

2. Answer the following questions (7+7+7+7 points):

- (a) (7 points) By hand, compute the three least significant (decimal) digits of $25114997^{9301403}$. Explain your logic.

Solution.

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

$$(r\|m) = 21, \sigma = 226, N = 339, e = 23$$

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

Solution.

- (c) (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.

- (d) (7 points) Consider an encryption scheme where $Enc(m) := m^e \bmod N$ where e is a positive integer relatively prime to $\varphi(N)$ and $Dec(c) := c^d \bmod N$ 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 $(m_1 \times m_2)^6$.

Solution.

(e) (7 points) Suppose $n = 76499 = 227 \cdot 337$, where 227 and 337 are primes. Let $e_1 = 6039$ and $e_2 = 9031$.

- i. (2 points) Only one of the two exponents e_1, e_2 is a valid RSA encryption key, which one?

Solution.

- ii. (3 points) For the valid encryption key, compute the corresponding decryption key d .

Solution.

- iii. (2 points) Decrypt the cipher text $c = 33$.

Solution.

3. 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 $\mathbb{Z}_N^* = \{x : 0 \leq x < N - 1, \gcd(x, N) = 1\}$ and $\varphi(N) = |\mathbb{Z}_N^*|$. 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.

(b) (5 points) For any $x \in \mathbb{Z}_N^*$, prove that

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

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 $x^e: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$ is a bijection.

Solution.

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

Solution.

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

Solution.

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

Solution.

4. **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 $p = \frac{(\sum_{X \in G} p_X)}{N}$ 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.

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

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

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

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

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

(*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. 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 $x^e: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$ 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 $x^e = y^e \pmod N$, 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 $\alpha = \alpha_p \pmod p$ and $\alpha = \alpha_q \pmod q$, using the Chinese Remainder theorem. We will write this observation succinctly as $\alpha = (\alpha_p, \alpha_q) \pmod{(p, q)}$.
- For $\alpha, \beta \in \mathbb{Z}_N$, and $e \in \mathbb{N}$ we have $\alpha^e = \beta \pmod N$ if and only if $\alpha_p^e = \beta_p \pmod p$ and $\alpha_q^e = \beta_q \pmod q$. We will write this succinctly as $\alpha^e = (\alpha_p^e, \alpha_q^e) \pmod{(p, q)}$.
- 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 $x^{p-1} = 1 \pmod p$ if x is a natural number that is relatively prime to the prime p .

Solution.

7. 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

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

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}_ε (which, possibly, makes multiple calls to the adversary \mathcal{A}) such that

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

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

Solution.

Collaborators :