Ayoola Etiko, CS2413, 3598133

1) Explain how the proactive password checker approach can improve password security.
   - It requires at least 16 characters making the password less predictable.
   - Password must have at least 8 characters including an uppercase and lower-case letter, a symbol, and a digit. It may contain a dictionary word.
   - One way could be using the bloom filter which is based on rejecting words on a list that has been implemented on a number of systems.
2) List and briefly describe the principal physical characteristics used for biometric identification.
   - Fingerprints -> is one of the most well known and publicized biometrics which uses a variety of sensors scanning the direction of the ridge endings and bifurcations along a ridge path.
   - Hand geometry -> biometrics used to identify users due to the shape of their hands
   - Facial Characteristics -> biometrics used to identify users due to the patterns on their face
   - Retinal and Iris patterns -> these are biometric techniques which look for unique patterns in a person's retinal and iris blood vessels.
3) In the context of biometric user authentication, explain the terms, enrollment, verification and identification.
   - Enrollment -> This is the initial process of collecting biometric data samples from a person and subsequently storing the data in a reference template representing the user's identity to be used for later comparison.
   - Verification -> This is any means by which an individual is uniquely identified by evaluating one or more distinguishing biological and physical triats.
   - Identification -> This is when an individual is correlated set of data gotten with from the enrollment to identify the user.
4) Assume sources of length k are mapped in some uniform fashion into a target elements of length p. if each digit can take on one of r values, then the number of source elements is r^k and the number of target elements is the smaller number r^p. A particular source element xi is mapped to a particular target element yi.

a) What is the probability that the correct source element can be selected by an adversary on one try?
   - 1/r^k

b) What is the probability that a different source element that results in the same target
   - Each element in the r^p targets elements is mapped to r^k/r^p == r^k-p target elements. -> Hence there are r^(k-p) -1 different source elements. -> probability is (r^(k-p)-1)/r^k

c) Producing an adversary = 1/ not producing an adversary = 1/(r^p).

5) Why is it asserted that salt increases security.
   - Salt significantly increases the difficulty of attacks. -> If a salt is of "a' bit length, then the number of possible passwords is amplified by a factor of (2^a).