

1. Consider the RSA exponent $e = 43 = (101011)_2$. Emulate the exponentiation algorithms to compute $c = m^e \pmod{n}$ for each one of the algorithms in table:
 - (a) Square-and-Multiply Algorithm
 - (b) Square-and-Multiply-Always Algorithm
 - (c) Montgomery Powering Ladder
 - (d) Atomic Square-and-Multiply Algorithm
 - (e) Right-to-Left Binary Algorithm (classical)
 - (f) Right-to-Left Binary Algorithm (atomic)

2. Consider the RSA key set $(p, q, n, \phi(n), e, d) = (43, 49, 2107, 2016, 709, 1453)$. Emulate (numerically) for computing $s = m^d \pmod{n}$ where $m = 25$ using each one of these DPA-type countermeasure algorithms by selecting suitable random parameters:
 - (a) Randomizing m , where e is known
 - (b) Randomizing m , where e is unknown
 - (c) Randomizing m , using a short r
 - (d) Randomizing d , using a short r
 - (e) Randomizing d , where $\phi(n)$ is unknown
 - (f) Randomizing d , where e is unknown
 - (g) Randomizing n , using short random r_1 and r_2

3. For each one of the pure DRNG designs given in Schindler's notes
pages 18, 24, 27 (DES), 27 (3DES), 27 (AES), 33, 34, 38, 42, 47
determine and justify whether the design satisfies R_1, R_2, R_3, R_4 .
See: <http://cs.ucsb.edu/~koc/cs290g/epf1/>

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