# **COMS3000: 2011 exam answers**

## **[UQattic](http://www.uqattic.net/)**

## **Get more out of your study time. Join UQattic's revision chat.**

### **Read this page first!**

### Please **contribute** to these documents.

### If you're looking for an effective way to familiarise yourself with the course material, you can't go past collaborating with fellow students. We have laboured to put these up, and so at the very least point out where you think we are wrong!

### You'll get more out of the course, you'll do better in the exam, and other students will benefit from your input as well.

### **Style.**

### If you're unsure of your answer, highlight your answer text then hit Ctrl+Alt+M to create a comment beside the text. Once you're satisfied with the answer, click the "Resolve" button on the comment.

### If you want some extra explanation from someone else on their answer, highlight the other person's answer and repeat the procedure above.

### If you are confident that your answer is correct, then just type it in red below each question.

### Finally, if you don’t want to appear anonymous, just share the document with yourself (the top-right blue button)

### **Communicate.**

### Head over to [uqattic.net](http://uqattic.net/) and click "Chat Now!". You'll find a chatroom full of students just like you. Talk about a revision document (like this one) or swap open book prep tips.

You can disable automatic email alerts of comment discussions via the "Discussions" button.

# **COMS3000: 2011 exam answers**

Q1. [2 marks] Describe the difference between the "Strong Collision Resistance" and the "Weak Collision Resistance" of cryptographic hash functions?

“Strong Collision Resistance”: it is computationally infeasible (practically impossible) to find any two distinct inputs x1 and x2 so that h(x1) = h(x2)

“Weak Collision Resistance”: for a given output y=h(x1), it is infeasible to find another input x2 so that h(x1) = h(x2)

Strong: There is no two inputs which will produce the same hash

Weak: it is infeasible to find two inputs which produce the same hash.

Not sure about above answer, specifically “Strong: There is no two inputs which will produce the same hash”. Given that the nature of a hash is that it reduces an arbitrary length to a fixed length collisions are inevitable. The answer from the lecture slides is “It is computationally infeasible to find any two distinct inputs x1 and x2 so that h(x1) = h(x2)”, which is slightly different from the answer provided above as there are two inputs which could produce the same hash but there is no method more efficient than brute force to find any case of this.

Q2. [2 marks] What is the purpose of the WS-SecurityPolicy standard?

Sending security tokens to assert user identity

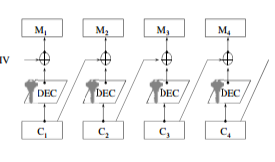
Signing data to ensure data integrity and verify sender

Encrypting data to ensure confidentiality of data

A standard set of extensions which can be used when building secure web services to implement integrity and confidentiality

Q3. [6 marks] Draw a block diagram of a block cipher in Cipher Block Chaining (CBC) mode for decryption. Due to a transmission error, a ciphertext block (say C2) has a single bit error in the first bit of the block. How does this affect the plaintext blocks after decryption at the receiver?

A single bit error will not have a negative effect on the blocks after the corrupted bit, as CBC is  
self recovering from bit errors.



A single bit error in C2 would cause that corresponding bit to have an error in M3 and M2  
decryption as M2 is decrypted from c1 and c2 and M3 is decrypted from C2 and C3.

Q4. [6 marks] Describe what is meant by the terms SaaS, PaaS, and IaaS and state who is typically responsible for securing which components for each.

In general, the lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.

SaaS: “Software as a Service”

* Software is licensed on a subscription basis and is centrally hosted.

PaaS: “Platform as a Service”

* Networks, servers, storage, OS, ‘middleware’, database and other services are provided to host customer applications.

IaaS: “Infrastructure as a Service”

* Providers offer computing infrastructure such as virtual machines as a service to subscribers.

QS. [3 marks] Describe and explain the difference between three different factors of authentication mechanisms .

