Name: ____________________
Date: ____________________

Homework 1

Answer the questions in the spaces provided. If you run out of room for an answer, continue on the back of the page

Question:	1	2	3	4	5	6	7	8	9	10	Total
Points:	12	3	3	3	3	10	16	15	10	25	100
Score:											

1. (12 points) What is the purpose of Diffie-Hellman?

2. (3 points) What is a Merkle-Damgard transform?
   A. A type of tree in which hashes are combined to make a root that can be used to verify a hash's existence.
   B. A method of transforming variable length inputs to fixed length outputs
   C. A method of exchanging private keys publically
   D. A bitstring, determined by implementation, that the first block gets hashed with in SHA-256

3. (3 points) What is the pigeonhole principle?
   A. A method of brute force searching for Cryptographic Hash collisions
   B. A method of verifying a hash output given a key and message
   C. The state of having spread-out outputs for a Cryptographic Hash Function
   D. The idea that if the input sample space is larger than output sample space, collisions must exist

4. (3 points) The ______________ is a phenomenon in which the probability of collisions rises much faster than expected.

5. (3 points) A ______________ is a math problem that requires searching a large amount to find a solution without shortcuts

6. (10 points) What is the difference between Symmetric and Asymmetric Encryption?

7. (16 points) What are the two properties of Digital Signatures and why are they important?

8. (15 points) What are the three properties of Cryptographic Hash Functions and why are they important?

9. (10 points) What is the point of message digests?

10. (25 points) I am performing a Diffie Hellman Key Exchange with you. Given prime numbers 3 and 5, and secret numbers 18 and 23, what is our shared key?