Net ID:

University of Illinois at Urbana-Champaign
Department of Computer Science

Midterm 1
CS461/ECE422 – Information Assurance
Fall 2007
Wednesday, September 26, 2006
Time Limit: 1 hour and 15 minutes

Instructions for the Student

Print your name and NetID in the space provided below**; print your NetID in the upper right hand corner of every page.**

Name: _____

NetID: _____

1. A single page of supplementary notes is allowed
2. Closed book
3. A calculator is allowed.
4. Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
5. Students can use scratch paper if desired.

Number of pages of the exam: 11

Number of questions on the exam: 18

Maximum grade on this exam is: 100 pts

Problem	Points	Score	Grader
1	2		
2	2		
3	2		
4	2		
5	2		
6	2		
7	2		
8	2		
9	2		
10	5		
11	12		
12	9		
13	14		
14	15		
15	8		
16	12		
17	4		
18	3		

Net ID:

Information Assurance: Midterm 1

Multiple Choice – 2 points each

1. Which of the following most accurately defines **vulnerability**.
    a. A set of circumstances that has the potential to cause loss or harm.
    b. Techniques for keeping data and resources hidden.
    c. A weakness in the system that can be exploited to cause harm.
    d. Techniques for detecting unexpected behavior.

2. What is the name for the following equation?
   ((Risk Exposure) – (Risk Exposure after Control))/(Cost of control)
    a. Risk Leverage
    b. Control costs benefits analysis
    c. Annualized Loss Exposure
    d. Risk Impact

3. What type of cipher is AES?
    a. Substitution
    b. Transposition
    c. Product
    d. Feistel Network

4. Which of the following is **not** a standard AES key length?
    a. 128
    b. 160
    c. 192
    d. 256

5. Which of the following uses ciphertext to generate the keystream?
    a. AES Electronic Codebook (ECB)
    b. DES Cipher Feedback (CFB) mode
    c. AES Output Feedback (OFB) mode
    d. AES Cipher Block Chaining (CBC) mode

6. The cryptographic strength of RSA depends on which hard problem?
    a. Discrete logarithms
    b. Factoring large primes
    c. Bin packing
    d. Elliptic curves

7. Which element is key to the non-linearity in the DES algorithm?
    a. Key schedule
    b. Splitting and swapping left and right halves of the data
    c. Initial permutation
    d. Substitution boxes

8. Which best identifies the purpose of an organizational security policy?
    a. A means of defining the secure states of the system
    b. Blueprint for the security implementation
    c. Document to satisfy legislative requirements
    d. A means of tracking the latest in security technology

9. Consider a double encryption of the form $C = E_{k1}(E_{k2}(P))$, where k1 and k2 are n bits long. What attack shows that the number of keys that must be checked to break a ciphertext/plaintext pair is 2^{n+1} instead of 2^{2n}.
    a. Man-in-the-middle attack
    b. Avalanche attack
    c. Birthday attack
    d. Meet-in-the-middle attack

Net ID:

Short answer

10. (5 points) If you and a colleague had to use a cipher by hand in the field, which one of the following ciphers would you select and why?
    a. Caesar
    b. Vigenere
    c. n-Transposition
    d. Book cipher
    e. One time pad

11. (12 points) For each of the following hashing functions state why that function would make a good cryptographic hash, or state why it would not.
    a. (2 points) 256 cyclic redundancy check (CRC)

    b. (2 points) 64 bit DES Cipher Block Chaining (CBC) MAC

    c. (2 points) SHA-256

    d. (2 points) 256 AES-CBC MAC

    e. (4 points) You need to post crypto hashes of your company's binaries on a central web site. Your customers fetch the binaries from a variety of mirrored sites and they need a way to ensure that the downloaded binary is indeed the legitimate copy. Which of the hash functions listed in this question would you use? Why?

12. (9 points) You have been hired by a company to review the communication confidentiality design created in house. Obviously the designers had not taken CS461. Identify the three worst security design errors and describe the problems caused by each of these three errors.

In the SecureComm architecture, we avoid the overheads of installing a PKI infrastructure by relying on a simpler approach of manually distributed shared keys between all pairs of communicators. Since the organization only has 25 communicators which will eventually grow to 50 over the next five years or so, we feel this approach will cost less in software and time than dealing with a full PKI solution. The keys will be passed to communicators via a separate channel such as a floppy disk or thumb drive, so the sensitive key will not be sent in the clear.

The master key file includes all the pairwise shared keys, and it can be stored on the central server. It will be stored under a very restrictive access control, so only members of the Administrative group can access the file to add or distribute keys. The master key file also provides a natural key escrow benefit. If an employee loses his or her key or leaves the organization, the administrator can access the appropriate keys from the master key file to access his or her networked conversations.

The shared key will be used in a block encryption algorithm designed by us called SuperCrypt. The algorithm is more sophisticated than AES, plus it has the benefit that it is proprietary so the attacker will not be able to attack the structure of the encryption algorithm. The SuperCrypt algorithm will be run in Electronic Code Book mode. The message integrity will be tracked by a HMAC-SHA crypto hash in the message.