Multi-factor Authentication - Most commonly two factors are used as a combination of:

* Something you **know** eg: Passwords
* Something you **have** eg: Physical Keys
* Something you **are** eg: Biometrics (fingerprints etc)

These factors are defined as Authorisation, Authentication and Identification.

Identification is determining the identity of someone, whereas authentication is VERIFYING that identity (making sure they are who they say they are) and authorisation is determining whether to allow that person access to a certain resource based on the authenticated identity.

Q6. [4 marks] Describe how a wireless station may be forced to disconnect from a legitimate access point in an attempt to get it to use a "Fake AP" and how can this be averted.

A Deauthentication/Disassociation attack can cause this. It is protected against in the IEEE 802.11w standard which protects against Injection Attacks, Disassociation attacks, and Fake APs. This is achievable through the use of protected management frames.

Q7. [6 marks] Classify each of the following controls from the PCI DSS as a Preventative, Detective or Reactive measure [3 marks] and explain why each is so classified [3 marks]:

*PC/DSS Requirement 10.6: "Review logs for all system components at least daily."*

Detective: anomalies in the system logs will be exposed by this requirement.

*PC/DSS Requirement 3.6.8: "Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities."*

Preventative: Reviewing the logs will reveal any suspicious activity after the fact, and most likely include usernames/IP addresses of the culprits. Does not prevent attack or specify what action should be taken upon attack detection.

*PC/DSS Requirement 1.1.6: "Review firewall and router rule sets at least every six months."*

Reactive - An incident response plan specifies how to behave in the event of a breach, which neither prevents nor detects attacks.

Preventive? Attack has not happened yet

Q8. (20 marks) Give an example of an information security control for each of the domains of the *Certified Information Systems Security Professional* Common Body of Knowledge'®

**[2 marks each]**

Q9. (3 marks) Explain whether or not ***Stuxnet***is an "APT".

Stuxnet satisfies each of the conditions to be considered an APT

APT =

Advanced

* Stuxnet was developed by a group of dedicated experts in cyber intrusion methods, capable of crafting custom exploits and tools.

Persistent

* A long-term objective existed, with the developers persistently working over 6 months of development.

Threat

* The group of attackers were organized, funded, well trained, and highly motivated.

Q10. (2 marks) Give two reasons why a company or government agency would choose to use a common standard for web single sign-on?

A common standard allows specification of security requirements of a system, and rigorous evaluation against them. An SSO solution can also greatly reduce the number of passwords a user has to remember, which might encourage the user to choose a much stronger password.

Q11. (5 marks) Explain how you could use certificate-based authentication to provide a practical two-factor authentication system? Ensure you explain how it achieves two-factor authentication.

Use the Certificate as something you have, and a Password as something you know to achieve two-factor authentication.

A practical implementation of this might be to have a user authorised to use a service, creating a user account on an authentication server and in a certificate database. The user enrolls with the PKI and installs their unique digital certificate. The user can now log in with their password from the authenticated machine.

Q12. (22 marks] The ciphertext "EHAWK ZGBHX KMPAI BJZCX AFBHX BJLXK FMJIY

UEXDJ CKPHX IJFBX IBHXK ZVXZB KZGAF FIXQU XZCYJ ZJL YE KE" was produced

from English text with a Monoalphabetic cipher.

Note: monoalphabetic is the rearrangement of the alphabet like a caesar shift except each letter is linked to an out of position letter.

For example: **abcdefghijklmnopqrstuvwxyz**  
 **jtcdxfghksnlmzapqiebuvwoyr (key)**

a) (10 marks] Demonstrate the most efficient method to decrypt the ciphertext with only the resources you have available to you in this examination.

The most efficient way to break a monoalphabetic is the use of frequency analysis. Otherwise bruteforce has to be done.

