Total points: 100. Total time: 115 minutes. 6 problems over 6 pages. No book, notes, or calculator

Unless stated otherwise, the following conventions are used:

- K{X} denotes X encrypted with secret key K (e.g., DES-CBC)
- Passive attacker: can only eavesdrop.
- Active attacker: can intercept messages and send messages with another's sender id.
- Server handles at most one client at a time

1. [10 points]

Company xLtd has principals X, A_1, A_2, …, where X issues certificates for the A_i's, and is their trust anchor.
Company yLtd has principals Y, B_1, B_2, …, where Y issues certificates for the B_i's, and is their trust anchor.
One day, xLtd acquires yLtd. You are to obtain a new PKI for the new xLtd. Parts a and b are independent.

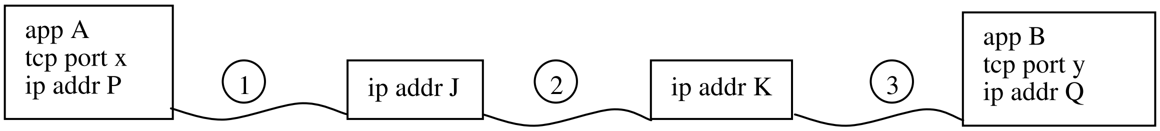
a. Modify the old PKIs to obtain a new PKI in which X is the sole trust anchor for all A_i's and B_i's; minimize the number of new certificates.
   Give the certificate chain that A_1 needs to get the public key of B_1 in the new PKI.
   Give the certificate chain that B_1 needs to get the public key of A_1 in the new PKI.

b. Modify the old PKIs to obtain a new PKI in which X is the sole trust anchor for all A_i's, and Y be the sole trust anchor for all B_i's; minimize the number of new certificates.
   Give the certificate chain that A_1 needs to get the public key of B_1 in the new PKI.
   Give the certificate chain that B_1 needs to get the public key of A_1 in the new PKI.

2. [20 points]

Below, “structure of an IP packet” means its headers (IP, TCP, etc, up to payload) and the values of addresses, ports, SPIs.

a. Applications A and B communicate over TCP over IP as shown, where J and K are intermediate IP routers. Give the structure of an IP packet from A to B at points 1, 2, and 3.



b. The above configuration is now modified as follows: P and Q operate IPsec-AH with SPI of 11 (for both directions); J and K operate IPsec-AH with SPI of 22. Give the structure of an IP packet from A to B at points 1, 2, and 3.

3. [20 points]

A (client, has K)	**B** (server, has entry [A, K])
send [A, B, conn] // msg1	
	receive msg1 generate random R_B send [B, A, R_B] // msg2
receive msg2 $S_B \leftarrow K\{R_B\}$ generate random R_A send [A, B, S_B, R_A] // msg3	
	receive msg3 if $S_B = K\{R_B\}$ then A authenticated else abort $S_A \leftarrow K\{R_A\}$ send [B, A, S_A] // msg4
receive msg4 if $S_A = K\{R_A\}$ then A authenticated else abort	
←--- exchange data encrypted with session key = function(R_A, R_B, K) ----→ Close session	

A and B share a high-quality secret key K and periodically establish sessions as shown above.
Each part below defines a specific session key function and a question for a kind of attacker.
If you answer yes, give the attack, and if you answer no, explain briefly.

a. If the session key is R_A+R_B, can a passive attacker decrypt the data exchanged in a session?
b. If the session key is $K\{R_A+R_B\}$, can a passive attacker decrypt the data exchanged in a session?
c. If the session key is $K\{R_A+R_B\}$, can an active attacker decrypt the data exchanged in a session?
d. If the session key is $(K+1)\{R_A+R_B\}$, can an active attacker decrypt the data exchanged in a session?

4. [15 points]

A (has pw)	**B** (has entry A:V)
obtain V from pw generate random a $T_A \leftarrow g^a$ mod-p send [A, B, V{T_A}] // msg1	
	receive msg1 extract T_A from V{T_A} using V generate random b $T_B \leftarrow g^b$ mod-p $K_B \leftarrow (T_A)^b$ mod-p send [B, A, T_B] // msg2
receive msg2 $K_A \leftarrow (T_B)^a$ mod-p send[A,B, K_A{M}] // msg3 ←--------- close connection ---------→	

Principal A periodically delivers plaintext information M to principal B using the above protocol, where V is a key obtained from A's password, g and p are public Diffie-Hellman parameters, and M changes across sessions.
In each part below, if you answer no, explain briefly; if you answer yes, describe the attack.

a. Can a passive attacker capable of off-line dictionary attack obtain M?
b. Can an active attacker capable of off-line dictionary attack obtain M?

5. [15 points]

It is the year 2020, and quantum computing has just made it feasible for the general public to factor large numbers.
Your company uses the following protocol, where g and p are Diffie-Hellman parameters, and K_1 and K_2 are explained below.

	A at tcp port x	**B at tcp port y**
	←---------- establish tcp connection between x and y ----------→	
1	generate random a send [x, y, K_1{A, B, g, p, g^a mod p}] // msg1	
2		receive msg1 generate random b send [y, x, K_2{B, A, g^b mod p}] // msg2 compute g^{ab} mod p
3	receive msg2 compute g^{ab} mod p send [x, y, hash{g^{ab} mod p }] // msg3	
4		receive msg 3 send [y, x, hash{1, g^{ab} mod p}] // msg4
	←----------------- A and B use g^{ab} mod p to encrypt data -------------------→	

a. Suppose K_1 is B's RSA public encryption key, and K_2 is A's RSA public encryption key.
   a1. Does the protocol hide B's identity against a passive attacker? If yes, explain. If no, show an attack.
   a2. Does the protocol provide perfect forward secrecy against a passive attacker? If yes, explain. If no, show an attack.
b. Repeat part a but now suppose that K_1 is a shared secret key (and hence the same as K_2).
c. In what situation would the protocol in part b not be practical.

6. [20 points]

In the following Needham-Schroeder-like protocol, K_{AB}, N_1, N_2, N_3, and N_4 are randomly generated.

A (has master key K_A)	**KDC** (has [A, K_A], [B, K_B], …)	**B** (has master key K_B)
send [A,KDC, N_1, 'A to B'] // msg1		
	receive msg1 $tkt_{AB} \leftarrow K_B\{K_{AB}, A, N_2\}$ send [KDC,A, $K_A\{N_1, N_2, B, K_{AB}, tkt_{AB}\}$] // msg2	
receive msg2 if (N_1 in msg1) $\neq$ (N_1 in msg2) then abort send [A,B, tkt_{AB}, $K_{AB}\{N_2, N_3\}$] // msg3		
		receive msg3 if (N_2 in tkt_{AB}) $\neq$ (N_2 in $K_{AB}\{N_2,N_3\}$) then abort $M_3 \leftarrow N_3 - 1$ send [B,A, $K_{AB}\{M_3, N_4\}$] // msg4
receive msg4 if $M_3 = N_3 - 1$ then B authenticated else abort $M_4 \leftarrow N_4 - 1$ send [A,B, $K_{AB}\{M_4\}$] // msg5		
		receive msg5 if $M_4 = N_4 - 1$ then A authenticated else abort
←--------------- A and B use K_{AB} to encrypt data -----------------→		

a. An attacker can eavesdrop and send messages with sender id A (but not B).
The attacker learns A's master key K_A after which A changes it.
Show how the attacker can have itself authenticated as A to B.

b. Modify the protocol to stop the attack in part a. You can add new messages and/or augment existing messages.

c. Modify the code executed by B to stop the attack in part a. Do not add new messages or change the existing messages.