Homework 6

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

   (a) Compute $\varphi(N)$ and write down the set $\mathbb{Z}_N^*$.
   Solution.
   From question, $p, q = 5, 7$,
   $\varphi(N) = (p-1)(q-1)$
   $= 4 \times 6$
   $= 24$
   Then, $\mathbb{Z}_N^* = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$.

   (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

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

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

Solution.

Since we are only interested in the three least significant digits, we can apply mod 1000 to obtain it. Equivalently, this means that $N = 1000$.
Firstly, $6251007 \equiv 7 (mod\ 1000)$
Secondly, we note that $gcd(7, 1000) = 1$. Thus, this means that:

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

(since $x^{\varphi(N)} \equiv 1\ mod\ N$, $\forall x \in \mathbb{Z}_N^*$, and that $7 \in \mathbb{Z}_{1000}^*$)
Thirdly, we note that:

$$\varphi(1000) = 5^3 * 2^3 * (1 - \frac{1}{5}) * (1 - \frac{1}{2})$$

(From lecture, if exponents are present such that $N = p^3q^3$, $\varphi(N) = p^3q^3(1 - \frac{1}{p})(1 - \frac{1}{q})$)
$=$

$$400$$

Fourthly, taking into account the exponent,

$$1960404 \equiv 4\ (mod\ 400)$$

Lastly, this means that the three least significant digits are:

$$6251007^{1960404} \equiv 7^4\ (mod\ 1000)$$

$$\equiv 2401\ (mod\ 1000)$$

$$\equiv 401\ (mod\ 1000)$$

(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, 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.
The signature is not valid.
This is because $\sigma^e = 196^{43}$ $(mod\ 1165)$
$\equiv 24$ $(mod\ 1165)$ (Supposedly, assuming valid scheme).
Then, since $1165|5$, $196^{43} \equiv 24 \equiv 4$ $(mod\ 5)$.
However, the case here is that $196 \equiv 1$ $(mod\ 5)$. Thus, $196^{43} \equiv 1^{43}$ $(mod\ 5) \equiv 1$ $(mod\ 5)$.
Thus, the 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 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.
Since $N = pq,\ \varphi(N) = (p-1)(q-1)$
$= pq - p - q + 1$ (Algebraic manipulation)
$= N - (p+q) + 1$.
Hence, we can factorise N by solving the following, since we can obtain value of $(p+q) = N - \varphi(N) + 1$ and $pq = N$:

$$(x-p)(x-q) = x^2 + pq - (p+q)x$$

$$= x^2 + N - (N - \varphi(N) + 1)x$$

Thus, we can obtain p and q by solving for the roots of the above equation.

(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 we have $(m_1)^e \equiv c_1\ mod\ N$ and $(m_2)^e \equiv c_2\ mod\ N$, then we have $((m_1)^5)^e \equiv (c_1)^5\ mod\ N$, and $((m_2)^5)^e \equiv (c_2)^5\ mod\ N$.
Thus, we ultimately have:

$$(m_1^5 m_2^5)^e\ mod\ N = c_1^5 c_2^5\ mod\ N = (c_1 c_2)^5\ mod\ N$$

(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.
$\varphi(N) = (101 - 1)(113 - 1) = 11200$
$gcd(8765, 11200) = 5$, $gcd(7653, 11200) = 1$.
Thus, e_2 is a valid RSA encryption key and not e_1.

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

Solution.
Since decryption key is such that $e \cdot d \equiv 1 \; mod \; \varphi(N)$, we can run $XGCD(e, \varphi(N))$ to obtain d such that $e \cdot d \equiv 1 \; mod \; \varphi(N)$.
Hence, we can obtain $d = 9517$.

iii. (2 points) Decrypt the cipher text $c = 3233$.

Solution.
Since the following values are: $N = 101 \times 113 = 11413$, $e = 7653$, $d = 9517$, $c = 3233$, and we know that $m = c^d \; mod \; N$, we can obtain $m = 3233^{9517} \; mod \; 11413 = 10101 \; mod \; 11413$.

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.

Let A_i denote the subset of $\{1, 2, ..., n\}$ such that all of the elements in A_i are divisible by p_i. Then, the set A $:= \{m|1 \leqslant m \leqslant n, gcd(m, n) > 1\}$ is exactly equal to the union of all A_i.

Then, using the principle of inclusion-exclusion,

$$|A| = \sum_i |A_i| - \sum_{i<j} \left|A_i \cap A_j\right| + \sum_{i<j<k} \left|A_i \cap A_j \cap A_k\right| - ...$$

$\Leftrightarrow$

$$= \sum_i N/p_i - \sum_{i<j} N/p_i p_j + \sum_{i<j<k} N/p_i p_j p_k - ...$$

Thus, we have $\varphi(N)$:

$$\varphi(N) = N - |A| = N - \sum_i N/p_i - \sum_{i<j} N/p_i p_j + \sum_{i<j<k} N/p_i p_j p_k - ...$$

$\Leftrightarrow$

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

(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.

For an arbitrary value of $x \in \mathbb{Z}_N^*$, let the subgroup generated by x be denoted as: $< X > = \{x, x^2, x^3, ..., x^k = e\} \subseteq \mathbb{Z}_p^*$
$\Rightarrow k|\varphi(N)$ since order of subgroup divides order of group).
This means that $X^{\varphi(N)} = (X^k)^{\varphi(N)/k} = 1^{\varphi(N)/k} = 1$.
Thus, $x^{\varphi(N)} = 1 \ mod \ N$.

(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.

Since $gcd(e, \varphi(N)/2 = 1$, this means that for any $e \in \mathbb{Z}_{\varphi(N)/2}$, there exists an inverse d in $\mathbb{Z}_{\varphi(N)/2}$ such that $e \cdot d = 1 \ mod \ \varphi(N)/2$. Hence, $x^e \colon \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ is a bijection.

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.

Using result from Q3 part b, $x^{\varphi(N)} = 1 \ mod \ N$.

Then, since $N = pq$, $p|N$ and $q|N$, and that $gcd(x, N) = 1$.

This means that $gcd(x, p) = 1$ and $gcd(x, q) = 1$. Hence, $x^{\varphi(N)/2} = 1 \ mod \ p$ and $x^{\varphi(N)/2} = 1 \ mod \ q$.

iii. (3 points) Consider any $x \in \mathbb{Z}_N^*$. Prove that $x^{\frac{\varphi(N)}{2}} = 1 \mod N$.
Solution.
Using result from Q3 part b, $x^{\varphi(N)} = 1 \; mod \; N$.
Since $x \in \mathbb{Z}_N^*$, this means that $gcd(x, N) = 1$. Thus, $x^{\varphi(N)/2} = 1 \mod N$.

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 $e \cdot d = 1 \mod \frac{\varphi(N)}{2}$, this means that d is the modular inverse of e. Hence, $(x^e)^d = x \mod N$, for any $x \in \mathbb{Z}_N^*$.

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 $\mathcal{B}$ is as follows:
   Run the algorithm $\mathcal{A}_{DL}$). Then, if $g^x \neq X$, follow rejection sampling method.
   This means that we continue to run the algorithm $\mathcal{A}_{DL}$), until we obtain a satisfactory answer($g^x = X$).

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. **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.

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

Solution.

Collaborators :