

1. Let $e = (1001\ 1111)$ be the exponent. Illustrate the addition chains produced by each one of the following algorithms. Compute the length of each addition chain.
 - (a) binary method
 - (b) m -ary method for $d = 2, 4$
 - (c) m -ary method for $d = 2, 4$ and with reduced preprocessing
 - (d) CLNW with $d = 2, 4$
 - (e) VLNW with $d = 4$ and $q = 2$
 - (f) Factor method
 - (g) Booth recoding for $d = 1, 2$
 - (h) Canonical recoding for $d = 1, 2$
2. Illustrate the steps of the standard multiplication algorithm for computing $c = a \cdot b = 215 \cdot 348$.
3. Illustrate the steps of the standard squaring algorithm for computing $c = a \cdot a = 215 \cdot 215$.
4. Illustrate the steps of the restoring division algorithm for computing $R = 243 \pmod{13}$.
5. Illustrate the steps of the nonrestoring division algorithm for computing $R = 243 \pmod{13}$.
6. Let $r = 32$, $n = 25$, $a = 13$, and $b = 15$. Compute $c = a \cdot b \cdot r^{-1} \pmod{n}$ using the standard Montgomery multiplication algorithm. Illustrate the steps and give all temporary results.
7. Repeat Question 6 using the binary CIOS Montgomery multiplication algorithm.
8. Let $n = 29$, $e = 23$, and $M = 10$. Compute $M^e \pmod{n}$ using the binary method of exponentiation and the Montgomery multiplication where $r = 32$. Show the steps of the binary method, and illustrate at least two Montgomery multiplications and one Montgomery squaring.
9. Let an RSA key be determined by the parameters $\{p, q, e, d\} = \{13, 17, 25, 169\}$. Compute $M^d \pmod{n}$ for $M = 30$ using the Chinese remainder theorem.
10. Let the elliptic curve equation $y^2 = x^3 + 2x + 1$ defined over the finite field $GF(17)$ be given. Compute and list all points over the curve. What is the order of the elliptic curve? Compute the point addition operation $(1, 15) + (3, 0)$ using the elliptic curve point addition rules.

¹Send the assignment by email (PDF) to koc@cs.ucsb.edu or deliver it to me in class.