

Submission Policy: Submissions must be typed (not handwritten) and stapled hardcopies are to be turned in (no softcopies). Only two late submissions (maximum delay from due date is "two days") per student are acceptable.

Answer as **True** or **False**. No explanations are required. Each correct answer is worth 4 points.

1. Even if DES can be broken, Double-DES cannot be broken.
2. AES is a stream cipher.
3. XOR in AES can be replaced by the bit-wise AND operation and still AES can remain secure.
4. AES has four modes of operation, and ECB is the most secure mode among them.
5. It is possible to carry out symmetric encryption using only asymmetric encryption mechanisms.
6. In private-key crypto: for 'm' users, in order to communicate between each pair of them in a secure manner, 'm' keys are sufficient.
7. Asymmetric encryption is better than symmetric encryption in terms of key distribution.
8. -. Two AES keys can be created such that one would be a public and the other would be a private key in order to establish asymmetric encryption.
9. It is theoretically impossible to carry out a brute-force attack on public-key encryptions.
10. Given a large random R, a message M, both of size n-bits,  $C = M \text{ (XOR) } R$  is theoretically secure, i.e., it is impossible to infer M from the knowledge of C.
11. RSA is based on the following problem: it is hard to determine whether a number is a prime or not.
12. Suppose you created K and K' as the public and private keys using RSA, respectively; it is absolutely fine to publicize K' as the public key and K as the private key.
13. In RSA, if p, q are small, then it is not hard to look up a table of primes and carry out factoring of 'n' easily.
14. Irrespective of whether (m) is True or False, for such p, q (as defined in (m)), RSA remains secure.
15. Given a hash function 'h', which outputs n-bit message digest, for messages of length  $m > n$ , there are two distinct messages  $m_1$  and  $m_2$ , such that  $h(m_1) = h(m_2)$ . (Hint: Use the Pigeon-hole principle; google it).
16. If (15) is True, then it is easy to find two such messages for SHA-1. If (15) is False, then it is easy to develop secure hash functions.
17. One-way property is the only requirement for a hash function to be a cryptographic hash function.
18.  $MD2 < MD5 < SHA-1$ , where < denotes that the hash function on the left-hand is less secure than the one on right-hand.
19. Checksum is not second pre-image resistant, but still can be used as a cryptographic hash function.
20. Hash function h, message m:  $h(m)$  can be used to prove the source of m.
21.  $MAC(K|m) = c$ ,  $MAC(K'|m') = c'$ . It is practically feasible to find K, m, K', m', such that  $c = c'$ .
22. The secret K in a MAC is shared between the sender and receiver; if the sender and receiver are previously unknown to each other, such sharing of K can be carried out by either symmetric cryptography or asymmetric cryptography.
23. Strength of the digital signature technique using public-key encryption taught in the class depends on the secrecy of the private key.
24. If timestamps are used in the computation of digital signatures, then such signatures cannot be easily duplicated.
25. If random numbers (instead of timestamps as in (25)) are used in the computation of digital signatures, then such signatures cannot be easily duplicated.
26. (**Bonus: 10pts**) Using RSA as the public-key encryption: ciphertext of 100 \* ciphertext of 10 = ciphertext of 1000; i.e.,  $(100^e \text{ mod } n) * (10^e \text{ mod } n) = (1000^e \text{ mod } n)$ , e and n are defined as in the RSA specification in the class. (Hints: read on modular arithmetic, Homomorphic encryption).