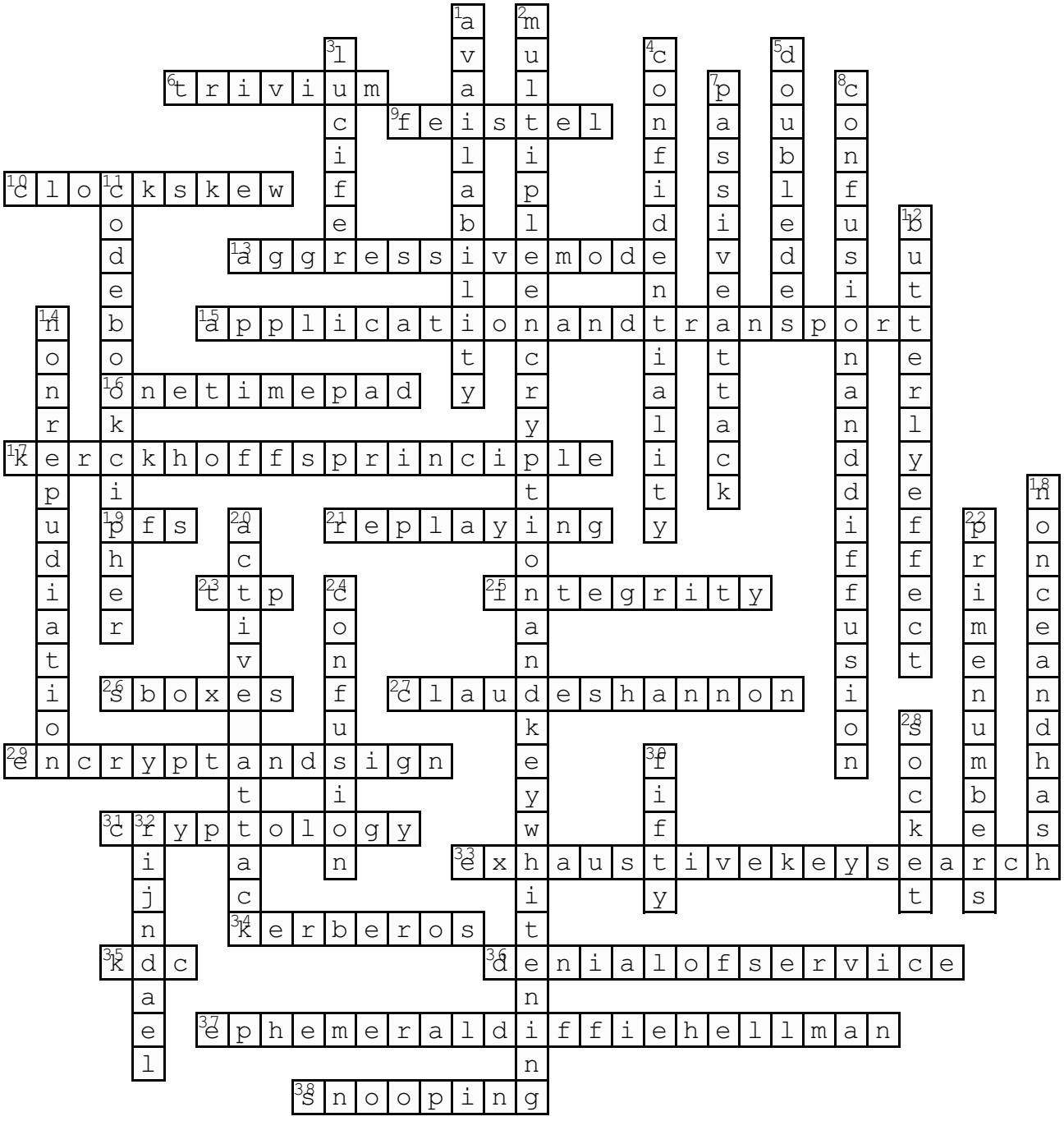
Name: _____

Complete the crossword below



Created with TheTeachersCorner.net Crossword Puzzle Generator

Across

6. A SHIFT REGISTER BASED SYMMETRIC CIPHER SHARING ITS NAME WITH AN AMERICAN HEAVY METAL BAND FROM ORLANDO, FLORIDA (**trivium**)
9. DES INCORPORATES THIS DESIGN PRINCIPLE (**feistel**)
10. THIS CAN BE A PROBLEM WHEN USING TIMESTAMPS FOR AUTHENTICATION (**clockskew**)
13. THE IPSEC VPN MODE VULNERABLE TO SNIFFING AS THE HASH IS SENT OUT IN CLEARTEXT (**aggressivemode**)
15. SSL WORKS IN BETWEEN THESE LAYERS (**applicationandtransport**)
16. THE ONLY PROVABLE SECURE CIPHER WHEN USED IN A CRYPTO SYSTEM CORRECTLY (**onetimepad**)
17. THE PRINCIPLE IN CONTRAST TO SECURITY THROUGH OBSCURITY AND STATES THAT CRYPTO ALGORITHMS SHOULD NOT BE SECRET (**kerckhoffsprinciple**)
19. THIS 3 LETTERED ACRONYM STANDS FOR THE PRINCIPLE THAT A SESSION KEY CANNOT BE COMPROMISED IF ONE OF THE LONG TERM KEYS IS COMPROMISED IN THE FUTURE (**pfs**)
21. A THREAT TO INTEGRITY (**replaying**)
23. OPERATIONS USED IN KERBEROS (**ttp**)
25. SECURITY GOAL OF A CRYPTO SYSTEM (**integrity**)
26. SECURITY OF DES DEPENDS ON THESE (**sboxes**)
27. AUTHOR OF A 1949 PAPER INTRODUCING THE PRINCIPLES OF CONFUSION AND DIFFUSION (**claudeshannon**)
29. THIS METHOD, WHEN USED WITH TIMESTAMPS IN ASYMMETRIC KEY BASED AUTHENTICATION, IS INSECURE AS AN INTRUDER CAN USE THE INITIATOR'S PUBLIC KEY AND DO A REPLAY ATTACK (**encryptandsign**)
31. ART AND SCIENCE OF MAKING AND BREAKING SECRET CODES (**cryptology**)
33. CAN BREAK DES (**exhaustivekeysearch**)
34. THIS AUTHENTICATION MODEL'S NAME IS DERIVED FROM GREEK MYTHOLOGY (**kerberos**)
35. THE CENTER OF OPERATIONS IN KERBEROS (**kdc**)
