

Midterm Exam

Name: _____

Soc.Sec#: _____

Write clearly!!! I must be able to read what you write!!!

Question 1: Diffie-Hellman

1. Is Diffie-Hellman a public key or secret key system.
2. Is Diffie-Hellman primarily used for authentication, key exchange, or encryption?
3. Describe how it is used for the case you picked in item 2 above. There is no need to supply math to justify its use.

4. What type of attack is Diffie-Hellman vulnerable to?

5. Give two ways to prevent or reduce this attack.

(a)

(b)

Question 2: Karn Symmetric Key Algorithm

1. Is the Karn Symmetric Key algorithm designed for a public key or a secret key cryptosystem?
2. Does it make use of the Data Encryption Standard or the Advanced Encryption Standard? If so, how?
3. Describe what it needs and what it does, roughly. Pictures might be helpful.
4. What does it rely on for security?
5. Can this algorithm be used for authentication? If so, how?

Question 3: Zero-Knowledge Proofs

1. For what purpose can a Zero-Knowledge proof be used?
2. Give an example of a Zero-Knowledge Proof - preferably Ali Babas cave.
3. What fact is trying to be proved in your example?
4. How do you know this is a Zero-Knowledge Proof?

Question 4: RSA

1. Is RSA a public key or secret key system?
2. What is good about RSA?
3. Describe how RSA works. Why is it considered secure? What can happen to compromise RSA forever, if it happens?