- **Problem 1 (6 points), due by 17:00 April 2**

1. Below is a rotor machine example.
   - There is a keyboard of m keys for the 26 letters, space, punctuation marks and so on. There are $r > 1$ rotors $C_1, ..., C_r$, each C_i has m input pins and m output pins corresponding to the m keys. The circuit in rotor C_i connects one input to one output, defines a permutation from the m inputs to the m outputs of C_i.
   - One key of the keyboard touches one input pin of rotor C_1 (one-to-one mapping between the keys of the keyboard and the inputs of C_1). One output pin of rotor C_i, $1 \leq i < r$, touches one input pin of rotor C_{i+1} (one-to-one mapping between the outputs of C_i and the inputs of C_{i+1}).
   - Rotors rotate at different speeds. Rotor C_r rotates one pin position for one stroke on the keyboard (one circle for m strokes). Rotor C_i, $1 \leq i < r$, rotates one pin position when rotor C_{i+1} rotates one circle.
   - The keyboard gives the input to the machine and the output pins of rotor C_r give the output of the machine.

   Below is a secret key encryption scheme framework based on the rotor machine above for secure communications between a client and a server.
   - Both the server and client have a list of N security schemes $S_0, ..., S_{N-1}$.
   - Each security scheme S_i, $0 \leq i \leq N-1$, specifies a number r of rotors in the rotor machine and a permutation between the m inputs and m outputs of each rotor.
   - The client and server use the Diffie-Hellman algorithm (W. Diffie and M.E. Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, Vol. IT-22, Nov. pp. 644-654, 1976, or refer to the lecture notes) to deliver a secret integer k (key) between them.
   - Let $i = k \bmod N$. The client and server uses the security scheme S_i to realize the secure communication between them: the sender uses the rotor machine specified by S_i to encrypt the plaintext and the receiver uses the reverse process of the encryption to decrypt the ciphertext.

   Design a secret key encryption scheme using the above framework with $N \geq 5$, $r \geq 2$, and $m \geq 30$ keys to include at least the 26 letters, space, and punctuation marks of comma, full stop and question mark. Write programs (in JAVA or C++, please get the approval from your TA if other languages are used) which realize secure communications between a client and a server using your secret key encryption scheme.

   Submit a document which specifies your design for the encryption scheme, the programs which realize the secure communication, and data samples (before the encryption, after the encryption, captured from the network, and after the decryption) in the secure communications.

   Your programs must work in the virtual networks.

You need to submit your programs and document to the directory `/assignment/4/yourid` in the gateway machine `cs-vnl-e01.csil.sfu.ca` by 17:00 April 2. Please have clear comments in your programs to explain how they work.

2. A simple firewall is a filter which blocks the packets based on the pre-defined filter rules. There are two general strategies to set-up a filter. One strategy is `restrictive firewall` which blocks all packets except those specified. The other is `connectivity-based firewall` which allows all packets to pass through but blocks those specified. The packets to be allowed to pass through the filter in a restrictive firewall and the packets to blocked in a connectivity-based firewall can be defined case-by-case by the filter rules. The filter rules can be defined by the protocol type, host/network IP-address/name, TCP/UDP port number, interface name, etc. In the Linux the filter rules are set-up and maintained by `ipchains` or `iptables` commands (`iptables` is more powerful than `ipchains`).

   Set-up and test a simple restrictive firewall and a simple connectivity-based firewall in a host. The restrictive firewall should allow the input packets of a (or a few) specific protocol type(s) to pass through the filter and block all the other packets. The connectivity-based firewall should block the input packets of a (or a few) specific protocol type(s) but allow all the other packets to pass through. Log the allowed packets in the restrictive firewall and the blocked packets in the connectivity-based firewall. Submit a document to explain the design of your firewall (filter rules), the scripts for setting-up and testing the firewall, and a brief summary of each type of the logged packets (protocol type, source and destination IP addresses and host names, etc).

   Some notes

   - Consult the `man` page to find the details of `iptables` command. Further information is available at `www.netfilter.org`.
   - You may need to clean out any existing filter rules for the assignment and you **should clean out** what you have set-up after you finish your test. The following is a sample for clean out.

