Homework 6

1. **RSA Assumption (5+12+5).** Consider RSA encryption scheme with parameters $N = 35 = 5 \times 7$.

   (a) Find $\varphi(N)$ and $\mathbb{Z}_N^*$.
   Recall that for $N = p \cdot q$, we have $\varphi(N) = (p-1)(q-1)$, where p and q are prime numbers. Thus $\varphi(35) = (5-1)(7-1) = 24$.

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

   (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^5 and show that X^5 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^4	1	16	11	11	1	1	16	11	16	1	16	11
X^5	1	32	33	9	6	8	4	16	17	13	11	12

X	18	19	22	23	24	26	27	29	31	32	33	34
X^4	11	16	1	16	11	16	1	1	11	11	16	1
X^5	23	24	22	18	19	31	27	29	26	2	3	34

   It is clear from the table that X^5 is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_N^*$.

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

   (a) (7 points) Compute the three least significant (decimal) digits of $6251007^{1960404}$ by hand. Explain your logic.

   Solution.

$$6251007 \equiv 7 \pmod{1000}$$

Since $\gcd(7, 1000) = 1$, we have

$$7^{\varphi(1000)} \equiv 1 \pmod{1000}$$

where

$$\Phi(1000) = 5^3 \times 2^3 \times (1 - \frac{1}{5})(1 - \frac{1}{2}) = 400$$

$$1960404 \equiv 4 \pmod{400}$$

$$6251007^{1960404} \equiv 7^4 \pmod{1000} \equiv 2401 \pmod{1000} = 401$$

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

$$(r||m) = 24, \sigma = 196, N = 1165, e = 43$$

Here, m denotes the message, and 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.

$\sigma^e \equiv 196^{43} \pmod{1165}$. Since 1165 is divisible by 5, then if we had $196^{43} \equiv 24 \pmod{1165}$, then we should have had $196^{43} \equiv 24 \equiv 4 \pmod 5$. But $196 \equiv 1 \pmod 5$ and so $196^{43} \equiv 1^{43} = 1 \pmod 5$. So, this signature is not valid.

(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 a 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.

Suppose $N = pq$, then $\varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N - (p+q) + 1$, so $pq = N$ and $p + q = N - \varphi(N) + 1$. This means that we know both the multiplication and summation of p and q, so p and q are roots of equation $(x-p)(x-q) = x^2 - (p+q) + pq = x^2 - (N - \varphi(N) + 1)x + N$.

(d) (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 $(m_1 \times m_2)^5$.

Solution.

Suppose $m_1^e \equiv c_1 \pmod N, m_2^e \equiv c_2 \pmod N$, then $(m_1^5)^e \equiv c_1^5 \pmod N, (m_2^5)^e \equiv c_2^5 \pmod N, (m_1^5 m_2^5)^e \pmod N = c_1^5 c_2^5 = (c_1 c_2)^5 \pmod N$.

(e) (7 points) Suppose $n = 11413 = 101 \cdot 113$, where 101 and 113 are primes. Let $e_1 = 8765$ and $e_2 = 7653$.

i. (2 points) Only one of the two exponents e_1, e_2 is a valid RSA encryption key, which one?
Solution:
$\varphi(N) = 100 \cdot 112 = 11200$ which is divisible by $2, 5, 7$ and $e_1 = 8765$ is divisible by 5, then e_2 is valid and e_1 is not.

ii. (3 points) For the valid encryption key, compute the corresponding decryption key d.
Solution:
Using extended GCD algorithm and get $d = XGCD(11200, 7653) = 9517$.

iii. (2 points) Decrypt the cipher text $c = 3233$.
Solution:
Recall the Chinese Remainder theorem:

(Chinese Remainder Theorem) If $\gcd(p, q) = 1$, then

$$x = a \mod pq \iff \begin{cases} x = a \mod p \\ x = a \mod q \end{cases}$$

In this case, $11413 = 101 \cdot 113, p = 101$ and $q = 113$. Apply the Chinese remainder theorem,

$$m = 3233^{9517} \mod (101 \cdot 113) \iff \begin{cases} m = 3233^{9517} \mod 101 \\ m = 3233^{9517} \mod 113 \end{cases}$$

