Homework 6

Collaborators:

Practice Questions

These are practice questions. They will **NOT** be graded. We have also provided the final answers. However, it is up to you to understand how or why the given solution is correct. You do not need to submit these on Gradescope. However, you may find it easier to just include them in the PDF. In that case, please do not mark these questions on Gradescope.

1. **RSA Assumption (0 points).** Consider RSA encryption scheme with parameters $N = 35 = 5 \times 7$.

   (a) (0 points) Compute $\varphi(N)$ and write down the set $\mathbb{Z}_N^*$.
   Solution.
   $\varphi(35) = 24$

   $\mathbb{Z}_{35}^* = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

   (b) (0 points) Use repeated squaring and complete the rows X, X^2, X^4 for all $X \in \mathbb{Z}_N^*$ as you have seen in the class (slides), that is, fill in the following table by adding as many columns as needed.
   Solution.

X	1	2	3	4	6	8	9	11	12	13	16	17
X^2	1	4	9	16	1	29	11	16	4	29	11	9
X^4	1	16	11	11	1	1	16	11	16	1	16	11

X	18	19	22	23	24	26	27	29	31	32	33	34
X^2	9	11	29	4	16	11	29	1	16	9	4	1
X^4	11	16	1	16	11	16	1	1	11	11	16	1

(c) (0 points) Find the row X^7 and show that X^7 is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_N^*$.
Solution.

X	1	2	3	4	6	8	9	11	12	13	16	17
X^2	1	4	9	16	1	29	11	16	4	29	11	9
X^4	1	16	11	11	1	1	16	11	16	1	16	11
X^7	1	23	17	4	6	22	9	11	33	27	16	3

X	18	19	22	23	24	26	27	29	31	32	33	34
X^2	9	11	29	4	16	11	29	1	16	9	4	1
X^4	11	16	1	16	11	16	1	1	11	11	16	1
X^7	32	19	8	2	24	26	13	29	31	18	12	34

We can see that every value of X shows up once and exactly once in the row for X^7.

2. (0 points) By hand, compute the three least significant (decimal) digits of $25114997^{9301403}$. Explain your logic.

   Solution.

   973

3. (0 points) Suppose $n = 76499 = 227 \cdot 337$, where 227 and 337 are primes. Let $e_1 = 6039$ and $e_2 = 9031$.

   (a) (0 points) Only one of the two exponents e_1, e_2 is a valid RSA encryption key, which one?

   Solution.

   Only e_2 is valid.

   (b) (0 points) For the valid encryption key, compute the corresponding decryption key d.

   Solution.

   $d = 68503$

   (c) (0 points) Decrypt the cipher text $c = 33$.

   Solution.

   $m = 62638$

4. **Properties of Euler Phi Function** (0 points) Let $N = p_1^{e_1} \cdot p_2^{e_2} \cdots p_t^{e_t}$ represent the unique prime factorization of a natural number N, where $p_1 < p_2 < \cdots < p_t$ are prime numbers and $e_1, e_2, \ldots, e_t$ are natural numbers. Let $\mathbb{Z}_N^* = \left\{x \colon 0 \leqslant x < N, \gcd(x, N) = 1\right\}$ and $\varphi(N) = \left|\mathbb{Z}_N^*\right|$.

   (a) (0 points) Using the inclusion-exclusion principle, prove that

$$\varphi(N) = N \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

Solution.

The inclusion-exclusion principle states that for finite sets $A_1, \cdots, A_n$ one has the identity

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n| \\ &= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right)\end{aligned}$$

Let $I_N = \{1, 2, \cdots, N\}$. For every $i \in \{1, 2, \cdots, t\}$, let A_i be the set of elements of I_N that are divisible by the prime p_i. Since $\mathbb{Z}_N^* = \left\{x \colon 0 \leqslant x < N, \gcd(x, N) = 1\right\}$ and $\varphi(N) = \left|\mathbb{Z}_N^*\right|$, we have

$$\varphi(N) = N - |A_1 \cup \cdots \cup A_t|$$

and by the inclusion-exclusion principle

$$|A_1 \cup \cdots \cup A_t| = \sum_{i=1}^{t} |A_i| - \sum_{1 \leqslant i_1 < i_2 \leqslant t} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{t-1} |A_1 \cap \cdots \cap A_t|$$

An element in the intersection $k \in A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j} \subset I_N$ is divisible by $p_{i_1}, p_{i_2}, \cdots, p_{i_j}$. Then, there are $\left|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}\right| = \frac{N}{p_{i_1} \cdot p_{i_2} \cdots p_{i_j}}$ such elements.

