1) True because you only need to pick a d that then satisfies ed = 1 (mod o). o = (p - 1)(q - 1)

2) False because 3^2 + 7^2 = 58 which doesn't have a gcd with 21 and 21 is relatively prime to 58.

3) True because with X = 1 (mod p) and X = q - 1 (mod q) Eve knows p divides X - 1 and q divides X + 1. This allows Eve to find the GCD of N and X - 1 or X + 1 and Eve will get either p or q and will be able to divide N to get the other.

4) True because if the ciphertext is not relativley prime to N then Eve can get a gcd(N, ciphertext) and see that the ciphertext is not relatively prime to N

5) False because this makes p and q approximately N/2 and you just look at the few primes that are around that number and you can quickly factor N

6) True beacause the miller rabin test has a 1/4 chance of failing so if you repeat it 300 times you get a (1/4^300) chance of it failing and 4^300 is >> 2^265 or the particles of the universe

7) True because you have to find x to get the LSB(x)

8) True because for 7 two generators would be 3 and 5 and 5 = 3^-1 (mod 7). For 11 two generators would be 2 and 6 and 6 = 2^-1 (mod 11)

9) True because the inverse of a quadratic nonresidue is also a quadratic nonresidue. QNR7 ={3,5,6} and the inverse of 3 (mod 7) = 5

10) False because -1 (mod n) = n - 1 and a generator hits all numbers 1 through n -1

11) True because quadratic non residues are non perfect squares and perfect squares will not generate all the numbers 1 through N - 1

12) False because it just gives you another way to reproduce b. You don't get more information to help solve what the secret exponenet is to break the system.

13) False because Eve can only discover the message m if e is relatively prime to 3 because of the common modulus attack on RSA - applied cryptograpghy p.472

14) False because the encryption of each message uses a random variable k

15) False because that would produce a d = 31 and not all very large primes are going to be have the property of 31 != 0 (mod p). Example 62

16) False because an Elliptical Curve can hit the point (0,0) so it can't be used as the point of infinity

17) False because infinity can never be hit when you call x (mod n)

18) True because gcd(t, p-1) implies that t is the inverse of g which inverse of g is a generator because problem 8 is True

19) True because if number 11 is true. Quadratic nonresidues only make up half the numbers of p so then at most only half the numbers can be generators

20) True because there is a LSB attack on RSA