This is a 75 minute, CLOSED notes, books, etc. exam.
ASK if anything is not clear.
WORK INDIVIDUALLY.
Strategy: Scan the entire exam first. Work on the easier ones before the harder ones. Don't waste too much time on any one problem. Show all work on the space provided. Write your name on each page. Check to make sure you have 7 pages.

Question	Points	Score
1	10	
2	5	
3	10	
4	10	
5	15	
6	15	
7	10	
8	15	
9	15	
10	5	
11	10	
Total:	120	

Notation:

X_{Bob}	Apply Bob's public key to X.
$[X]_{Bob}$	Apply Bob's private key to X.
$E(P, K)$	Encrypt P with symmetric key Y.
$D(C, K)$	Decrypt C with symmetric key Y.
$h(x)$	Apply the cryptographic hash function h to x.

1. (10 points) Define the following terms:
   (a) Kerckhoff's principle

   (b) confidentiality

   (c) integrity

   (d) availability

2. (5 points) In class, we saw how we could hide a PDF in a bitmap file without changing the size of the bitmap or its appearance. How is this possible?

3. (10 points) Alice encrypts a message with key K using a stream cipher. She sends the resulting ciphertext $C = (1000, 1011, 0110, 1011)$ to Bob. Suppose that Trudy is able to intercept the ciphertext and she knows that the plaintext for this message is $P = (1011, 0001, 0101, 1100)$.
   (a) Recover the keystream K_s.

   (b) Show how Trudy can use the keystream K_s from part a to produce the ciphertext C', where $D(C', K)$ will yield the plaintext $P' = (0001, 1101, 1001, 0000)$.

4. (10 points) A co-worker proposes the following protocol: Each plaintext block of 128 bits is encrypted with AES, and then XORed with the previous block of ciphertext. For the first block, the result is instead XORed with a randomly chosen initialization vector (IV). More formally:

$$C_0 = E(P_0, K) \oplus IV$$
$$C_i = E(P_i, K) \oplus C_{i-1} \quad \text{where } i \geq 1$$

Then $(IV, C_0, C_1, ..., C_N)$ will be transmitted across the network. The intended recipient is expected to have the key K, and therefore can decrypt easily.

What are some potential issues with this protocol?

5. (15 points) (a) Give the formulas that define Feistel encryption and decryption.

(b) Is the TEA cipher a Feistel cipher? Why or why not?

(c) Consider a Feistel cipher with four rounds that uses the round function $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$. The plaintext is denoted $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. What is the ciphertext C in terms of L_0, R_0, and the subkey?

6. (15 points) (a) Give the formulas for CBC mode encryption and decryption.

(b) Suppose that Alice encrypts the plaintext blocks $P_0, P_1, P_2, P_3, P_4, P_5$ using CBC mode and shared symmetric key K, producing ciphertext blocks $C_0, C_1, C_2, C_3, C_4, C_5$. She sends the ciphertext to Bob along with the initialization vector IV. Suppose that a transmission error flips a bit in block C_2, resulting in block X. Which blocks can Bob decrypt correctly?

(c) Now suppose that Alice computes a MAC on the plaintext blocks $P_0, P_1, P_2, P_3, P_4, P_5$ using a shared symmetric key K. She then sends the plaintext, the IV, and the MAC to Bob. Trudy intercepts the communication and replaces P_3 with Y. Show that Bob will be able to detect the change.

(d) Alice wants to encrypt the plaintext and guarantee the integrity of her message. Suppose she first encrypts the plaintext as she did in part b. Then using the same initialization vector IV and key K, she calculates the MAC. She sends IV, the ciphertext, and the MAC to Bob. Finally, Bob decrypts the message using IV and K, calculates the MAC of the resulting plaintext using IV and K, and verifies that his calculation matches the MAC sent by Alice. Will this strategy work? Why or why not?

7. (10 points) This question deals with the RSA public key cryptosystem.
Alice's public key is $(N, e) = (33, 3)$. Her private key is $d = 7$.
You do not need to simplify your results for this problem.

   (a) Encrypt the message $M = 19$ with Alice's public key, i.e. find $\{19\}_{Alice}$.

   (b) Decrypt the ciphertext $C = 29$ encrypted with Alice's private key. In other words, calculate $[29]_{Alice}$.

8. (15 points) Alice and Bob wish to create a secure connection, so they use the Diffie-Hellman key exchange. They select the public values of $p = 43$ and $g = 9$.

   (a) Alice chooses a secret value of $a = 3$. Calculate her initial message to Bob.

   (b) Bob responds with 10. Calculate the shared secret value.

   (c) The Diffie-Hellman key exchange has an important vulnerability. Describe how Trudy might intercept communication between Alice and Bob if they are not careful. What measures can they take to defend against this attack?

9. (15 points) This problem deals with the knapsack cryptosystem. Suppose Bob's private key is $(3, 5, 10, 23)$ with the multiplier $m^{-1} = 6$ and the modulus $n = 47$.

   (a) Find the plaintext for the ciphertext $C = 20$. Give your answer in binary.

   (b) Find the plaintext for the ciphertext $C = 29$. Give your answer in binary.

   (c) Find m and the public key.

10. (5 points) What is the difference between a cryptographic-quality random number and a non-cryptographic pseudorandom number?

11. (10 points) This question deals with cryptographic hashes.
    (a) What are the key properties for a cryptographic hash?

    (b) Given a hash value of n bits, what is the expected work to find a collision?

    (c) What is a salt value (in the context of hashed passwords) and why is it important?

    (d) Suppose Trudy has obtained a file of usernames, hashed passwords, and salt values. Assume she also has a list of common passwords. Write pseudocode for a password cracking program. (No pepper value is used).