Monoalphabetic not Vigenère. This would be an easy mistake to make in the exam.  
Frequency analysis is therefore required.  
Answer something like: “showi ngthe impor tance ofthe talei fmary useda ciphe rafte rthei nvent ingof frequ encya nal ys is”  
Or ”showing the importance of the tale if mary used a cipher after the inventing of frequency analysis”

Key:  
J R C D X F G H K S T L M Z A P Q I E B U V W N Y O  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Letter frequencies:

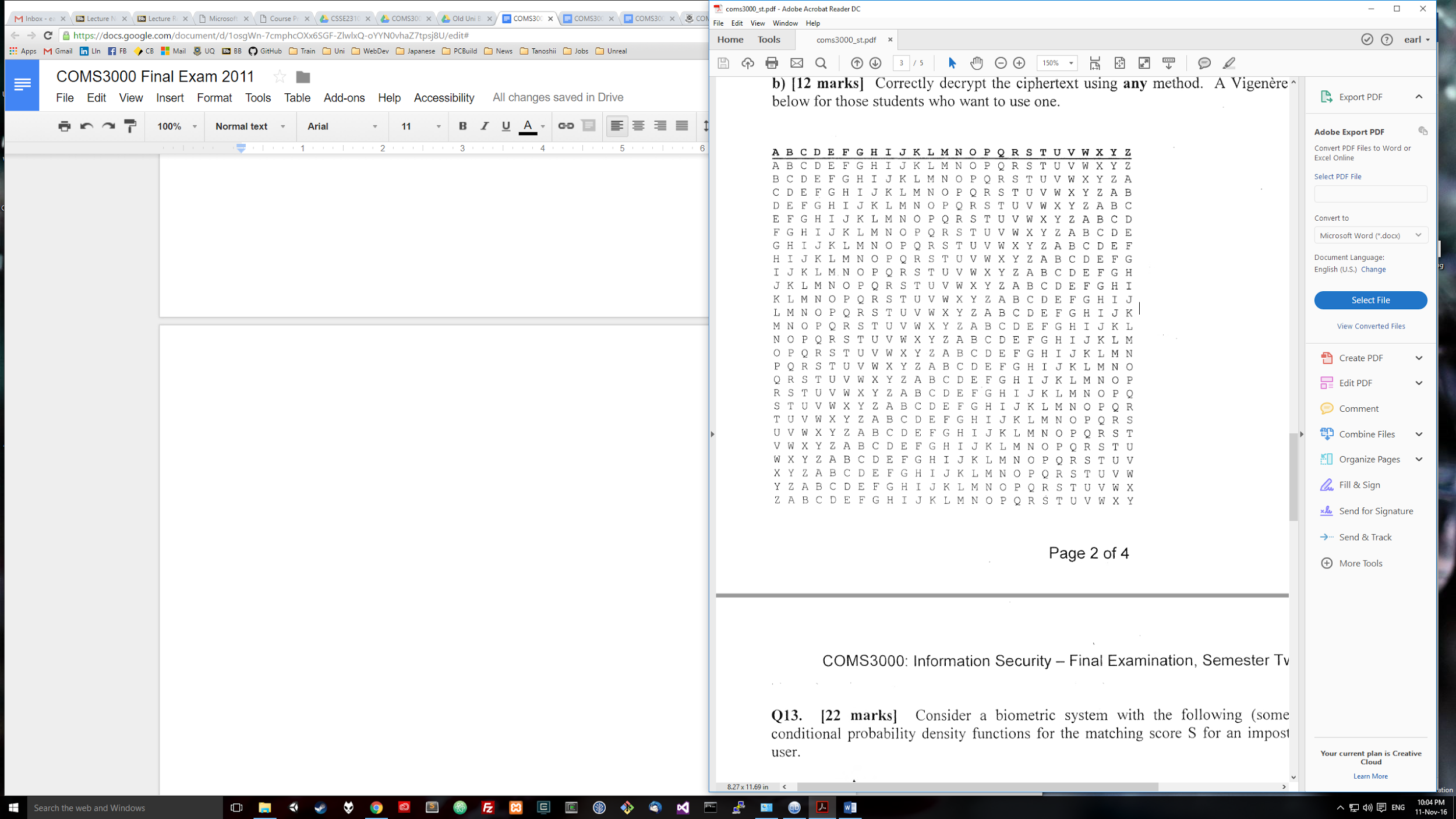
11 X  
7 J  
7 K  
7 B  
7 Z  
5 H  
5 I  
5 F  
4 E  
4 A  
3 Y  
3 C

2 P  
2 U  
2 G  
2 L  
2 M  
1 W  
1 Q  
1 D  
1 V

b) [12 marks] Correctly decrypt the ciphertext using any method. A Vigenere table is provided below for those students who want to use one.