- $m = 3233^{9517} \mod 101$.
Note that $3233 = 1 \mod 101$.
From problem 3 (b), with a little work, we can show that if $\gcd(x, N) = 1$, (here $\gcd(1, 101) = 1$) then $x^{\varphi(N)} = 1 \mod N$ We have $\varphi(101) = 100$ and the exponent $9517 = 7 \mod 100$. The evaluation reduces to

$$\begin{aligned} m =& 3233^{9517} \mod 101 \\ =& (3233 \mod 101)^{9517 \mod \varphi(101)} \\ =& 1^7 \mod 101 \\ =& 1 \mod 101. \end{aligned}$$

- $m = 3233^{9517} \mod 113$.
Similarly, note that $3233 = 69 \mod 113, \varphi(113) = 112$, and $9517 = 109$

mod 112. The evaluation reduces to

$$\begin{aligned} m =& 3233^{9517} \mod 113 \\ =& (3233 \mod 113)^{9517 \mod \varphi(113)} \\ =& 69^{1}09 \mod 113 \\ =& 44 \mod 113. \end{aligned}$$

We start calculation from the larger prime 113. For $m = 44 \mod 113$, there exists integer k such that $m = 113 \cdot k + 44$. Then,

$$\begin{aligned} m =& 1 \mod 101 \\ 113 \cdot k + 44 =& 1 \mod 101 \\ 113 > 101 \implies (113 \mod 101) \cdot k + 44 =& 1 \mod 101 \\ 12 \cdot k + 44 =& 1 \mod 101 \\ \text{Using extended GCD} \implies k =& 89. \end{aligned}$$

Hence,

$$m = c^d = 3233^{9517} \mod 11413 = 113 \cdot 89 + 44 = 10101.$$

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 $e_1, e_2, \ldots, e_t$ 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.

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 a subset of I_N that are divisible by the prime p_i. Since $\mathbb{Z}_N^* = \left\{x \colon 0 \leqslant x < N-1, \gcd(x,N) = 1\right\}$ 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,

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

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

Therefore,

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

(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.

Solution.

The order of x divides the size of the group $\varphi(N)$. Then, there exists m such that $\varphi(N) = m \cdot k$ where $x^k = 1 \mod N$ and

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

(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:
$\varphi(N)/2$ and $\varphi(N)$ have the same prime factors. $\mathbb{Z}^*_{\varphi(N)/2}$ is a subgroup of $\mathbb{Z}^*_{\varphi(N)}$.
$x^e \colon \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ is a bijection for $e \in \mathbb{Z}^*_{\varphi(N)}$, then it is a bijection for $e \in \mathbb{Z}^*_{\varphi(N)/2}$ as well.

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:
$N = pq \implies \varphi(N) = (p-1)(q-1)$. As p, q are both odd, $(p-1), (q-1)$ are both even. By Fermat's Little theorem, $x^{p-1} = 1 \mod p$ and $x^{q-1} = 1 \mod q$. Hence,

$$x^{\frac{\varphi(N)}{2}} = (x^{p-1})^{(q-1)/2} = 1 \mod p$$

$$x^{\frac{\varphi(N)}{2}} = (x^{q-1})^{(p-1)/2} = 1 \mod q$$

iii. (3 points) Consider any $x \in \mathbb{Z}^*_N$. Prove that $x^{\frac{\varphi(N)}{2}} = 1 \mod N$.
Solution:
For $y = 1 \mod p$ and $y = 1 \mod q$, the Chinese Remainder Theorem says there exists a unique $y \in Z^*_N$ that satisfies the two equations. When $y = x^{\frac{\varphi(N)}{2}}$, the result follows directly from part (a).

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:
Since $e \cdot d = 1 \mod \frac{\varphi(N)}{2}$, then $e \cdot d = k \cdot \frac{\varphi(N)}{2} + 1$ for some integer k. Thus,

$$(x^e)^d = x^{k \cdot \frac{\varphi(N)}{2} + 1} = (x^{\frac{\varphi(N)}{2}})^k \cdot x = 1^k \cdot x \mod N = x \mod N$$

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 $x \in \{0, 1, \ldots, N-1\}$ 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 $p = \frac{(\sum_{X \in G} p_X)}{N}$ 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 $x \in \{0, 1, \ldots, N-1\}$ (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:

   The algorithm $\mathcal{B}$ has input $X \in G$ and outputs $x \in \{0, 1, \cdots, N-1\}$ where $N = |G|$ with probability $p = \frac{(\sum_{X \in G} p_X)}{N}$.

