ICS 505 Cryptography

Home Assignment 1

Dr. Muhammad Hataba, muhammad.hataba@giu-uni.de
TA. John Ehab, john.ehab@giu-uni.de

1. Find multiplicative inverse
   a) (11^{-1}) mod 17
   b) (1056^{-1}) mod 3

2. Modular Exponentiation
   a) (3 power 301) mod 5
   b) (7 power 105) mod 143

3. Use the Euclidean algorithm to compute gcd(30030, 257)

4. Find all solutions of $12x = 28 \pmod{233}$.

5. A gathering of individuals is organizing themselves for a festival march. When they attempt to arrange themselves in rows of three, one person is left unallocated. Similarly, when they attempt rows of four, two individuals are left over, and with rows of five, three individuals remain unassigned. What is the smallest feasible number of individuals present? And what follows as the next smallest number?
   (Hint: Interpret this problem in terms of the Chinese remainder theorem.)

6. In GF(2^8), find the multiplicative inverse of (x^5) modulo($x^8+x^4+x^3+x+1$).
   (Hint: use Extended Euclidean Algorithm)

7. Using AES encrypt this plaintext, only generate the first-round key and perform the first-round of encryption)
   Plaintext: 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 b7 34
   Key: 2b 7e 15 16 28 a2 d2 a6 ab f7 15 88 09 cf 4f 3c

8. Factor n = 35 by the elliptic curve method by using the elliptic curve $y^2 \equiv x^3 + 26$ and calculating 3 times the point P = (10, 9).

9. In the Diffie-Hellman key exchange protocol, Alice and Bob choose a primitive root α for a large prime p. Alice sends $x_1 \equiv \alpha^a \pmod p$ to Bob, and Bob sends $x_2 \equiv \alpha^b \pmod p$ to Alice. Suppose Eve bribes Bob to tell her the values of b and x_2. However, he neglects to tell her the value of α. Suppose gcd (b, p − 1) = 1. Show how Eve can determine α from the knowledge of p, x_2, and b.

10. **Coding Task** You want to represent the message 12345 as a point (x, y) on the curve y2 ≡ x3 + 7x + 11 (mod 593899). Write x = 12345 and find a valueof the missing last digit of x such that there is a point on the curve with this x-coordinate.

11. **Coding Task** Compute the difference (5, 9) − (1, 1) on the ellipticcurve $y^2 \equiv x^3 - 11x + 11 \pmod{593899}$. Note that the answer involves large integers, even though the original points have small coordinates

Submission Guidelines:

Please scan your handwritten solutions and submit them as a PDF. Additionally, upload your code to any publicly accessible link for grading. Thank you!

Submission Form: https://forms.office.com/r/BzffuM7NPJ

Submission Deadline: Thursday 24-Oct-2024 at 11:59 PM.