(p-1) = 2u_2(q-1)$, where $u_1 = \frac{q-1}{2} \in \mathbb{Z}^+$ and $u_2 = \frac{p-1}{2} \in \mathbb{Z}^+$ (both $u_1, u_2$ are positive integers).

By Euler’s Theorem, therefore, we have
\[
x^{\frac{1}{2}\phi(n)} \equiv x^{\frac{1}{2}2u_1(p-1)} \mod p \equiv x^{u_1(p-1)} \mod p \equiv 1 \mod p \\
x^{\frac{1}{2}\phi(n)} \equiv x^{\frac{1}{2}2u_2(q-1)} \mod q \equiv x^{u_2(q-1)} \mod q \equiv 1 \mod q.
\]
(b) By Lemma 1 following the Chinese Remainder Theorem, we have
\[
X \equiv m \mod p \tag{1} \\
X \equiv m \mod q \tag{2}
\]
implies $X \equiv m \mod pq$. Substituting $X = x^{\frac{1}{2}\phi(n)}$ and $m = 1$ gives the desired result.

(c) If $ed \equiv 1 \mod \frac{1}{2}\phi(n)$, we have $ed = 1 + r\frac{1}{2}\phi(n)$ for some integer $r$. and hence
\[
x^{ed} = x^{1+r\frac{1}{2}\phi(n)} = x \cdot (x^{\frac{1}{2}\phi(n)})^r \equiv x \cdot 1^r \equiv x \mod n,
\]
completing the proof.
Problem 3 (10 pts)  Answer:

Problem 4 (10 pts)  Answer: The given problem is the modification of the Diffie-Hellman key exchange problem, in which two communicating parties, Alice and Bob, agree upon a shared secret key, $K_{AB}$, by doing the following:

- Choose a large prime $p$ and its corresponding primitive root, $\alpha$,
- Alice chooses secret integer $a$ and computes a message $\beta_a = \alpha^a \pmod{p}$,
- Similarly, Bob chooses secret integer $b$ and computes a message $\beta_b = \alpha^b \pmod{p}$
- Alice and Bob exchange message $\beta_a$ and $\beta_b$, and
Upon receiving the corresponding message, both parties can compute the shared secret key as $\beta^b = \beta^a$, using the secret integer available to them.

When four parties are communicating, messages used to establish the shared secret key $K_{beta}$, are exchanged between the communicating parties in three iterations. In each iteration, the communicating parties are getting a step closer to establishing a shared secret key, $K_{beta}$, by obtaining the component $\alpha$ needed so that in the last step each person can raise the received $\alpha$ to the secret component that they posses in order to get the whole key. The modified protocol proceeds as follows:

- Bob, Ted, Carol and Alice choose a large prime $p$ and its corresponding primitive root, $\alpha$.
- Bob chooses a secret number $b$, Ted a secret number $t$, Carol a secret number $c$, and Alice a secret number $a$.

The First Iteration:
- Bob sends message $\alpha^b \mod p$ to Ted.
- Ted sends message $\alpha^t \mod p$ to Carol.
- Carol sends message $\alpha^c \mod p$ to Alice.
- Alice sends message $\alpha^a \mod p$ to Bob.

The Second Iteration:
- Bob sends message $\alpha^{bt} \mod p$ to Ted.
- Ted sends message $\alpha^{tb} \mod p$ to Carol.
- Carol sends message $\alpha^{ct} \mod p$ to Alice.
- Alice sends message $\alpha^{ac} \mod p$ to Bob.

The Third Iteration:
- Bob sends message $\alpha^{bac} \mod p$ to Ted.
- Ted sends message $\alpha^{bta} \mod p$ to Carol.
- Carol sends message $\alpha^{ctb} \mod p$ to Alice.
- Alice sends message $\alpha^{act} \mod p$ to Bob.

After the third iteration of message, each person obtains the shared secret key by raising the last received message to their own secret number.

Problem 5 (5 pts x 2) Answer:

(a) The Preimage problem for $h$ is to find $x$ such that $h(x) = x^2 \mod n$. To solve this problem, we need $d \in \mathbb{Z}$ such that

$$(x^2)^d \equiv x \mod n \implies 2d \equiv 1 \mod \phi(n)$$

But, gcd($\phi(n),2$) $\neq 1$ as $\phi(n) = (p-1)(q-1)$ is the product of even integers. So, finding $x$ is computationally infeasible.
(b) The Collision problem for \( h \) is to find \( x \) and \( x' \neq x \) such that \( h(x) = h(x') \).

The function \( h(x) = x^2 \text{mod} \ n \) is not strongly collision-free because one can easily construct \( x' = -x \text{mod} \ n \) that gives \( h(x) = h(x') \).