Thus,

$$\sum_{i=1}^{t} |A_i| = N \cdot \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_t}\right)$$

$$\sum_{1 \leqslant i_1 < i_2 \leqslant t} |A_{i_1} \cap A_{i_2}| = N \cdot \left(\frac{1}{p_1 \cdot p_2} + \frac{1}{p_1 \cdot p_3} + \cdots + \frac{1}{p_{t-1} \cdot p_t}\right).$$

Therefore,

$$\begin{aligned}\varphi(N) =& N - |A_1 \cup \cdots \cup A_t| \\ =& N \cdot (1 - (\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_t}) + \cdots + (-1)^t \frac{1}{p_1 \cdot p_2 \cdots p_t}) \\ =& N \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right)\end{aligned}$$

(b) (0 points) For any $x \in \mathbb{Z}_N^*$, prove that

$$x^{\varphi(N)} = 1 \mod N.$$

Hint: Consider the subgroup generated by x and its order.

Solution.

Let k be the order of x, so $x^k = 1 \mod N$ and k is the size of the subgroup generated by x. By Lagrange's theorem, k divides $\varphi(N)$, the size of the group $\mathbb{Z}_N^*$. Then, $\varphi(N) = m \cdot k$ for some integer m, and

$$x^{\varphi(N)} = (x^k)^m = 1 \mod N$$

5. **Properties of x^e when e is relatively prime to $\varphi(N)$** (0 points)

In this problem, we will partially prove a result from the class that was left unproven. Suppose $N = pq$, where p and q are distinct prime numbers. Let e be a natural number that is relatively prime to $\varphi(N) = (p-1)(q-1)$. In the lectures, we claimed (without proof) that the function $x^e \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ is a bijection. The following problem is key to proving this result.

Let $N = pq$, where p and q are distinct prime numbers. Let e be a natural number relatively prime to $(p-1)(q-1)$. Consider $x, y \in \mathbb{Z}_N^*$. If $x^e = y^e \mod N$, then prove that $x = y$.

Hint: You might find the following facts useful.

- Every $\alpha \in \mathbb{Z}_N$ can be uniquely written as (α_p, α_q) such that $\alpha = \alpha_p \mod p$ and $\alpha = \alpha_q \mod q$, using the Chinese Remainder theorem. We will write this observation succinctly as $\alpha = (\alpha_p, \alpha_q) \mod (p, q)$.
- For $\alpha, \beta \in \mathbb{Z}_N$, and $e \in \mathbb{N}$ we have $\alpha^e = \beta \mod N$ if and only if $\alpha_p^e = \beta_p \mod p$ and $\alpha_q^e = \beta_q \mod q$. We will write this succinctly as $\alpha^e = (\alpha_p^e, \alpha_q^e) \mod (p, q)$.
- From the Extended GCD algorithm, if u and v are relatively prime then, there exist integers $a, b \in \mathbb{Z}$ such that $au + bv = 1$.
- Fermat's little theorem states that $x^{p-1} = 1 \mod p$ if x is a natural number that is relatively prime to the prime p.

Solution.

Assume $x^e = y^e \mod N$, then $x^e - y^e = 0 \mod N$ and there exists an integer k such that $x^e - y^e = k \cdot N = k \cdot pq$. Therefore, $x^e - y^e = 0 \mod p$ which implies that $x^e = y^e \mod p$. Since e is relatively prime with $p-1$, then by the extended GCD algorithm, there exist integers $c, d \in \mathbb{Z}$ such that $c \cdot (p-1) + d \cdot e = 1$, so $d \cdot e = 1 \mod (p-1)$. Adding a multiple of $p-1$ to d if necessary, we may assume $d \geqslant 1$; then $d \cdot e = 1 + j(p-1)$ for some integer $j \geqslant 0$. Since $x, y \in \mathbb{Z}_N^*$, neither is divisible by p, so Fermat's little theorem gives $x^{ed} = x \cdot \left(x^{p-1}\right)^j = x \mod p$, and likewise $y^{ed} = y \mod p$. Hence,

$$x^e = y^e \mod p \implies x^{ed} = y^{ed} \mod p \implies x = y \mod p.$$

Then, $x - y = k' \cdot p$ for some integer k'. Similarly, we can derive that $x - y = k'' \cdot q$ for some integer k''. Now, $x - y = k'p = k''q$ where p, q are distinct primes. This implies that $x - y = k''' \cdot pq$ for some integer k'''. Thus,

$$x - y = 0 \mod pq \implies x = y \mod N$$

where $N = pq$.

