Tutorial Questions

Cryptography and Network Security

Date: 13/10/2023

Q1. Using Fermat's theorem, find 3^{201} mod 11 = 1.

Q2. Find Euler's Totient for the following:

a) 10
b) 41

Q3. (Euler's Theorem) Given a = 3, n = 10. Find $a^{\phi(n)}$.

Q4. (CRT – Chinese Remainder Theorem) Given following congruences:

- $x \equiv 6 \pmod{11}$
- $x \equiv 13 \pmod{16}$
- $x \equiv 9 \pmod{21}$
- $x \equiv 19 \pmod{25}$

find the solution for x.

Q5. Suppose Bob chooses, p = 11 and q = 23. How Bob can choose the key (e,n) to execute RSA. Consider the keys:

- Public Key, PU = (3, 253)
- Private Key, PR = (147, 253)

Now use these to encrypt M = 57 and also verify the decryption.

Q6. Use Fermat's Theorem to find a number "a" between 0 and 72 with "a" congruent to 9^{794} modulo 73.

Q7. Use Fermat's Theorem to find a number "x" between 0 and 28 with x^{85} congruent to 6 modulo 29. (solve it without any sort of brute force searching)

Q8. Show for an arbitrary positive integer "a", $\phi(a)$ is given by:

$\phi(a) = \prod_{\{i = 0 \text{ to } t\}} \left[(P_i\text{^}(a_i - 1))(P_{i\,-}\ 1) \right]$, where $a = p_1^{a1}\, p_2^{a2} \ldots\ldots\, p_t^{at}$.

(Scribe prepared by Jitendra Kulaste)