Name: _____

Student Number: _____

COMP SCI 3C03/SFWR ENG 4C03 (Networks & Security) Michael Soltys

DAY CLASS
DURATION OF EXAMINATION: 2 Hours
MCMASTER UNIVERSITY FINAL EXAMINATION April 12, 2014

THIS EXAMINATION PAPER CONSISTS OF 3 PAGES AND 6 QUESTIONS.

YOU ARE RESPONSIBLE FOR ENSURING THAT YOUR COPY OF THE PAPER IS COMPLETE.
BRING ANY DISCREPANCY TO THE ATTENTION OF YOUR INVIGILATOR.

No aids allowed.

All questions worth 10 marks, for a total of 60.

Q1. This question deals with nodal delay.

(a) Consider a packet of length L which begins at end system A and travels over three links to a destination end system. These three links are connected by two packet switches. Let d_i, s_i, and R_i denote the length, propagation delays, and the transmission rate of link i, for $i = 1, 2, 3$. The packet switch delays each packet by d_{proc}. Assuming no queuing delays, in terms of d_i, s_i, R_i $(i = 1, 2, 3)$, and L, what is the total end-to-end delay for the packet?

(b) Continuing with the same setup as in (a), suppose now the packet is $1,500$ bytes, the propagation speed on all three links is $2.5 \cdot 10^8$ m/s, the transmission rates of all three links are 2 Mbps, the packet switch processing delay is 3 msec, the length of the first link is $5,000$ km, the length of the second link is $4,000$ km, and the length of the last link is $1,000$ km. For these values, what is the end-to-end delay?

Q2. Consider distributing an F-bit file to N peers using a client-server architecture. Assume a model where the server can simultaneously transmit to multiple peers, transmitting to each peer at different rates, as long as the combined rate does not exceed u_S.

(a) Suppose that $u_S/N \leq d_{\min}$. Specify a distribution scheme that has a distribution time of NF/u_S.

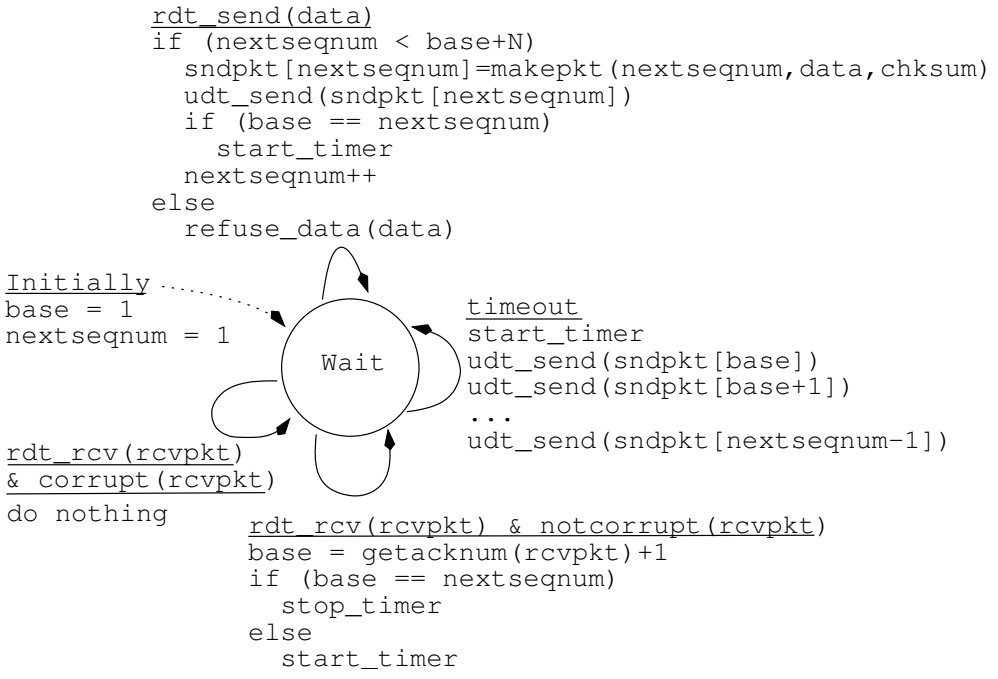
(b) Suppose that $u_S/N \geq d_{\min}$. Specify a distribution scheme that has a distribution time of $F/d_{\min}$.

(c) Conclude that the minimum distribution time is in general given by

$$D_{\text{C–S}} = \max\{NF/u_S, F/d_{\min}\}.$$

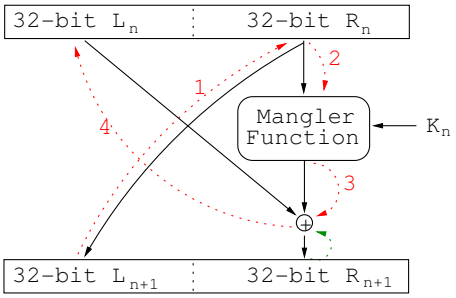
(*Hint*: You may use what we showed in class: $D_{\text{C–S}} \geq \max\{NF/u_S, F/d_{\min}\}$.)

Q3. This question is related to the transport layer of the protocol stack, and in particular to Reliable Data Transfer (RDT) over an unreliable channel. Consider the diagram for the "Go-Back-N" sender FSM:

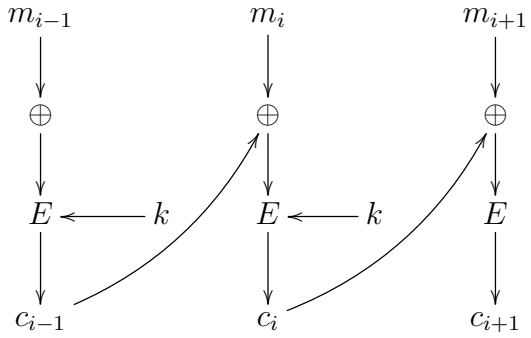


Provide an FSM for the receiver side and justify your design.

Q4. When we were discussing DES in class, we spent some time explaining how DES is reversible—i.e., how we can decrypt with the same key. We pointed out that regardless of how complicated the "Mangler function" is, we can still invert each round. Recall that this is what we called a "Feistel cipher." Explain how this inversion works; a diagram is included for your convenience.



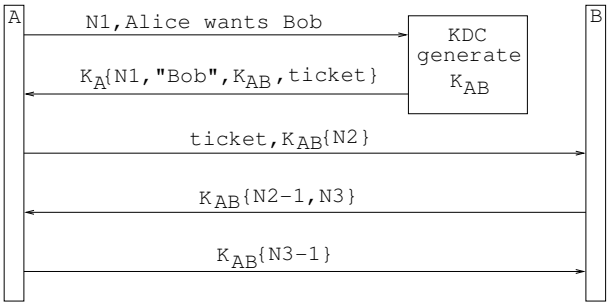
Q5. Consider a portion of cipher block chaining (CBC), depicted in the figure below.



(a) Suppose that an adversary intercepts the message, and wants to flip the 9-th bit of message block m_i, that is, he wants to change the ciphertext in such a way that the 9-th bit of message block m_i is flipped. How would he go about it? Justify your answer.

(b) How could the legitimate recipient of the message detect the tampering?

Q6. Consider the Needham-Schroeder protocol:



(a) What is the "ticket"?

(b) $N_1, N-2$ are called *nonces*; what is their role?

(c) Why do we send one way N_2 but return $N_2 - 1$?

(d) Why is "Bob" included in the second exchange?

END OF EXAM