Problem 6 (5 pts x 3) Answer:

(a)

Given an \((N,M)\)-hash function \( h: \mathcal{X} \rightarrow \mathcal{Y} \), with \(|\mathcal{X}| = N\), \(|\mathcal{Y}| = M\) and \( s_y = |h^{-1}(y)| = |\{x : h(x) = y\}|\), we want to find the probability of successfully solving Preimage Problem, i.e., we want to find the probability that, given \( y \in \mathcal{Y} \) and a randomly chosen set \( \mathcal{X}_0 \subset \mathcal{X} \), \(|\mathcal{X}_0| = q\), we successfully find \( x \in \mathcal{X}_0 \) such that \( h(x) = y \). We can therefore write:

\[
\epsilon = \mathbb{P}[\text{Algorithm 4.1. successfully finds } x, h(x) = y] = 1 - \mathbb{P}[\text{Algorithm 4.1. fails in finding } x, h(x) = y] = 1 - \mathbb{P}[\exists x \in \mathcal{X}_0, h(x) = y]
\]

Now, knowing that for every \( y \in \mathcal{Y} \) there exists a set \( \mathcal{X}_y \in \mathcal{X} \), such that \( \forall x \in \mathcal{X}_y, h(x) = y \) and that the cardinality of the set \( \mathcal{X}_y \) is equal to \( s_y \), we can rewrite equation (9) as:

\[
\epsilon = 1 - \mathbb{P}[\forall x \in \mathcal{X}_0, x \not\in \mathcal{X}_y] = 1 - \frac{\binom{N-s_y}{q}}{\binom{N}{q}} \quad (10)
\]

(b)

Under the assumption that every \( y \in \mathcal{Y} \), for which the Preimage Problem was solved, is chosen independently, we can calculate the average probability of success of the Algorithm 4.1. (over all \( y \in \mathcal{Y} \)) by summing the probabilities of success for every \( y \in \mathcal{Y} \) and dividing the result by the cardinality of the set \( \mathcal{Y} \). By defining \( N_1 = N - s_y \), we can write:

\[
\sum_{y \in \mathcal{Y}} \frac{\epsilon_y}{|\mathcal{Y}|} = \frac{\sum_{y \in \mathcal{Y}} \left(1 - \frac{\binom{N-s_y}{q}}{\binom{N}{q}}\right)}{\sum_{y \in \mathcal{Y}} 1} = \frac{M - \sum_{y \in \mathcal{Y}} \frac{\binom{N-s_y}{q}}{\binom{N}{q}}}{M} = 1 - \frac{1}{M} \sum_{y \in \mathcal{Y}} \frac{\binom{N-s_y}{q}}{\binom{N}{q}}
\]

(c)

In showing that for \( q = 1 \), the success probability in part (b) equals \( \frac{1}{M} \), we use the following two facts:

(a) \( \sum_{y \in \mathcal{Y}} 1 = M \)

(b) \( \sum_{y \in \mathcal{Y}} s_y = N \)

Now, for \( q = 1 \), we can write:

\[
1 - \frac{1}{M} \sum_{y \in \mathcal{Y}} \frac{\binom{N-s_y}{q}}{\binom{N}{q}} = 1 - \frac{1}{M} \sum_{y \in \mathcal{Y}} \frac{\binom{N-s_y}{1}}{\binom{N}{1}} = 1 - \frac{1}{M N_1} \sum_{y \in \mathcal{Y}} N - s_y = 1 - \frac{1}{M N} \sum_{y \in \mathcal{Y}} N + \frac{1}{M N} \sum_{y \in \mathcal{Y}} s_y = 1 - \frac{M N}{M N} + \frac{N}{M N} = \frac{1}{M}
\]
Let’s prove by contradiction that the hash function $h_2$ is collision resistant: let’s assume that there exist $x_1, x_2 \in \{0, 1\}^m$ such that $x_1 \neq x_2$, but $h_2(x_1) = h_2(x_2)$. Let’s further define $x_1$ and $x_2$ as:

$$x_1 = x_1' || x_1'' \text{ where } x_1', x_1'' \in \{0, 1\}^m$$

$$x_2 = x_2' || x_2'' \text{ where } x_2', x_2'' \in \{0, 1\}^m$$

Since $h_2(x_1) = h_2(x_2)$, we can write:

$$h_1[h_1(x_1') || h_1(x_1'')] = h_1[h_1(x_2') || h_1(x_2'')] \tag{24}$$

Using the fact that the hash function $h_1$ is collision resistant, i.e. there does not exist $x_i, x_j \in \{0, 1\}^m$ such that $x_i \neq x_j$, but $h_1(x_i) = h_1(x_j)$, equation (24) can be rewritten as:

$$h_1(x_1') || h_1(x_1'') = h_1(x_2') || h_1(x_2'') \tag{25}$$

Using the property of concatenation operation that two binary strings can be equal only if all concatenated parts are equal, we can rewrite equation (25) as:

$$h_1(x_1') = h_1(x_2')$$

$$h_1(x_1'') = h_1(x_2'') \tag{26}$$

Using again the fact that function $h_1$ is collision resistant, it follows that:

$$x_1' = x_2'$$

$$x_1'' = x_2'' \tag{27}$$

From equation (27), it finally follows that $x_1 = x_2$, which contradicts the initial assumption. Therefore, hash function $h_2$ is collision resistant.

Problem 8 (10 pts) Answer:
The first person can have birthday in any month (denoted as $m_1$) of a year, giving probability of $\frac{12}{12}$.
The second person can have birthday in any of the rest months except $m_1$, denoted as $m_2$, giving probability of $\frac{12-1}{12}$.
The third person can have birthday in any of the rest months except $m_1, m_2$, denoted as $m_3$, giving probability of $\frac{12-2}{12}$.
The fourth person can have birthday in any of the rest months except $m_1, m_2, m_3$, giving probability of $\frac{12-3}{12}$.

As a result, the probability that no two people have birthdays in the same month is giving by $p = \frac{12}{12} \cdot \frac{12-1}{12} \cdot \frac{12-2}{12} \cdot \frac{12-3}{12} = \frac{11 \cdot 10 \cdot 9}{12^4} = \frac{990}{1728} = \frac{55}{96} \approx 0.5729$.  

5