

**Faculty of Information Technology**

**Computer Science Department**

**Comp432 Midterm Exam**

**(Computer Security)**

Second Semester 2014-2015

Exam Date: March 22, 2015

Exam Time: 80 Minutes

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1) Overview and Management**

1. “ Explain one example in details where a security mechanism in one layer can be bypassed by an attacker who has access to a layer below.(6 Mark).

**5 examples mentioned in Gollmann+ any external example is accepted**

B) What we mean by risk analysis and for what risk analysis is used. Explain the Quantitative vs Qualitative methods in this field.(8 Mark).

**Risk Analysis = Threats\*Vulnerability\*Asset**

**Measuring security**

**Quantity: number**

**Quality: scale or Range**

C)what is the first priority for security manager to start to build security. Discuss your answer.(6Mark).

**Security Policy**

**Q2)Authentication and Biometrics**

A)What are the two different modules (phases) in any Biometric System(5Marks)

**Enrollment + Authentication**

B)Explain whether an online signature verification system can be classified as overt or as covert.(4marks)

**Overt . User awareness exist**

C)Give a brief explanation for following face features(Why not What):

**Universality H, all people have the face characteristics**

**Distinctiveness L, twins many similarities**

**Permanence M Faces will change among years**

**Collectability H, a lot of features can be collected**

**Performance L, should be taken in standard environment**

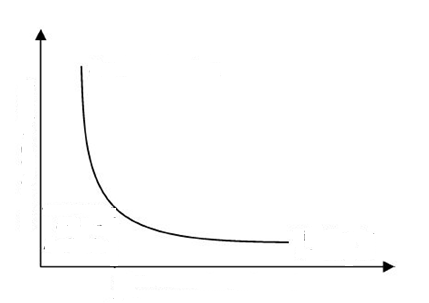
**Acceptability H people don't minds to take their pictures**

**Circumvention H Not easy to fool the system**

.(7marks) (H:High, M:Medium,L:Low)

D) For the following ROC curve please give the explanation by naming x axis and y axis and how the EER could be found using the curve.(6Marks)

**X axis FNMR Y axis FMR Draw x=y EER when FNMR=FMR**



E)The FMR and FNMR of a biometric system depend on the threshold. Explain the relation between the threshold and the values of the FMR and FNMR. (5Marks)

**Threshold increases FMR will increase FNMR will decrease**

**Threshold decreases FMR will decrease FNMR will increase**

**Q3)Cryptography**

The following message need to be Decrypted using Transposition Cipher TO BE Understandable The key used for Encryption process is (3,8,1,6,4,2,5,7) RLC IER SNI YKU DTS RIO OHE OTS

Answer the following

A) What is the Plain text.(7Marks**) sorry I don’t like this course**

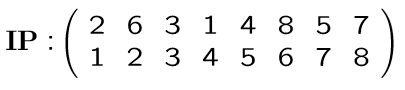
B)Possible number of keys(3marks)**8**!

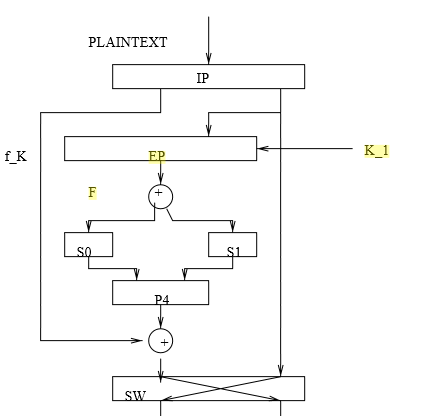
C)To make the transposition cipher more secure find an applicable way and explain it on the example above.(4marks) **longer key,….., etc**

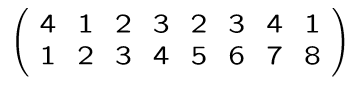
D) The diffusion and confusion principles of Shannon are implemented in modern ciphers and this can be easily shown in DES. Please discuss this statement.(6marks)

**Confusion through S-BOX**

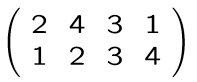
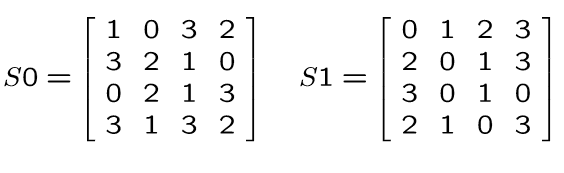
**Diffusion through P-BOX**

E)Given a block (3A)16 in simple DES and a key k1 (29)16 Find the cipher text for next round(simple iteration)





E



P4

**Final result: 1011 0011**

**Q4)Network Security**

A) What solutions on network level are proposed to implement confidentiality and integrity.(4)

Cryptography solution for both

B)According to OSI layers what are the two approaches to implement security services.(6)

**Independent layers, dependent layers**

C) Firewall is the best 100% security will be achieved through installing it. Discuss the statement(5)

**NOT True**

**Many limitations including viruses, insider,bad configuration, SQL,… etc**

D)Two types of policies are mentioned in Firewalls. Explain them Briefly and mention which of them you prefer to apply and why.(6)

Restrictive: block all and permit some

Permissive:permit all and block dangerous

E) According to stalling what are the differences between a mechanism and a service . Give an example on each.(4)

Mechanism certain and specific solution while service contains several mechanism to enhance a full aspect. (complete solution)