Question 1

1. Definitly The answer is NO. this can be shown easily through the 2 first chapters in Gollmann. He defines the security through aspects, another definition is through prevention, detection and reaction.
2. A way to measure security . Risk =AssetX VulnerabilityXThreat. Quantiitative relates to assign each input in Risk equation by a calculated numerical valve while qualitative assign a rank to each input in the risk equation.
3. Policy. It contains all the security concerns that should be considered in organization at both administrative and technical levels.

Question 2

A)Enrollment module :- considered as a first phase in authentication process includes extract the features with quality checkers and create the template which inserted in a database.

Authentication Module:- the second phase of authentication phase which includes the comparison between the extracted features and Template.

B) overt.

C) Universality H: Everybody has it

Distinctiveness L: Similar with twins, father/son, mother/dother

Permanence M: Changes over time; Aging really shows.

Collectability: H Very easy, also from long distance

Performance L: The recognition accuracy is low because of large variation

of facial expression, posing, lightning. Hair, glasses, and cosmetics might

also effect.

Acceptability H: Used long time in ID’s, people feel that it is non-intrusive

Circumvention H: Might be faked with mask, hairstyle, make-up, glasses

D)imposters :FMR

Genuine:FNMR

E)increase in Threshold will lead increase in FMR AND decrease in FNMR

Decrease in threshold will lead to decrease in FMR and increase in FNMR.

Question 3

1)94^8

2)94^8-42^8

3)94^8-42^8-84^8+32^8

4)2 from 8 \*(84^6-62^6)

Question 4

A)Eioss sileuo asayt wtsaem iranqi

B)5!

C)many ways . simple answer increase the key .

D)S-boxes for substitution . P-boxes for permutation

Question 5) Confidentiality by cipher algorithms

Same algorithms are used as one way function to enhance integrity

B) Transparent (each layer will depend on the other layers)or dependent (each layer will work independently )

C) Permissive policies :allow all but block certain dangerous service

Restrictive policies: prevent all but allow only traffic to meet a useful purpose http, pop3,SSH

restrictive policies is better

D) mechanism a:- a single solution to threat while service could combine many mechanisms