     ```
     iptables -F INPUT
     iptables -P INPUT ACCEPT
     iptables -F FORWARD
     iptables -P FORWARD ACCEPT
     iptables -F OUTPUT
     iptables -P OUTPUT ACCEPT
     ```
   - You may need to set-up the firewall on one machine and use a different machine to send packets to test the firewall.

     Absolutely do not use any of the routers **December, January, February, or March** for setting-up the firewall.

     Schedule your time accordingly since the Lab. may become crowed as the due date approaches.

   Your programs must work in the virtual networks.

You need to submit your programs and the document to the directory `/assignment/4/yourid` in the gateway machine `cs-vnl-e01.csil.sfu.ca` by 17:00 April 2. Please have clear comments in your programs to explain how they work.

- **Problem 2** (0 points)

1. IP must always check the destination addresses on incoming multicast datagrams and discard datagrams if the host is not in the specified multicast group. Explain how the host might receive a multicast destined for a group to which that host is not a member.
2. The IGMP general query message is used to monitor the memberships in multicast groups. This message may cause a large number of membership report messages. Explain briefly the main techniques used in the IGMP implementation to minimize the overhead of traffic caused by IGMP messages.
3. Assume that host H sends a leave report to router R, expressing H leaves multicast group G. What is the destination address in the IPv4 datagram which carries the leave report? What is the address in the address field in the IGMP leave report? Router R sends a group specific query to confirm the leave. What is the destination address in the IPv4 datagram which carries the query? What is the address in the multicast group address field in the query?
4. For the AS in Figure 1, assume that the routing tables for unicast computed by OSPF. Assume that G is a multicast group with members in $N_2, N_4, N_5, N_6.N_7$ and TRPF (Truncated Reverse Path Forwarding) is used by routers to deliver multicast messages. When Router R_5 receives a multicast message P with source N_2 and destination G from interface `eth0`, which interfaces R_5 forwards P to? If P receives P from `eth1`, which interfaces R_5 forwards P to?

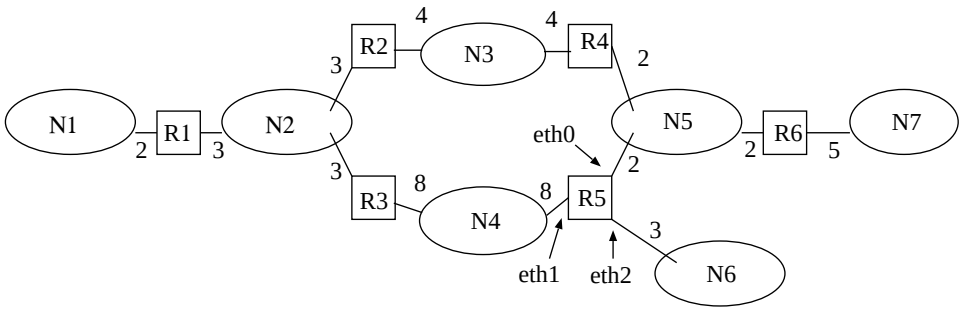

Figure 1: An autonomous system.

5. Main items in an NAT translation table include internal IP addresses, internal port numbers, external IP addresses, external port numbers, NAT port numbers, and payload type. Which items are used to identify a communication session between an NAT box and an internal host? Which items are used to identify a communication session

between an external host and an NAT box? Why is the payload type included as a main item in the table?

6. Select an English document (plaintext) of a reasonable length and find the top 5 letters in terms of the high relative frequency in the plaintext. Create the ciphertext of the plaintext by your encryption scheme designed in Problem 1 and find the relative frequencies of the top 5 letters in the ciphertext. Compare the relative frequencies of the 5 letters in the plaintext and ciphertext.
7. DES (Data Encryption Standard) has been widely used as secret key encryption scheme for many years. However, DES has been broken and is no longer considered as very secure. What weakness do you think DES has and how would you improve the security of DES if you are asked to modify it?
8. Explain briefly how public-key and secret-key encryption schemes are combined to make a more efficient encryption scheme.
9. Explain briefly how a public-key encryption scheme is used in digital signature.
10. The PGP protocols use several encryption/decryption keys. Explain the purpose of each key.