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	5	
2	5	
3	5	
4	5	
5	5	
6	10	
7	10	
8	5	
9	15	
10	5	
11	10	
12	10	
13	15	
14	5	
15	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 K.
$D(C, K)$	Decrypt C with symmetric key K.
$h(x)$	Apply the cryptographic hash function h to x.

1. (5 points) Select **all** of the following true statements about malware.
   - A. An advantage of flash worms is that they are easy to implement.
   - B. The main advantage of signature detection is its ability to detect previously unseen variants of malware.
   - C. Anomaly detection for malware looks for changes to the file system as a possible sign of new malware.
   - D. A backdoor is a type of virus that spreads over the network.
   - E. Signature detection for malware looks for patterns of bits that identify known malware.

2. (5 points) Select **all** of the following true statements about computer viruses.
   - A. A computer virus is a program that explicitly copies itself.
   - B. Polymorphic viruses encrypt the payload of the virus.
   - C. According to some definitions, a computer virus modifies other programs to include a possibly modified version of itself.
   - D. Metamorphic viruses rely on encryption to evade signature detection.
   - E. Change detection is the most widely used method of identifying computer viruses.

3. (5 points) Select **all** of the following true statements about digital rights management (DRM) and the Next Generation Secure Computing Base (NGSCB).
   - A. Attestation in NGSCB is the authentication of "things".
   - B. Only software-based DRM systems can protect the "analog hole".
   - C. Anti-reversing techniques such as anti-disassembly and anti-debugger techniques can be used to slow down an attacker reversing a DRM system.
   - D. NGSCB provides a secure path, which can prevent attacks like a screen capture.
   - E. The Nexus is the only component in the trusted computing base (TCB) of NGSCB.

4. (5 points) Select **all** of the following true statements about taint analysis and information flow analysis.
   - A. Taint analysis is primarily concerned with confidentiality.
   - B. Information flow analysis guarantees non-interference, meaning that public outputs do not depend on private inputs.
   - C. Secure multi-execution guarantees non-interference by running the same program (slightly modified) twice.
   - D. Only static information flow analysis is effective.
   - E. Languages like Perl and Ruby provide a taint mode to prevent untrusted strings from corrupting sensitive information like SQL queries.

5. (5 points) Select **all** of the following true statements about stream ciphers and block ciphers.
   - A. Block ciphers are more commonly implemented in software.
   - B. Block ciphers are generally preferred over stream ciphers when used on noisy channels.
   - C. Stream ciphers can be considered an advanced version of the classic codebook ciphers.
   - D. Cipher block chaining (CBC) mode can be used to give a block cipher some of the characteristics of a stream cipher.
   - E. Electronic codebook (ECB) mode should never be used for block ciphers.

6. (10 points) Define the following terms:
   (a) incomplete mediation

   (b) trojan horse

   (c) rabbit

   (d) salami attack

   (e) botnet

7. (10 points) Describe 3 different approaches used to avoid buffer overflow vulnerabilities.

8. (5 points) Describe the difference between mandatory access control (MAC) and discretionary access control (DAC).

9. (15 points) Consider the following code.

```
int main (int argc, const char *argv[]) {
     int i;
     boolean flag = true;
     char serial[9] = "S123456\n";
     if (strlen(argv[1]) < 8) {
          printf("Error\n");
     }
     for (i=0; i<8; ++i) {
          if (argv[1][i] != serial[i])
               flag = false;
     }
     if (flag)
          printf("Serial␣number␣is␣correct");
}
```

Describe how you might conduct a linearization attack against this code to determine the serial number.

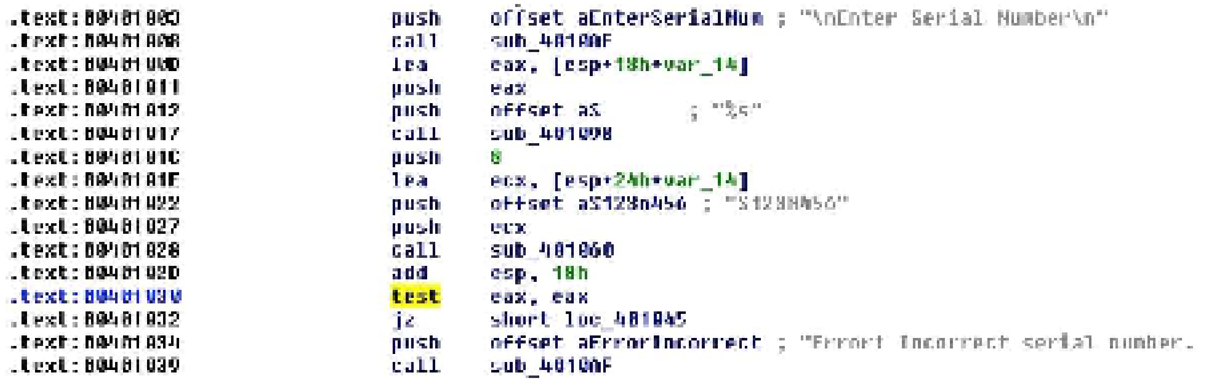
Correct this code to defend against the linearization attack.

