QUIZ 1, Crypto

Name:_____ NetID: _____ Grade:_____

1. In the three security properties, crypto protects _____ and _____, but not _____.
2. There are two types of attackers we consider in crypto: the ones that can eavesdrop, known as _____ attacker, and the ones who have full control of the channel, known as _____ attack.
3. _____ covers the existence of the information while crypto hides the meaning of the message.
4. To find the key length of Vignere cipher, we use _____ test by starting finding repeating patterns of length at least _____.
5. The adversarial model for ciphers include _____ attack, _____ attack, _____ attack and _____ attack.
6. In the binary version of One-time Pad, we use _____ (bit) operation to encrypt/decrypt.
7. To achieve perfect secrecy, one key can be used for ___ time(s) in OTP.
8. Perfect secrecy implies that key-length ___ message length.
9. The idea of stream cipher is to replace the random key in TOP with _____
10. A cryptographically secure PRNG satisfies the _____ test.
11. The same plaintext always gets the same ciphertexts. [True | False]
12. We propose two methods to formalize computational security: _____ and _____.
13. The encryption modes for black ciphers: _____, _____ and _____.
14. A MAC (message authentication code) scheme is a _____.
15. An RSA algorithm gives public key (e, n) and private key d. To encrypt, we should use _____ and to decrypt, we use _____. To generate a signature, we use _____ and to verify the signature, we use _____.
16. In IND-CPA security, IND stands for _____. And digital signature provides authentication, data integrity and _____.
17. Diffie-Hellman protocol can be used for _____
18. In Kerberos, if there are N parties and they are allowed to talk to each other, _____ keys are needed.