Total points: 40. Total time: 75 minutes. 6 problems over 6 pages. No book, notes, or calculator

1. [14 points]
Are n=187 and e=9 valid numbers for RSA. Explain. If you answer yes, obtain the corresponding d.

2. [6 points]
Consider a sensor X that periodically sends a 64-octet measurement to a receiver Y. One day the administrator decides that X should encrypt the measurement data using DES in CBC mode. How many octets does X now send for each measurement? Explain your answer.

3. [8 points]
Lish, Pish, and Kish are three languages like English, except that each of them has an alphabet of 4 characters, namely, “A”, “B”, “C”, and “D”. The frequency (as percentage) of letter usage in these languages is as follows:

	“A”	“B”	“C”	“D”
Lish	35	15	35	15
Pish	40	30	20	10
Kish	20	20	40	20

Let P be plaintext that can be in either Lish, Pish, or Kish. You are given ciphertext Q obtained from P using a permutation cipher (e.g., “A, B, C, D” → “D, C, B, A”). Q has 1300 A’s, 3700 B’s, 1700 C’s, 3300 D’s. Which language is P most likely to be in. Justify your answer.

4. [4 points]
In the authentication protocol below, pw is A's password and J is a key derived from pw. Can an attacker that can eavesdrop messages (but not intercept or spoof messages) obtain pw by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

A (has pw)	**B** (has J)
send [conn] to B	
	generate random challenge R send [R]
compute J from pw compute X ← encrypt(R) with key J send [X] to B	
	compute Y ← decrypt(X) with key J if Y = R then A is authenticated

5. [4 points]
In the authentication protocol below, pw is A's password, J is a key derived from pw, and L is a high-quality key (which A gets from B as shown below). Can an attacker that can eavesdrop messages (but not intercept or spoof messages) obtain pw by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

A (has pw)	**B** (has J, L)
send [conn] to B	
	$X \leftarrow$ encrypt(L) with key J generate random challenge R send [X, R]
compute J from pw $L' \leftarrow$ decrypt(X) with key J $Y' \leftarrow$ encrypt(R) with key L' send [Y'] to B	
	compute $Y \leftarrow$ encrypt(R) with key L if $Y' = Y$ then A is authenticated

.

6. [4 points]
The chart below shows an authentication protocol, followed by data exchange, followed by disconnection.Only an initial part of the authentication protocol is shown; here, pw is A's password, J is a key derived from pw, and L is a high-quality key. Assume an attacker that can (1) eavesdrop messages and (2) intercept and spoof messages sent by A (but not those sent by B). Complete the authentication protocol (i.e., supply the part indicated by the "• • …. • •") so that inspite of this attacker

- B authenticates A,
- this authentication is not vulnerable to off-line password guessing, and
- A and B establish a session key S (for encrypting data) such that after A and B disconnect and forget S, even if the attacker learns pw, the attacker cannot decrypt the data exchanged.

A (has pw)	**B** (has J, L)
send [conn] to B	
	X ← encrypt(L) with key J send [X]
compute J from pw L′ ← decrypt(X) with key J	
• • • • • • • • • .	
<------------------ A and B exchange data ---------------->	
<------------------ A and B disconnect --------------------->	