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 6 pages.

Question	Points	Score
1	5	
2	5	
3	5	
4	5	
5	5	
6	5	
7	10	
8	10	
9	10	
10	10	
11	10	
12	10	
13	15	
14	15	
15	0	
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. (5 points) Select **all** of the following true statements about a packet filter.
   A. Operates at the network layer.
   B. Operates at the transport layer.
   C. Defends against a TCP ACK scan.
   D. Is more efficient than an application proxy.
   E. Is aware of TCP connections.

2. (5 points) Select **all** of the following true statements about Kerberos.
   A. The key distribution center (KDC) is designed to be stateless to prevent denial of service attacks.
   B. Alice's password is encrypted and stored on her machine.
   C. The protocol uses nonces rather than timestamps for the sake of efficiency.
   D. A ticket granting ticket (TGT) is sent to the KDC to gain access to other resources.
   E. The KDC is a single point of failure for Kerberos.

3. (5 points) Select **all** of the following true statements about intrusion detection systems (IDS)?
   A. Anomaly-based IDS are unable to detect slight variants on known attacks.
   B. Provided that there are not too many signatures, signature-based IDS tend to be more efficient.
   C. IDS works by detecting "unusual" behavior.
   D. Signature-based IDS more easily provide details about specifics of an attack.
   E. Anomaly-based IDS are generally used to supplement signature-based IDS systems, rather than being used on their own.

4. (5 points) Select **all** all of the following statements about web cookies?
   A. Web cookies provide a strong means of authentication.
   B. They are stored only in the user's web browser.
   C. Web cookies are closely related to IPSec cookies.
   D. Sites use cookies to "remember" a returning visitor.
   E. Cross-site request forgery can be prevented by the use of web cookies.

5. (5 points) Compared to access control lists, capabilities (select **all** that are true):
   A. more easily handle delegation.
   B. are easier to implement.
   C. store permissions with the file.
   D. prevent the confused deputy attack.
   E. need a separate system for associating users to files.

6. (5 points) Assume that R is a random value sent in the clear from Alice to Bob and that K is a symmetric key shared between Alice and Bob. Select **all** of the following that may be used to establish a secure session key.
   A. $h(R, K)$
   B. $h(K, R)$
   C. $E(R, K)$
   D. $E(K, R)$
   E. $R \oplus K$

7. (10 points)

   (a) What are the primary advantages of IPSec over SSL?

   (b) What are the primary advantages of SSL over IPSec?

8. (10 points) Define the following terms:

   (a) authorization

   (b) authentication

   (c) perfect forward secrecy

   (d) confused deputy

   (e) two-factor authentication

9. (10 points) Suppose that a given password system uses 18 character passwords with 128 possible choices for each character.

   (a) If password P is stored as $h(P, S)$, where S is the salt value corresponding to the password, what is the attacker's expected work to crack the password?

      A. 2^{125}
      B. 2^{126}
      C. 2^{83}
      D. 2^{18}
      E. 2^{16}

(b) If password P is stored as $h(L, S_1), h(R, S_2)$, where L is the first 6 characters of the password, R is the remaining 12 characters of the password, and S_1 & S_2 are salt values, what is the attacker's expected work to crack the password?

A. 2^{125}
B. 2^{126}
C. 2^{83}
D. 2^{18}
E. 2^{16}

10. (10 points) This question is on security models.

(a) Compare and contrast Bell-LaPadula and Biba's model.

(b) Compare and contrast compartments and multilevel security.

11. (10 points) For a greatly simplified iris scan system, the following iris codes (in hex) are obtained:

Alice	`BE43`
Bob	`9C8B`
Charlie	`8855`

(a) During the recognition Phase, we get $X =$ `C975`.
Determine the following distances:
$d(\text{Alice}, X) =$

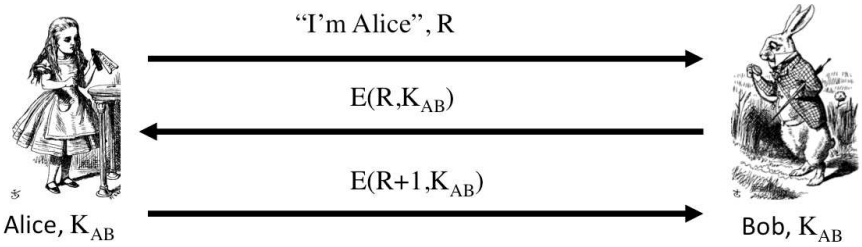
$d(\text{Bob}, X) =$

$d(\text{Charlie}, X) =$

(b) Assuming $d(x, y) < 0.32$ indicates a match, which user is a match?

A. Alice
B. Bob
C. Charlie
D. None of the above

12. (10 points) Consider the following protocol where K_{AB} is a secret, symmetric key shared between Alice and Bob.



Select **all** of the following true statements about this protocol.

A. Alice authenticates Bob.

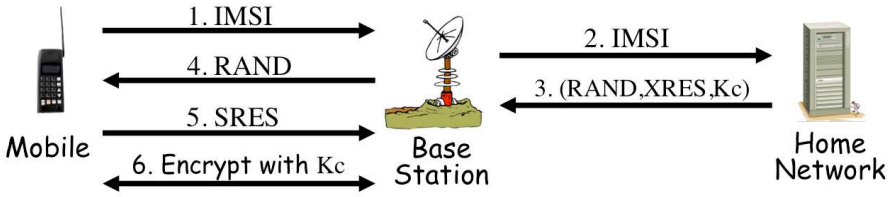
B. Bob authenticates Alice.

C. Trudy could use a replay attack to authenticate as Alice.

D. Trudy could use a replay attack to authenticate as Bob.

E. This protocol provides perfect forward secrecy.

13. (15 points) Consider the GSM protocol, where IMSI identifies the caller, RAND is a challenge, XRES is the expected response from the cell phone, SRES is the actual response, and K_C is a symmetric session key derived from a key Ki shared between the phone and the home network.



Give a secure one-message protocol that prevents cell phone cloning and establishes a shared encryption key.

14. (15 points) Describe some vulnerabilities in the wireless encryption protocol (WEP).

15. (0 points) **EXTRA CREDIT – 5 POINTS – NO PARTIAL CREDIT**
Consider the following protocol where $K = h(R_A, R_B, S)$.

Does this protocol provide plausible deniability? If so, why? If not, modify the protocol so that it does.