   1: Pick r uniformly at random from $\{0, 1, \cdots, N-1\}$
   2: Compute $\widetilde{x} = \mathcal{A}_{DL}(Xg^r)$
   3: **return** $\widetilde{x} - r$

   Correctness:

   Since g is a generator of G, then for $X \in G$, there exists $x \in \{0, 1, \cdots, N-1\}$ such that $g^x = X$ and $Xg^r = g^{r+x}$. $\mathcal{A}_{DL}$ solves the DL problem for Xg^r with probability p_{Xg^r} and returns $\widetilde{x} = x + r$. Therefore, $\widetilde{x} - r$ is our solution.

   Probability:

Note that $\Pr\left[\mathcal{A}_{DL}(X) = x\right] = p_X$.

$$\begin{aligned}
\Pr\left[\mathcal{B}(X) = x\right] &= \Pr_{r \leftarrow \{0,1,\cdots,N-1\}}\left[\mathcal{A}_{DL}(Xg^r) = r + x\right] \\
&= \sum_{\widetilde{r}=0}^{N-1} \Pr\left[\mathcal{A}_{DL}(Xg^{\widetilde{r}}) = \widetilde{r} + x, r = \widetilde{r}\right] \\
&= \sum_{\widetilde{r}=0}^{N-1} \Pr\left[\mathcal{A}_{DL}(Xg^{\widetilde{r}}) = \widetilde{r} + x\right] \cdot \Pr\left[r = \widetilde{r}\right] \\
&= \sum_{\widetilde{r}=0}^{N-1} p_{Xg^{\widetilde{r}}} \cdot \frac{1}{N} \qquad g \text{ is a generator of the group } G \\
&= \sum_{X \in G} p_X \cdot \frac{1}{N} = p
\end{aligned}$$

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 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:

For any message $m \in \{0,1\}^a$, we can rewrite S_m as shifting $r \in \{0,1\}^b$ a bits to the left and add $m \in \{0,1\}^a$:

$$S_m = \{2^m \cdot r + m : r \in \{0,1\}^b\}$$

Note that the size of S_m is $|S_m| = 2^b$ for fixed $m \in \{0,1\}^a$.

For message y chosen uniformly at random from S_m, there exists $r \in \{0,1\}^b$ such that $y = 2^a \cdot r + m \in S_m$. Then,

$$\begin{aligned}
p \text{ divides } y &\implies y = 0 \mod p \\
&\implies 2^a \cdot r + m = 0 \mod p \\
&\implies 2^a \cdot r = 0 \mod p, m = 0 \mod p \\
p \text{ is an odd prime} &\implies r = 0 \mod p, m = 0 \mod p
\end{aligned}$$

$$\begin{aligned}
\Pr_{y \xleftarrow{\$} S_m} [p \text{ divides } y] &= \Pr_{y \xleftarrow{\$} S_m} [p \text{ divides } r, p \text{ divides } m] \\
&= \Pr [p \text{ divides } r] \cdot \Pr [p \text{ divides } m] \\
&= \frac{\sum_{r \in \{0,1\}^b} \mathbf{1}_{\{p | r\}}(r)}{|S_m|} \cdot \Pr [p \text{ divides } m], \quad |S_m| = 2^b, \sum_{r \in \{0,1\}^b} \mathbf{1}_{\{p|r\}}(r) \leqslant \left\lceil 2^b / p \right\rceil \\
&\leqslant 2^{-b} \cdot \left\lceil 2^b / p \right\rceil
\end{aligned}$$

An alternative argument is as follows:

We can partition S_m to a sequence of subsets $\{M_k\}_k$ such that

$$\begin{aligned}
M_0 =& \{m + 0 \cdot 2^a, m + 1 \cdot 2^a, m + 2 \cdot 2^a, \cdots, m + (p-1) \cdot 2^a\} \\
M_1 =& \{m + p \cdot 2^a, m + (p+1) \cdot 2^a, m + (p+2) \cdot 2^a, \cdots, m + (2p-1) \cdot 2^a\} \\
& \vdots \\
M_k =& \{m + kp \cdot 2^a, m + (kp+1) \cdot 2^a, m + (kp+2) \cdot 2^a, \cdots, m + ((k+1)p-1) \cdot 2^a\}
\end{aligned}$$

Since m is divisible by p and $ip + j$ are not divisible by p for any i, j, then there are exactly one element in M_i that is divisible by p for any i and each M_i have size at most p. Thus, there are in total $\lceil \frac{2^b}{p} \rceil$ elements in S_m that are divisible by p.