Homework Questions

These are homework questions and will be graded. Please make sure to clearly mark each problem on Gradescope.

1. **Answer the following questions (5+7+5 points):**

   (a) (5 points) Is the following RSA signature valid? (Justify your answer)

   $$(r\|m) = 42, \sigma = 188, N = 391, e = 7$$

   Here, m denotes the message, r denotes the randomness used to sign m, and σ denotes the signature. Moreover, $(r\|m)$ denotes the concatenation of r and m. The signature algorithm $\mathsf{Sign}(m)$ picks the randomness r and returns (r, σ), where $\sigma = (r\|m)^d \mod N$ and d is the inverse of e modulo $\varphi(N)$. The verification algorithm $\mathsf{Ver}(m, r, \sigma)$ returns $((r\|m) == \sigma^e \mod N)$. If the signature is not valid, compute the valid signature σ for the same $(r\|m)$.

   Solution.

(b) (7 points) Remember that in RSA encryption and signature schemes, $N = p \times q$ where p and q are two large primes. Show that in the RSA scheme (with public parameters N and e), if you know N and $\varphi(N)$, then you can efficiently factorize N, i.e., you can recover p and q.

Solution.

(c) (5 points) Consider an encryption scheme where $\mathsf{Enc}(m) := m^e \mod N$ where e is a positive integer relatively prime to $\varphi(N)$ and $\mathsf{Dec}(c) := c^d \mod N$ where d is the inverse of e modulo $\varphi(N)$. Show that in this encryption scheme, given only the public key (N, e) and the ciphertexts $c_1 = \mathsf{Enc}(m_1)$ and $c_2 = \mathsf{Enc}(m_2)$, but not m_1, m_2 or d, you can compute the encryption of $m_1^3 \cdot m_2^4 \mod N$.

Solution.

2. **Replacing $\varphi(N)$ with $\frac{\varphi(N)}{2}$ in RSA (15 points)**

   In RSA, we pick the exponent e and the decryption key d from the set $\mathbb{Z}^*_{\varphi(N)}$. This problem shall show that we can choose $e, d \in \mathbb{Z}^*_{\varphi(N)/2}$ instead. Let p, q be two distinct odd primes and define $N = pq$.

   (a) (2 points) For any $e \in \mathbb{Z}^*_{\varphi(N)/2}$, prove that $x^e \colon \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ is a bijection.
   Solution.

   (b) (7 points) Consider any $x \in \mathbb{Z}^*_N$. Prove that $x^{\frac{\varphi(N)}{2}} = 1 \mod p$ and $x^{\frac{\varphi(N)}{2}} = 1 \mod q$.
   Solution.

(c) (3 points) Consider any $x \in \mathbb{Z}_N^*$. Prove that $x^{\frac{\varphi(N)}{2}} = 1 \mod N$.
Solution.

(d) (3 points) Suppose $e, d \in \mathbb{Z}_{\varphi(N)/2}^*$ satisfy $e \cdot d = 1 \mod \frac{\varphi(N)}{2}$. Show that $(x^e)^d = x \mod N$, for any $x \in \mathbb{Z}_N^*$.
Solution.

3. **Shor's algorithm for factoring large integers** (20 points)

   Shor's algorithm is a quantum algorithm for factoring large integers. It shows that a quantum computer can factor large numbers in polynomial time, whereas the best-known classical algorithms are sub-exponential but not polynomial. In this problem, we will investigate how Shor's algorithm finds a non-trivial factor for any integer N.

   (a) **From factorization to order-finding.** (5 points)

   Consider an integer N and the group $\mathbb{Z}_N^*$. Pick a *random* element $a \in \mathbb{Z}_N^*$. The order of a is the smallest positive integer r such that $a^r = 1 \mod N$. Show that if r is even and $a^{r/2} \neq \pm 1 \mod N$, then

   $$\gcd(a^{r/2} - 1, N)$$

   gives a non-trivial factor of N.
   (Hint: Let $x = a^{r/2}$ and consider $x^2 = 1 \mod N$.)
   Solution.

