CSE4232/5232 Spring 2006 Exam #3, open book, open notes. Name ____________________

Circle True or False (2 points each).

Answers in italics

T One major cause of security vulnerabilities is software bugs.

F Using hard to guess passwords will prevent buffer overflow attacks.

F Viruses cannot spread over an encrypted network connection.

F Keeping an encryption algorithm secret (in addition to the key) improves system security. *(This is Kerckhoff's principle. Algorithms that have not been publicly reviewed are almost always flawed).*

T A digital signature proves to the recipient that the sender of a message knows a secret without revealing that secret.

F A symmetric key system uses two keys. *(one key)*

F The strongest form of encryption is security against ciphertext-only attacks. *(Chosen plaintext resistance is a stronger requirement)*

F AES has been proven to be secure.

F RSA has been proven to be secure.

T The one time pad has been proven to be secure against ciphertext-only attacks. *(This is the only cipher proven to provide perfect secrecy).*

F The Java Random class can be used to generate random keys securely. *(A hardware source of randomness is required)*

T A MAC prevents a message from being tampered with.

T A MAC requires the sender and receiver to both know a secret key.

T "Nonce" means "number used once".

F If a stream cipher uses an IV, the IV must be kept secret. *(The IV is normally appended to the ciphertext and is needed for decryption).*

F X.509 is a standard for a secure hash function. *(It is a standard for certificates).*

F The SSL protocol requires a password.

T {1,10} is a subgroup of Z_{11}^*. *(10*10 = 1 (mod 11), 1 is the identity, $1^{-1} = 1$, $10^{-1} = 10$).*

F Z_{11}^* has order 11. *(order 10 because 0 is not included)*

F If $a^{n-1} = 1$ (mod n) then *a* must be prime. *(it says n might be prime)*

Questions are 5 points each.

What SMTP feature is normally disabled to help stop spam? *Relaying (to disguise the source address), or VRFY and EXPN (to verify email addresses). (Either answer is acceptable).*

Which two block cipher modes effectively convert them to stream ciphers? *OFB and CTR.*

Why does HMAC hash a message twice? *To prevent a length extension attack. Otherwise an attacker can append to a message and compute the hash without knowing the key.*

Why is ECB mode insecure? *Because identical plaintext blocks produce identical ciphertext blocks, revealing some information.*

Consider RSA with p = 5, q = 11, e = 3.

What is the public key? *n = pq = 55, e = 3.*

What is the ciphertext of the plaintext message 4? 4^3 *= 64 (mod 55) = 9.*

What algorithm (with what inputs) will find the decryption exponent?

Extended-Euclid(t, e) where t = LCM(p-1, q-1) = LCM(4, 10) = 20, and e = 3 to find the inverse of e (mod n).

Consider Diffie-Hellman with p = 5, g = 2.
 Alice picks secret key 2. What does she send to Bob? *2^2 mod 5 = 4.*
 Bob picks secret key 3. What does he send to Alice? *2^3 mod 5 = 8 mod 5 = 3.*
 What is the shared secret? *$(2^2)^3 = (2^3)^2 = 2^6 = 64 = 4$ (mod 5)*

Let p be the prime number $2^{11213} - 1$. What is 2^p mod p?
2^p mod p
= $2(2^{p-1})$ mod p (by factoring out 2)
= 2(1) mod p (by Fermat's little theorem)
= 2.

Let h be a secure 128 bit hash function. How much work is required to find two inputs x_1 and x_2 such that $h(x_1) = h(x_2)$?

2^{64}computations of h (on average).