Net ID:

13. (14 points total) Alice is setting up a RSA key pair. She has selected p=13 and q=11
    a. What is n? (1 point)

    b. What is Φ(n)? (1 point)

    c. She has picked e=13. Which of the following would work for d: 11, 37, 119? Why?(2 points)

    d. What values can be posted publicly and still preserve the security of the key pair?(2 points)

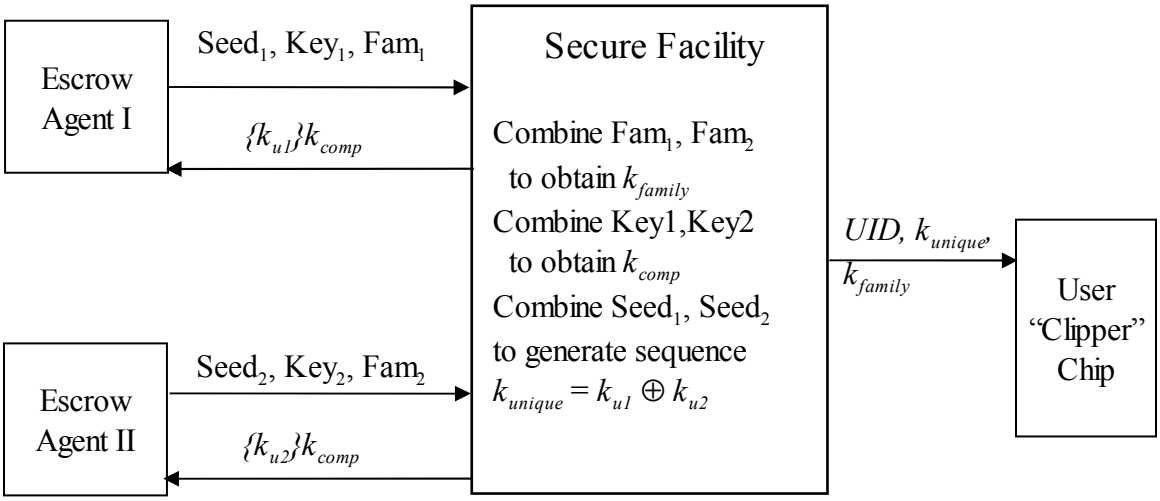
    e. What RSA operation would Alice apply to a message m to convince Bob that she originated m?(1 point)

    f. Apply that operation to the message EXAM. Assume a block size of one character and a character encoding of letters to numbers starting with A=1. (3 points)

    g. Alice has picked a session key k. Assume Alice already has access to Bob's public key. How should Alice compose a message to Bob to pass the session key while preserving confidentiality and integrity of data and identity. (4 points)

Net ID:

14. (15 points) You are hired to perform a risk analysis for an organization that is considering deploying a key escrow system similar to the Escrow Encryption Standard (or Clipper Chip system) discussed in class. Outline of the major components is shown below.



a. Name two risks they may be trying to control by deploying such a system. (3 points)

b. Would you choose to perform a qualitative or a quantitative risk analysis? Why? (2 points)

c. What are two assets in the key escrow system? (3 points)

(two more parts on the next page!)

d. What are two vulnerabilities in the key escrow system? (3 points)

e. Identify two threat sources and a motivation for each threat source. (4 points)

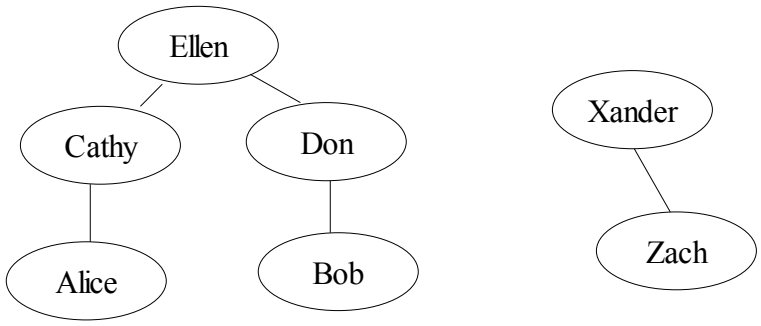
15. (8 points total, 2 points each) Is the following part of a policy or part of a mechanism
    a. File system access control list

    b. Departmental procedure for entering student information

    c. Department must prevent confidential information from being revealed to the public.

    d. Confidential information must be protected, and confidential information includes employee home address.

16. (12 points) Consider the certificate authority hierarchy below. In this question the notation *signer*<<*signee*>> means that *signer* has signed the certificate of *signee*.



a. (4 points) Alice receives Bob's certificate, Don<<Bob>>. What information does Alice need to verify this certificate?

b. (4 points) If Alice is concerned about a man-in-the middle attack, what is the minimal information should she fetch from a separate, secure channel to store on her computer?

c. (4 points) Alice receives Zach's certificate, Xander<<Zach>>. Zach is from a different organization. What additional information does Alice need to verify Zach's certificate? Can she meaningfully verify Zach's certificate? What change in the certificate authority relationships would help?

Net ID:

17. (4 points) Consider a Vigenere encryption C = E(k, msg).
    a. Assuming you are given a ciphertext and the length of the key, what is an upper bound on the number of keys you must test before you are guaranteed to break the key?

    b. Consider double encryption where the two Vigenere keys are of the same length, i.e., C = E(k1, E(k2, msg)) where length(k1) = length(k2). What is an upper bound on the number of cases you must test before you are guaranteed to break the key?

18. (3 points) Use the attached Vigenere's tableau to decrypt the following message encrypted with the Vigenere's key of EGB (461).

XNFITE

Net ID:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y