10. (5 points) Suppose that you insert 100 bugs into an application that you are developing. Your QA team finds 25 of these bugs, as well as 80 additional bugs. Based on this information, estimate the number of bugs remaining in your application.

11. (10 points) This question deals with the RSA public key cryptosystem.
Alice's public key is $(N, e) = (33, 3)$.
Encrypt the message $M = 2$ with Alice's public key, i.e. find $\{2\}_{Alice}$.
You do not need to simplify your results for this problem.

Recall that $N = pq$ where p and q are "large" prime numbers, and that Alice's private key d is the multiplicative inverse of e modulo $(p-1)(q-1)$. Determine Alice's private key.

12. (10 points) Consider the following disassembled code that prints out a message when the correct serial number is entered.



```
.text:00401003                 push    offset aEnterSerialNum ; "\nEnter Serial Number\n"
.text:00401008                 call    sub_4010AF
.text:0040100D                 lea     eax, [esp+18h+var_14]
.text:00401011                 push    eax
.text:00401012                 push    offset aS       ; "%s"
.text:00401017                 call    sub_401098
.text:0040101C                 push    8
.text:0040101E                 lea     ecx, [esp+24h+var_14]
.text:00401022                 push    offset aS123n456 ; "S123N456"
.text:00401027                 push    ecx
.text:00401028                 call    sub_401060
.text:0040102D                 add     esp, 18h
.text:00401030                 test    eax, eax
.text:00401032                 jz      short loc_401045
.text:00401034                 push    offset aErrorIncorrect ; "Error! Incorrect serial number.
.text:00401039                 call    sub_4010AF
```

Give two ways to patch this code so that any serial number will work.

13. (15 points) Consider the following Digital Rights Management (DRM) system. A software application allows users to purchase and download videos. The videos are encrypted with AES using a 256 bit key. The key for all of the users content is hidden in the logo for the application.

    (a) What are the benefits of this scheme for storing the key?

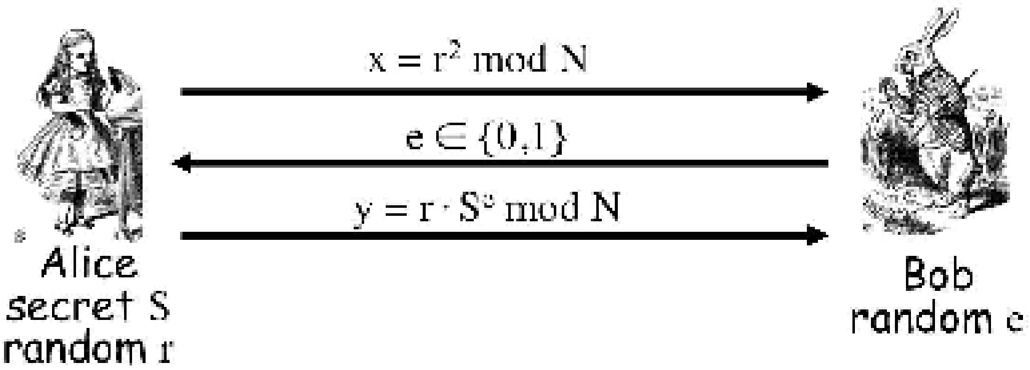
    (b) If Trudy suspects that this scheme is being used, what might she do to verify it?

    (c) A salesman gives a presentation to your company on this DRM system and claims that it is unbreakable. Give some reasons why you might be suspicious of this claim.

14. (5 points) Give two examples of different code injection attacks.

    What are some methods that can be used to defend against the code injection attacks that you mentioned?

15. (10 points) This question is on the Fiat-Shamir protocol, shown below.



To verify that Alice knows S without actually knowing S, Bob can verify that $y^2 = xv^e$ `mod N`, where $v = S^2$ `mod N`.

Suppose that $N = 35$ and $S = 2$.

(a) Calculate the (public) value for v.

(b) Suppose that Alice chooses $r = 7$. Calculate the value she sends for x.

(c) If Bob responds back with $e = 1$, what should Alice send in her final message?

(d) Show Bob's calculations to verify the values sent by Alice.