

# 1 Tutorial 6

1. Encrypting the message “singapore” using a mono alphabetic substitution cipher created using the keyword “secure” results in the ciphertext:  
(a) PFKBSMLOR (b) ODJASLKNR (c) RHMFSOQNB (d) QGLDSNMPA (e) None of the above
2. When the Miller-Rabin primality test fails for a number  $n$ ,  $n$  is definitely composite. But if it succeeds for  $n$ ,  $n$  is not necessarily a prime.  
(a) True (b) False (c) Can't really tell (d) None of the above.
3. Is  $\log n$   
(a)  $O(n)$  (b)  $O(n^2)$  (c)  $O(2^n)$  (d) all of the above (e) none of the above
4. Consider the equality  $(a + b)^p \equiv a^p + b^p \pmod{p}$ . Is it  
(a) True (b) False (c) Depends on  $a, b, p$  (d) None of the above.
5. For  $n = 101$ , will the table  $3 \times x \pmod{101}$  ( $0 \leq x < 101$ ) generate a permutation of  $(0 \dots 100)$ ?  
(a) True (b) False (c) Can't really tell without generating the whole table (d) Damn!
6. Approximately how many samples will one need to find a prime around 10000000000000000. That is, if one were to randomly generate numbers close to  $10^{16}$ , how many might you need to run the Miller-Rabin test on before you accept it as a probable prime.  
(a) 5000000000000000 (b) 37 (c) 19 (d) Can't really say.
7. What can be said about the DES initial permutation  $IP$ ?  
(a) DES would be substantially weakened without it (b) The strength of DES is equivalent to its strength without the IP (c) Without IP the keyspace to be searched to mount a known plaintext attack could be reduced substantially (d) It's hard to say anything definitive.
8. In DES, suppose that  $F(R, K) = 0$ , i.e., for any input the  $F$  function output 0. What function does DES compute?  
(a) Inverse (b) Identity (c) Some other permutation (d) None of the above.
9. In DES, how many bits in  $(L_1, R_1)$ , i.e., the 64 bits of the result of the first round, are related to bit 1 in  $(L_0, R_0)$ ? I.e., if the value of bit 1 in  $L_0$  changes, how many bits of  $(L_1, R_1)$  may be changed? Assume key is the same in both cases.  
(a) 1 (b) 2 (c) 4 (d) 32 (e) 64 (all bits in  $L_1$  and  $R_1$ )

10. Suppose DES is modified so that the high order 44 key bits are set to 0 so that only the 20 low order bits are used. What is the effective key length of this system?  
(a) 20 (b) 18 (c) 17 (d) 15 (e) 12
11. What is  $\phi(p^2)$  where  $p$  is an odd prime?  
(a)  $p(p - 1)$  (b)  $(p - 1)(p - 1)$  (c) There isn't a closed form expression just involving  $p$  (d)  $p^2 - 1$
12. For how many primes  $p$  is  $17p + 1$  a square?  
(a) None (b) One (c) Two (d) Infinitely many (e) Can't really tell.
13. Consider building a message digest function (similar to SHA) using DES. In particular, consider using the CBC mode of DES. Let  $K$  be a fixed known encryption key and let  $IV$  denote a fixed public initialization vector. The message could be padded appropriately using zeros to make it of block length suitable for encrypting with DES.  
To generate a hash, encrypt the (possibly padded) message in CBC mode of DES using key  $K$  and initialization vector  $IV$ . Output the final block  $C_n$  of the resulting ciphertext as the message digest of the message. What can be said about this setup:  
(a) This hash scheme is not collision resistant. (b) This hash scheme is not preimage resistant.  
(c) This hash scheme is not second preimage resistant. (d) All of the above. (e) a & b only.
14. What is  $2579^{2579} \bmod 19$ ?
15. For the RSA system in which  $n = 852337$ ,  $e = 3$ ,  $d = 566091$ , find the factors of  $n$ . Indicate the smaller factor in the answer.