September 30, 2014

Midterm I

Please read the following rules before starting.

There are 16 questions, totaling 100 points.

Write your name on each sheet. Helps if the staple comes undone after you turn it in.

If you are uncertain about the details of a particular problem, make any reasonable assumptions that you feel are necessary to solve it. Be sure to write down your assumptions.

You are to neither give nor receive aid on this exam. You may not show or discuss this exam paper or your solution with anyone. Please sign and turn in this exam copy with your solution to acknowledge that you have followed these rules.

PRINT NAME : ____________________

IIT A# : ____________________

SIGNATURE : ____________________

01 - 06	07	08	09	10	11	12	13	14	15	16	Total

1. (2 pts) Order the following four items to match with the process of digital signature generation and verification: (circle one)

    1. Encrypt the digest with your private key.
    2. Compare the message digest to one you created.
    3. Generate a message digest.
    4. Decrypt the signature with the sender's public key.

    A. 4, 2, 1, 3

    B. 1, 4, 3, 2

    C. 3, 1, 4, 2

    D. 3, 4, 2, 1

2. (2 pts) What is the purpose of including Message Authentication Code (MAC) with the message?

3. (2 pts) What is the difference between a MAC and a HMAC?

4. (2 pts) Who generates the authenticator in Kerberos and what is the purpose of the authenticator?

5. (2 pts) What primary problem does public-key cryptography solve?

6. (2 pts) Explain the difference between stream ciphers and block cipher.

7. (4 pts) Which of the following statements are true about Diffie-Hellman (D-H) key exchange?

   A. The security of the scheme depends on it being difficult to solve $a^x = b \bmod n$ for a given b, n and x

   B. The security of the scheme depends on it being difficult to solve $a^x = b \bmod n$ for x given a, b and n

8. (4 pts) Suppose a One-way hash function is used in a message exchanged between Alice and Bob.

   A. (2 pts) Provide an example forgery scenario if the hash function lacks weak collision resistance property.

   B. (2 pts) Provide an example forgery scenario if the hash function lacks strong collision resistance property.

9. (10 pts)

   A. (5 pts) Decrypt the following English cipher-text which has been produced by using substitution (Caeser) cipher:
   kbkxeutk
   (Hint: Use the frequency distribution table of the letters of English language and the Vigenere Tableau given at the end of this script)

B. (5 pts) Consider a substitution cipher where 52 symbols were used instead of 26. In particular, each symbol in the cipher text is for either a lowercase English letter, or an uppercase English letter. For example, let E be the encryption function then we could have E(A) = T and E(a) = m. Such a modification augments the key space to 52! (52 factorial). Does this provide added security compared to a standard substitution cipher? Why or why not?

10. (10 pts) Suppose Alice wants to send a message to Bob containing her name N, her computers IP address IP, and a request R for Bob. Design encrypted messages that Alice must send to meet the security requirements below. Suppose that K_{-A} and K_{-B} are the private keys of Alice and Bob respectively. Assume that Alice and Bob share a symmetric key K and have securely distributed their public keys K_{+A} and K_{+B} to each other. Assume that all the messages include Alice's name, IP address, and the request.

Recall the notation that x||y means the concatenation of x with y, {x}k denotes the encryption of x using key k, and that h(x) denotes a hash of x. Using the notation above, answer each question below using a message exchange diagram (like the ones we used in class), being specific about what is computed, what is transmitted, and who the sender and receiver of the message is.

A. (2 pts) Using the symmetric key, design a message that enables Bob to verify that the messages integrity has not been violated and that it is from Alice.

B. (3 pts) Using the symmetric key, design a message that protects the confidentiality of the request and ensures that Bob can verify the messages integrity and source.

C. (2 pts) Using public key cryptography, design a message that enables Bob to verify that the messages integrity has not been violated and that it is from Alice.

D. (3 pts) Using public key cryptography, design a message that protects the confidentiality of the request and ensures that Bob can verify the messages integrity and source.

11. (10 pts)

A. (5 pts) Illustrate how Meet-in-the-Middle attacks can be devised with a double DES encryption scheme? How does 3DES protect against this attack.

B. (5 pts) Explain the self-healing property of cipher block chaining mode.

12. (10 pts)

A. (5 pts) Perform encryption and decryption using the RSA algorithm where p = 3, q = 11, e = 7, and M = 5.

B. (5 pts) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root g = 2.

i) If user A has public key Y_a = 9. What is A's private key X_a?

ii) if user B has public key Y_b = 3, what is the shared secret key K?

14. (10 pts)

A. (5 pts) A system allows the user to choose a password with a length of one to five characters, inclusive. Assume that 10,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of having been guessed. Determine the expected time to meet this probability under the condition that the password characters may be any number from 0 to 9.

B. (5 pts) Does using passwords with salts make attacking a single account more difficult than using passwords without salts? Explain why or why not.

15. (10 pts)

A. (5 pts) Read the following scenario and answer the question. You are in charge of upgrading the database system used by your company. There are 20,000 entries in the database worth protecting. You have estimated that each entry is worth $10. You can hire a team to reinforce security, which will lower the probability of an attack to 8%, but it will cost you $5,000. You have estimated the current probability of an attack and the impact of the attack, should one happen.

Situation 1: Impact = 0.8; current probability of an attack = 0.9.
Situation 2: Impact =0.3; current probability of an attack= 0.1.
In which situation, would you hire the security team? Justify your answer.

B. (5 pts) Suppose, you are writing a security policy for your organization. List at least three things that you need to consider.

16. (10 pts)

A. (3 pts) What security properties are ensured when you use https to access sites? Explain briefly.

B. (3 pts) What is the difference between transport mode and tunnel mode in IPSec?

C. (4 pts) What are the key differences between SSL and IPSec? Mention one application where IPSec is used.

17. (10 pts)

A. (6 pts) Consider the following three kinds of attack on a cryptosystem: cipher-text only, known plaintext, chosen plaintext. For each type of attacks list the information that needs to be available to an attacker.

B. (4 pts) Recognize the following modes of encryption for block ciphers based on their mathematical expressions. Notation: P_i is the ith block of plaintext, C_i of cipher-text, $E_k()$ is the block cipher encryption function, and $\oplus$ denotes the XOR function

for example: $C_i = E_k(P_i)$. Answer: ECB mode.

$C_i = E_k(C_{i-1} \oplus P_i)$. Answer:

$C_i = E_k(i) \oplus P_i$. Answer:

a	b	c	d	e	f	g	h	i
8.17	1.49	2.78	4.25	12.70	2.23	2.015	6.09	6.97
j	k	l	m	n	o	p	q	r
0.15	.77	4.025	2.41	6.75	7.5	1.93	0.095	5.99
s	t	u	v	w	x	y	z	
6.33	9.06	2.76	0.98	2.36	0.150	1.97	0.074	

Vigènere Tableau

	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