Total points: 71. Total time: 75 minutes. 9 problems over 9 pages. No book, notes, or calculator

1. [14 points]

a. Are n=221 and e=3 valid numbers for RSA. Explain. If you answer yes, obtain the corresponding d.

b. Are n=221 and e=5 valid numbers for RSA. Explain. If you answer yes, obtain the corresponding d.

2. [6 points]
Sensor X periodically sends a 32-octet measurement to a receiver Y (1 octet = 8 bits). One day the administrator decides that X should protect the measurement data by adding a MAC obtained using DES in CBC mode (in the standard way). How many octets does X now send for each measurement? Explain your answer.

3. [10 points]
An organization wants you to implement a PKI (public key infrastructure) for its employees. It has a large number of employees, divided into class-A employees and class-B employees. Class-A employees stay with the organization for several years on an average. When a class-A employee leaves, his/her access privileges must be revoked within an hour. Class-B employess stay with the organization for either six or seven days. When a class-B employee leaves, his/her access privileges must be revoked within a day.

Identify the documents of the PKI (e.g., certificates) and their structure (e.g., fields).
Impose constraints, if any, that would improve performance by exploiting the nature of the employees.

4. [15 points]

client A (has J)	**server B** (has J)
generate random N_A send [A, B, conn, N_A] // msg 1	
	receive [A, B, conn, N_A] S_A ← encrypt N_A with key J generate random N_B send [B, A, S_A, N_B] // msg 2
receive [B, A, S_A, N_B] T_A ← decrypt S_A with key J if $T_A = N_A$ then B is authenticated else abort S_B ← encrypt N_B with key J send [A, B, S_B] // msg 3	
	receive [A, B, S_B] T_B ← decrypt S_B with key J if $T_B = N_B$ then A is authenticated else abort

Client A and server B use the above authentication protocol. J is a key obtained from a password. B handles at most one client at a time. Answer the following; each part below is independent.

a. Consider an attacker that can **only eavesdrop** (i.e., hear messages in transit but cannot intercept messages or send messages with somebody else's sender id). Can this attacker obtain J by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

b. Consider an attacker that can **only spoof A** (i.e., send messages with sender id A and receive messages with destination id A, but not eavesdrop or intercept messages). Can this attacker obtain J by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

c. Consider an attacker that can **only spoof B**. Can this attacker obtain J by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

5. [5 points]
The same protocol as in problem 4 except that J is now a high-quality key; B still handles at most one client at a time.

client A (has J)	**server B** (has J)
generate random N_A send [A, B, conn, N_A] // msg 1	
	receive [A, B, conn, N_A] $S_A \leftarrow$ encrypt N_A with key J generate random N_B send [B, A, S_A, N_B] // msg 2
receive [B, A, S_A, N_B] $T_A \leftarrow$ decrypt S_A with key J if $T_A = N_A$ then B is authenticated else abort $S_B \leftarrow$ encrypt N_B with key J send [A, B, S_B] // msg 3	
	receive [A, B, S_B] $T_B \leftarrow$ decrypt S_B with key J if $T_B = N_B$ then A is authenticated else abort

Consider an attacker who can **eavesdrop, intercept messages, spoof A, and spoof B**. Can this attacker impersonate A to B. If you answer no, explain briefly. If you answer yes, describe the attack.

6. [5 points]
The same protocol as in problem 4 except that J is now a high-quality key, B can handle muliple clients at a time, and the different instances of B do not communicate with each other.

client A (has J)	**server B** (has J)
generate random N_A send [A, B, conn, N_A] // msg 1	
	receive [A, B, conn, N_A] $S_A \leftarrow$ encrypt N_A with key J generate random N_B send [B, A, S_A, N_B] // msg 2
receive [B, A, S_A, N_B] $T_A \leftarrow$ decrypt S_A with key J if $T_A = N_A$ then B is authenticated else abort $S_B \leftarrow$ encrypt N_B with key J send [A, B, S_B] // msg 3	
	receive [A, B, S_B] $T_B \leftarrow$ decrypt S_B with key J if $T_B = N_B$ then A is authenticated else abort

Consider an attacker who can only **spoof A**. Can this attacker impersonate A to B. If you answer no, explain briefly. If you answer yes, describe the attack.

7. [5 points]
Human principal A uses an RSA public-key pair {<*e*, *n*>, <*d*, *n*> for signature purposes. However, A does not remember the public-key pair. Instead A remembers a password *pw* and obtains its public key pair from a directory server D, which provides *e*, *n*, and *L*, where *L* is *d* encrypted with a key *J* obtained from *pw*. Here is the protocol A uses to obtain its public-key pair and send a signed message to B.

<table>
<tr><td>A (has <i>pw</i>)</td><td>D (has <A, <i>e</i>, <i>n</i>, <i>L</i>>)</td><td>B</td></tr>
<tr><td>send [A, D, gimme] // msg 1</td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2">receive [A, D, gimme]
send [D, A, e, n, L] to A // msg 2</td></tr>
<tr><td colspan="3">receive [D, A, e, n, L]
compute key J from pw
d ← decrypt L with key J</td></tr>
<tr><td colspan="2">send [A, B, msg, signature on msg] // msg 3</td><td></td></tr>
<tr><td colspan="2"></td><td>receive [A, B, msg, signature on msg]
….</td></tr>
</table>

Can an attacker who can only eavesdrop (i.e., hear messages but not intercept messages or spoof messages) obtain *d* by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

8. [10 points]
Principals A and B use the following authentication protocol involving a shared high-quality secret key K and Diffie-Hellman parameters g and p (not secret).

A (has K, g, p)	**B** (has K, g, p)
generate random N_A and S_A $T_A \leftarrow g^{SA} \bmod p$ send [A, B, K{N_A}, T_A]	
	receive [A, B, K{N_A}, T_A] $M_A \leftarrow$ decrypt K{N_A} using K generate random N_B and S_B $T_B \leftarrow g^{SB} \bmod p$ send [B, A, M_A, K{N_B}, T_B] session key $S \leftarrow T_A^{SB} \bmod p$
receive [B, A, M_A, K{N_B}, T_B] if $M_A = N_A$ then B authenticated else abort $M_B \leftarrow$ decrypt K{N_B} using K session key $S \leftarrow T_B^{SA} \bmod p$ send [A, B, M_B]	
	receive [A, B, M_B] if $M_B = N_B$ then A authenticated else abort
<-- ---- A and B use session key S for data exchange ------->	

Consider an attacker C that can eavesdrop, intercept messages, and send messages with another's sender id. Can this attacker decrypt the data exchange between A and B? If you answer no, explain briefly. If you answer yes, describe the attack.

9. [1 point]
When checking whether a number is prime, one helpful fact is the following:
a number is divisible by 9 if and only if the sum of its digits is divisible by 9.
For example, 12834 (and 84312 and 1283484312) is divisible by 9 because 1+2+8+3+4 equals 18 which is divisible by 9.

Prove the above fact.