

CSE497B/Spring 2007 - Quiz
Thursday, February 8, 2007 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. You have 20 minutes to complete this quiz, so focus on those questions whose subject matter you know well. Write legibly and check your answers before handing it in.

Short Answer - some will be one or two words – no more than 3 sentences

1. (3pts) Define the computer security concept of a *security model*.

answer: Describes the basis for security via a *trust model* and the challenges of achieving security guarantees via a *threat model*.

2. (3pts) List one way that *password policies* (i.e., in password choice and frequency of changes) improve the security of password choices and two ways that they reduce the security of password choices.

answer: Helps: (1) by eliminating obvious bad (short, dictionary, etc.) passwords; Hurts: (2) reduces the password entropy by precluding some possible choices in the password keyspace; Hurts: (3) Too frequent changes may result in poor choices of passwords to improve memorability. Other answers are possible.

Long Answer - no more than 2 paragraphs

3. (6pts) Why is it required that the private and public keys in RSA are *relatively-prime* to $\phi(n)$? Suppose $\phi(n) = 18$, choose two legal values for public and private keys (don't forget to include n).

answer: If a key is not relatively-prime, then it has no modular inverse, and we cannot generate a key pair. Plus, the substitution is not one-to-one for these numbers, so we do not get a proper encryption, either.

If $\phi(n)$ is 18, then we can choose $d = 5$ as it is relatively-prime to 18. A multiplicative inverse of $d \bmod 18$ is $e = 11$. Since $n = pq$ and $\phi(n) = (p - 1)(q - 1)$, then n can equal $(3 + 1)(6 + 1) = 28$ or $(2 + 1)(9 + 1) = 30$ or $(1 + 1)(18 + 1) = 38$. Only the last is the product of two primes, so a private key is $\{5, 38\}$ and a public key is $\{11, 38\}$.