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) 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) 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) 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.

   $m = 62638$

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 (7+7+7 points):**

   (a) (7 points) Is the following RSA signature scheme valid? (Justify your answer)

   $$(r\|m) = 5, \sigma = 125, N = 187, e = 3$$

   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 $Sign(m)$ returns $(r\|m)^d \mod N$ where d is the inverse of e modulo $\varphi(N)$. The verification algorithm $Ver(m, \sigma)$ returns $((r\|m) == \sigma^e \mod N)$.

   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) (7 points) Consider an encryption scheme where $Enc(m) := m^e \mod N$ where e is a positive integer relatively prime to $\varphi(N)$ and $Dec(c) := c^d \mod N$ where d is the inverse of e modulo $\varphi(N)$. Show that in this encryption scheme, if you know the encryption of m_1 and the encryption of m_2, then you can find the encryption of $(m_1 \times m_2)^7$.

Solution.

2. **Euler Phi Function (30 points)**

   (a) (10 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 $e_1, e_2, \dots, e_t$ are natural numbers. Let $\mathbb{Z}_N^* = \left\{x \colon 0 \leqslant x < N-1, \gcd(x, N) = 1\right\}$ and $\varphi(N) = \left|\mathbb{Z}_N^*\right|$. Using the inclusion exclusion principle, prove that

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

   Solution.

(b) (5 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.

(c) **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 $N = pq$.

i. (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.

ii. (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.

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

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

3. **Understanding hardness of the Discrete Logarithm Problem.** (15 points) Suppose $(G, \circ)$ is a group of order N generated by $g \in G$. Suppose there is an algorithm $\mathcal{A}_{DL}$ that, when given input $X \in G$, it outputs $x \in \{0, 1, \dots, N-1\}$ 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 $p = \frac{\left(\sum_{X \in G} p_X\right)}{N}$ represent the average success probability of $\mathcal{A}_{DL}$ solving the discrete logarithm problem when X is chosen uniformly at random from G.

   Construct a new algorithm $\mathcal{B}$ that takes *any* $X \in G$ as input and outputs $x \in \{0, 1, \dots, N-1\}$ (by making one call to the algorithm $\mathcal{A}_{DL}$) such that $g^x = X$ with probability p. This new algorithm that you construct shall solve the discrete logarithm problem for *every* $X \in G$ with the same probability p.

   (*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.

4. **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.

5. **Properties of x^e when e is relatively prime to $\varphi(N)$** (20 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 exists 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.

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

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

   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.