"EHAWK ZGBHX KMPAI BJZCX AFBHX BJLXK FMJIY UEXDJ CKPHX IJFBX IBHXK ZVXZB KZGAF FIXQU XZCYJ ZJL YE KE"

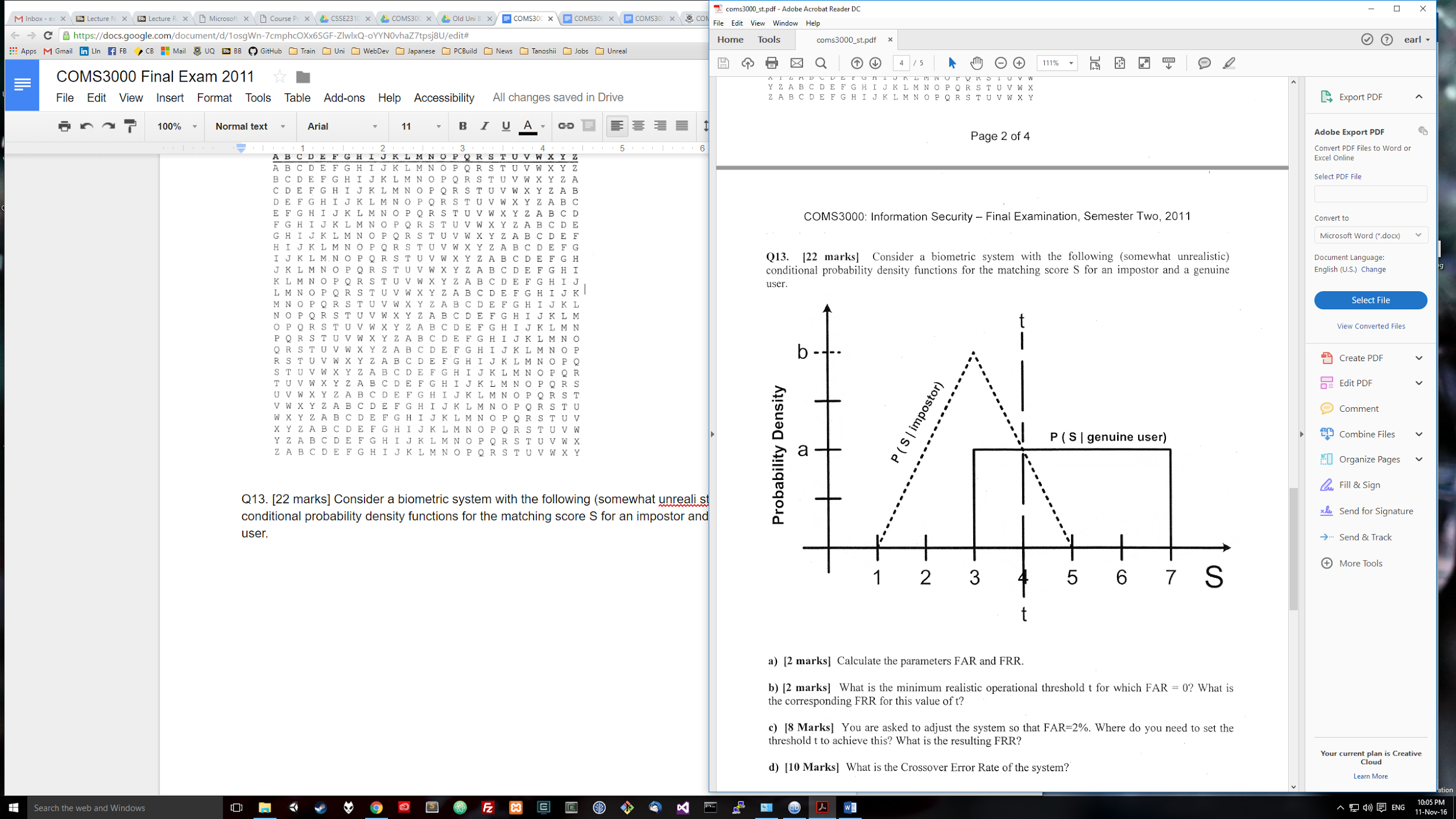
= “Showing the importance of the tale if mary used a cipher after the invention of frequency analysis” (using the key above)



