Tutorial Week 5

Question 1

1. One of the weaknesses of the PAP authentication system is that it transmits the password in the clear. How does CHAP avoid doing this?
2. What is the difference between a firewall that does ‘deep-packet inspection’ and a firewall that does ‘stateful-inspection’?

Question 2

Two biometric systems have the following error rates at different settings.

System 1

Setting	1	2	3	4	5	6	7	8	9	10
False rejects (%)	0.5	1	1	2	2.5	3	4	6	9	12
False accepts (%)	4	4	3	3	2.5	2.5	2	1.5	1.5	1

System 2

Setting	1	2	3	4	5	6	7	8	9	10
False rejects (%)	0	0	0	0	0	3	6	10	15	20
False accepts (%)	11	8	6	4	3	3	1	0	0	0

NOTE: False reject = classifying authorised user as an imposter

False accept = classifying imposter as an authorised user

1. Using the cross-over error rate as a performance criterion, which is the superior system?
2. Using total error rate at a particular setting as a performance criterion, which is the superior system?
3. If a false acceptance rate of 3% is acceptable which is the preferable system?

Question 3

Hash functions based on modulo arithmetic are often used in the generation of one-time passwords. Modulo arithmetic is very difficult to reverse. `X mod Y` is the remainder when `X` is divided by `Y`.

1. Calculate the following:

   `5 mod 3, 10 mod 11, 15 mod 12, 2 mod 1, 5 mod 5, 10 mod 5.`

2. Suppose we use the function `F(X) = (5 X ) mod 9` to generate our one time passwords.
   a. Generate the first 8 passwords (including the seed value). Start with a seed value of `X = 5`
   b. What will be the first password we use? The second? The third?
3. Suppose we use the function `F(X) = (5 X) mod 3.`
   a. Generate the first 4 passwords starting with X = 5
   b. Can you make any general observations about use of modulo arithmetic to generate passwords?

Tutorial Week 5

Question 4

Consider a simple challenge-response mechanism used for authentication. To calculate the response to the challenge, the key is added to the challenge and the hash is calculated. The hash is then returned as the response to the challenge.

The hash function is F(X) = 5 X mod 9. Each party has a shared secret key of 15. The challenge is an integer between 10 and 20.

What will be the response to a challenge of 11?