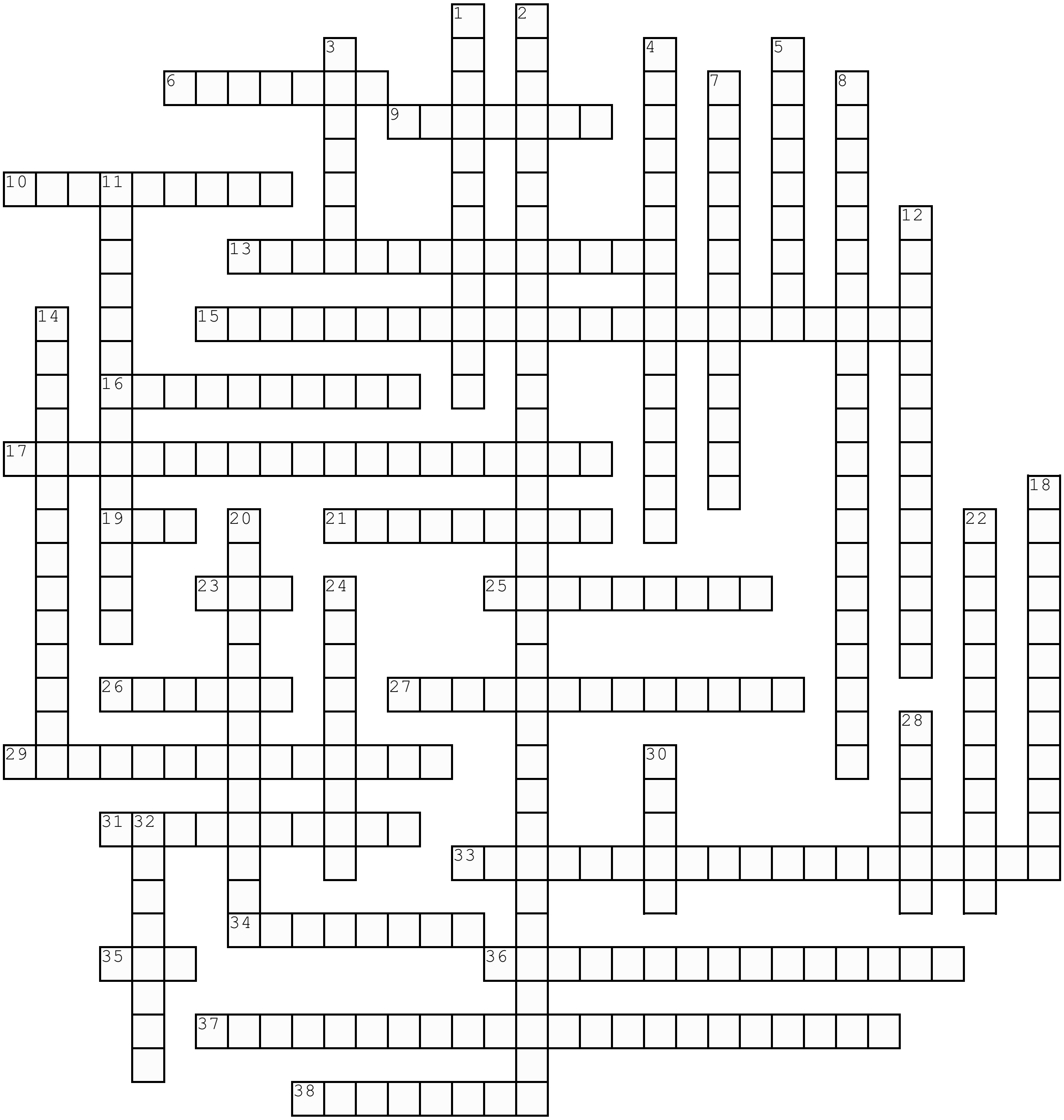
Name: ______________________________

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
9. DES INCORPORATES THIS DESIGN PRINCIPLE
10. THIS CAN BE A PROBLEM WHEN USING TIMESTAMPS FOR AUTHENTICATION
13. THE IPSEC VPN MODE VULNERABLE TO SNIFFING AS THE HASH IS SENT OUT IN CLEARTEXT
15. SSL WORKS IN BETWEEN THESE LAYERS
16. THE ONLY PROVABLE SECURE CIPHER WHEN USED IN A CRYPTO SYSTEM CORRECTLY
17. THE PRINCIPLE IN CONTRAST TO SECURITY THROUGH OBSCURITY AND STATES THAT CRYPTO ALGORITHMS SHOULD NOT BE SECRET
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
21. A THREAT TO INTEGRITY
23. OPERATIONS USED IN KERBEROS
25. SECURITY GOAL OF A CRYPTO SYSTEM
26. SECURITY OF DES DEPENDS ON THESE
27. AUTHOR OF A 1949 PAPER INTRODUCING THE PRINCIPLES OF CONFUSION AND DIFFUSION
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
31. ART AND SCIENCE OF MAKING AND BREAKING SECRET CODES
33. CAN BREAK DES
34. THIS AUTHENTICATION MODEL'S NAME IS DERIVED FROM GREEK MYTHOLOGY
35. THE CENTER OF OPERATIONS IN KERBEROS
36. A THREAT TO AVAILABILITY
37. PERFECT FORWARD SECRECY CAN BE ACHIEVED USING THIS EXCHANGE METHOD
38. A THREAT TO CONFIDENTIALTY

Down

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