(b) **The Continued Fraction algorithm.** (15 points)
Pick $Q > N^2$ to be a power of 2. Consider a quantum order-finding algorithm that returns an integer c such that $\left|\frac{c}{Q} - \frac{k}{r}\right| < \frac{1}{2Q}$, where r is the unknown order we want to recover and $k < r$ is an integer. We use a continued fraction to reconstruct the order r.
Consider $N = 91$ and $Q = 2^{14} = 16384 > N^2$. Suppose the quantum order-finding algorithm returns $c = 13653$. Answer the following.

i. (2 points) Continued Fraction Expansion.
For a real number x, its continued fraction expansion is written

$$x = [a_0; a_1, a_2, a_3, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}},$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{Z}_{\geqslant 1}$ for $i \geqslant 1$.
Write out the continued fraction expansion for $x = \frac{c}{Q}$ in both forms.
Solution.

ii. (5 points) The n-th convergent of continued fraction expansion of x is the rational number obtained by truncating after a_n:

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

The convergents form a sequence of rational approximations to x.
Write out the convergents $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_5}{q_5}$ of the continued fraction expansion of $x = \frac{c}{Q}$.
Solution.

iii. (5 points) Legendre's theorem states the following. Let $x \in \mathbb{R}$. If a reduced fraction p/q satisfies $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, then p/q is a convergent of the continued fraction expansion of x.
Apply Legendre's theorem to show that the unknown reduced fraction k/r must appear among the convergents of x.
Solution.

iv. (3 points) Pick $a = 3 \in \mathbb{Z}_{91}^*$. What is the order r? Once r is found, factor $N = 91$ by computing

$$\gcd\left(a^{r/2} - 1, N\right) \qquad \text{and} \qquad \gcd\left(a^{r/2} + 1, N\right).$$

Solution.

4. **Understanding hardness of the Discrete Logarithm Problem.** (15 points) Suppose G is a cyclic group of order N generated by $g \in G$. Suppose there is an algorithm $\mathcal{A}_{DL}$ that, when given input $X \in G$, outputs $x \in \{0, 1, \ldots, N-1\}$ such that $g^x = X$ with probability p_X.

   Think of it this way: The algorithm $\mathcal{A}_{DL}$ solves the discrete logarithm problem; however, for different inputs $X \in G$, its success probability p_X may be different.

   Let $p = \frac{1}{N} \sum_{X \in G} p_X$ represent the average success probability of $\mathcal{A}_{DL}$ solving the discrete logarithm problem when X is chosen uniformly at random from G.

   Using a single call to $\mathcal{A}_{DL}$, construct a new algorithm $\mathcal{B}$ that takes *any* $X \in G$ as input and outputs $x \in \{0, 1, \ldots, N-1\}$ such that $g^x = X$ with probability p. Briefly justify why your construction is correct.

   (*Remark:* Intuitively, this result shows that solving the discrete logarithm problem for *any* $X \in G$ is no harder than solving the discrete logarithm problem for a *random* $X \in G$.)

   Solution.

5. **Concatenating a random bit string before a message.** (15 points)

   Let $m \in \{0,1\}^a$ be an arbitrary message. Define the set

$$S_m = \left\{ (r \| m) \colon r \in \{0,1\}^b \right\}.$$

   Let p be an odd prime. Recall that in the RSA encryption algorithm, we encrypted a message y chosen uniformly at random from this set S_m.

   Prove the following

$$\Pr_{y \xleftarrow{\$} S_m} [p \text{ divides } y] \leqslant 2^{-b} \cdot \left\lceil 2^b / p \right\rceil.$$

   (*Remark:* This bound is tight as well. There exists m such that equality is achieved in the probability expression above. Intuitively, this result shows that the message y will be relatively prime to p with probability (roughly) $(1 - 1/p)$.)

   Solution.

6. **Challenging: Inverting exponentiation function.** (20 points)

   Fix $N = pq$, where p and q are distinct odd primes. Let e be a natural number such that $\gcd(e, \varphi(N)) = 1$. Suppose there is an adversary $\mathcal{A}$ running in time T such that

   $$\Pr\left[\mathcal{A}([x^e \mod N]) = x\right] = 0.01$$

   for x chosen uniformly at random from $\mathbb{Z}_N^*$. Intuitively, this algorithm successfully finds the e-th root with probability 0.01, for a random x.

   For any $\varepsilon \in (0, 1)$, construct an adversary $\mathcal{B}_\varepsilon$ (which, possibly, makes multiple calls to the adversary $\mathcal{A}$) such that

   $$\Pr\left[\mathcal{B}_\varepsilon([x^e \mod N]) = x\right] \geqslant 1 - \varepsilon,$$

   for *every* $x \in \mathbb{Z}_N^*$. The algorithm $\mathcal{B}_\varepsilon$ should have a running time polynomial in $T, \log N$, and $\log 1/\varepsilon$.

   Solution.