Name: ______________________
Date: ______________________

Homework 1

Vincent Yang

March 21, 2016

Question:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Points:	5	5	15	15	10	0	0	0	0	0	0	0	0	0	0
Score:															

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

1. (5 points) What is the purpose of Diffie-Hellman?

2. (5 points) What is the difference between Symmetric and Asymmetric Encryption?

3. (15 points) What are the two properties of Digital Signatures and why are they important?

4. (15 points) What are the three properties of Cryptographic Hash Functions and why are they important?

5. (10 points) What is the point of message digests?

6. (2 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

7. (2 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

8. (2 points) The ______________ is a phenomenon in which the probability of collisions rises much faster than expected.

9. (2 points) A ______________ is a math problem that requires searching a large amount to find a solution without shortcuts

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?

11. Is it true that $x^n + y^n = z^n$ if x, y, z and n are positive integers?. Explain.

12. Is it true that $x^n + y^n = z^n$ if x, y, z and n are positive integers?. Explain.

13. Prove that the real part of all non-trivial zeros of the function $\zeta(z)$ is $\frac{1}{2}$

14. Compute

$$\int_0^\infty \frac{\sin(x)}{x}$$

15. Which of these guys invented time

A. Stephen Hawking B. Albert Einstein C. Isaac Newton D. This makes no sense

16. Which of these guys published a paper on Browninan Motion

○ Stephen Hawking

○ Albert Einstein

○ Isaac Newton

○ I don't know

17. Given the equation $x^n + y^n = z^n$ for x, y, z and n positive integers.

    (a) (10 points) For what values of n is the statement in the previous question true?

    (b) (10 points) For $n = 2$ there's a theorem with a special name. What's that name?

    (c) (10 points) What famous mathematician had an elegant proof for this theorem but there was not enough space in the margin to write it down?

18. (20 points) Compute

$$\int_0^\infty \frac{\sin(x)}{x}$$