6. **x^e if and only if 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 that is 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:

Assume $x^e = y^e \mod N$, then $x^e - y^e \mod N$ 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 exists integer $c, d \in \mathbb{Z}$ such that $c \cdot (p-1) + d \cdot e = 1$ which is equivalent as $d \cdot e = 1 \mod (p-1)$ for some $d \in \mathbb{Z}_{p-1}^*$. 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 $N = pq$.

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

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

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 running time polynomial in $T, \log N$, and $\log 1/\varepsilon$.

Solution:

First, we try to homogenize $\mathcal{A}$ using a similar approach as in Problem 4, and then we will try to boost the success probability by running the homogenized algorithm many times.

The algorithm $\mathcal{B}_\varepsilon$ has input $X \in \mathbb{Z}_N^*$, $N = pq$ and e such that $\gcd(e, \varphi(N)) = 1$ and outputs $x \in \mathbb{Z}_N^*$ which is the e-th root of X, i.e. $X^{1/e} = x$.

$k \leftarrow \frac{\log(1/\varepsilon)}{\log(1/0.99)}$
for $i = 1$ `to` k **do**
  Pick r uniformly at random from $\mathbb{Z}_N^*$
  Compute $\widetilde{x} = \mathcal{A}(X \cdot r^e \mod N)$
  if then$(r^{-1} \cdot \widetilde{x})^e = X \mod N$
    return $r^{-1} \cdot \widetilde{x}$
  end if
end for

Correctness:

If x is the e-th root of X, $X = x^e$, then

$$X \cdot r^e \mod N = x^e \cdot r^e \mod N = (xr)^e \mod N,$$

$(xr) \mod N$ is the e-th root of $X \cdot r^e \mod N$.

$$(X^{1/e} \cdot r)^e \mod N = (X \cdot r^e)^{1/e} \mod N$$

Probability:

Note that $\Pr\left[[\mathcal{A}([X \cdot r^e \mod N]) = xr]\right] = 0.01$. After running th inner loop k times, the probability that we never hit an easy instance (failure probability) is $(1-0.01)^k$. Therefore, the success probability is

$$\Pr\left[[\mathcal{B}_\varepsilon([X \mod N]) = x]\right] = 1 - (1-0.01)^k = 1 - \varepsilon.$$

Thus, $\varepsilon = (1-0.01)^k = 0.99^k$ and

$$k = \frac{\log(\varepsilon)}{\log(0.99)} = \frac{\log(1/\varepsilon)}{\log(1/0.99)}.$$

Complexity:

- The run time of $\mathcal{A}$ is T.
- The run time for the modular arithmetics (exponentiation, inverse, etc) is polynomial in terms of the length of the input which is $\log_2(N)$. Since $X \in \mathbb{Z}_N^*$, N can be represented using $\log_2(N)$ bits, then the length of X is at most $\log_2(N)$. The run time is $O((\log_2(N))^m)$.
- There are $k = O(\log(1/\varepsilon))$ iterations.

Together, the run time of the algorithm is

$$O(\log(1/\varepsilon) \cdot (T + (\log_2(N))^m))$$

which is polynomial in terms of $T, \log N$, and $\log 1/\varepsilon$.

Summary: Random Self-Reducibility

If the random instance had a non-trivial probability of being easy, ($\Pr_{x \leftarrow \mathbb{Z}_N^*}\left[[\mathcal{A}([x^e \mod N]) = x]\right] =$ 0.01), then we can solve any arbitrary instance by randomly transforming the arbitrary instance a number of times ($X \cdot r^e$). If we happen to hit an easy instance, $((r^{-1} \cdot \widetilde{x})^e = X \mod N)$, then we can solve the original problem.

Collaborators :