Homework 6

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

   (a) Find $\varphi(N)$ and $\mathbb{Z}_N^*$.

   (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												
X^2												
X^4												

X												
X^2												
X^4												

(c) Find the row X^5 and show that X^5 is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_N^*$.
Solution.

X												
X^4												
X^5												

X												
X^4												
X^5												

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

   (a) Compute the three least significant (decimal) digits of $87341011^{324562002}$ by hand.
   Solution.

   (b) Is the following RSA signature scheme valid?(Justify your answer)
   $(r||m) = 342454323, \sigma = 13245345356, N = 155, e = 664$
   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.

(c) 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 find the factorization of N i.e. you can find p and q.

Solution.

(d) 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.

Collaborators :