36. A THREAT TO AVAILABILITY (**denialofservice**)
37. PERFECT FORWARD SECRECY CAN BE ACHIEVED USING THIS EXCHANGE METHOD (**ephemeraldiffiehellman**)
38. A THREAT TO CONFIDENTIALTY (**snooping**)

Down

1. SECURITY GOAL OF A CRYPTO SYSTEM (**availability**)
2. DES CAN BE MADE RESISTANT TO BRUTE FORCE USING THESE (**multipleencryptionandkeywhitening**)
3. DES IS BASED ON THIS CIPHER CREATED BY IBM (**lucifer**)
4. SECURITY GOAL OF A CRYPTO SYSTEM (**confidentiality**)
5. A SEMI PRACTICAL KNOWN PLAINTEXT ATTACK CALLED 'MEET IN THE MIDDLE' IS POSSIBLE IN THIS ENCRYPTION ALGORITHM (**doubledes**)
7. ATTEMPTS TO LEARN OR MAKE USE OF INFORMATION FROM THE SYSTEM BUT DOES NOT AFFECT SYSTEM RESOURCES (**passiveattack**)
8. BLOCK CIPHERS EMPLOY THESE CHARACTERISTIC FOR SECURITY (**confusionanddiffusion**)
11. THE ZIMMERMAN TELEGRAM IS AN EXAMPLE OF THIS KIND OF CLASSIC CIPHER (**codebookcipher**)
12. PHENOMENON WHEREBY A MINUTE LOCALIZED CHANGE IN A COMPLEX CRYPTO SYSTEM CAN HAVE LARGE EFFECTS ON THE OUTPUT (**butterlyeffect**)
14. A KEY FEATURE LACKED BY SYMMETRIC KEY CRYPTOGRAPHY MAKING IT WEAK (**nonrepudiation**)
18. USED AS A CHALLENGE AND A RESPONSE FOR MUTUAL AUTHENTICATION (**nonceandhash**)
20. ATTEMPTS TO ALTER SYSTEM RESOURCES AND/OR AFFECT THEIR OPERATION (**active attack**)
22. THESE TYPES OF NUMBERS ARE VERY IMPORTANT IN CRYPTO (**primenumbers**)
24. STREAM CIPHERS EMPLOY THIS CHARACTERISTIC FOR SECURITY (**confusion**)
28. SSL PROTOCOL WORKS AT THIS LAYER (**socket**)
30. THE PERCENTAGE CHANCE OF THE KEYSTREAM BEING COMPUTATIONALLY INFEASIBLE TO PREDICT, GIVEN N CONSECUTIVE OUTPUT BITS, OF A KEYSTREAM GENERATED USING CSPRNG (**fifty**)
32. AES IS BASED ON THIS ALGORITHM (**rijndael**)