Q13. [22 marks] Consider a biometric system with the following (somewhat unrealistic)

conditional probability density functions for the matching score S for an impostor and a genuine

user.



a) [2 marks] Calculate the parameters FAR and FRR.

Calculate b: (5-1) \* b \* 0.5 = 1 so b = 0.5

Calculate a: (7-3) \* a = 1 so a = 0.25

FAR: 50%

FRR: 25%

1 = a \* 4

a = 0.25

FAR = (1 \* a)/2 = 0.125 ??

FFR = (4-3) \* a = 0.25

4\*a=1 (a=0.25)  
FAR => False Accept Rate (imposters allowed in) (FMR) = (1\*a)/2 = 0.125 (12.5%)  
FRR => False Reject Rate (genuine users locked out) (FNMR) = 1\* a = 0.25 (25%)

b) [2 marks] What is the minimum realistic operational threshold t for which FAR = 0? What is

the corresponding FRR for this value of t?

FAR = 0 = 0.25 \* (5-t) = 5/4 - t/4 = t/4 = 5/4 -> t = 5

FRR = (3-3) \* a = 0

t = 5  
FRR => False Reject Rate (genuine users locked out) (FNMR) = (5-3)\* 0.25 = 0.5

c) [8 Marks] You are asked to adjust the system so that FAR=2%. Where do you need to set the

threshold t to achieve this? What is the resulting FRR?

FAR = 0.02 = 0.25 x (5-t) = 5/4 - t/4 -> .25 = 4 - t -> t = 3.75

t = 3.75

FRR = 0.75/5 = 0.15 = 15%

Gradient = a / 1 = 0.25 / 1 = 0.25  
0.02 = (W \* H) / 2, H = 0.25 \* W  
Therefore 0.02 = (W \* 0.25 \* W) / 2 = 0.125 \* (W ^ 2)  
W = sqrt(0.02 / 0.125) = 0.4  
Therefore t = 5 - 0.4 = 4.6  
FRR = 1.6 \* 0.25 = 40%

d) [10 Marks] What is the Crossover Error Rate of the system?

Crossover occurs when FAR=FRR

// this may be wrong, input appreciated

FAR = (t - 5) \* 0.5 (for 5<t<6)

FRR = (6 - t) \* 0.25 (for 5<t<6)

FAR = (t - 5) \* 0.5 = (6 - t) \* 0.25 = FRR

Solve for t = 5, ⅓

Therefore CER=FAR=FRR=(t-5)\*0.5 = 1/6 = 16.7%

FAR= (5 - t) \* 0.50

FRR= (t - 3) \* 0.25

Since FAR= FRR:

(5 - t) \* 0.50 = (t - 3) \* 0.25

t =4 ⅓

Therefore CER= (4 ⅓- 3) \* 0.25 = ⅓ or 33.33%

So the 5 is the FMR highest point and the 3 is the FNMR lowest?

Q14. [8 marks] Outline the structure of an X.509 version 3 digital certificate noting carefully

where the various names, keys and algorithms are; and which components are included in the hash, which components are signed, which key is used to create the signature and which key is used to verify the signature.

(Identical to 2009 exam question)

The structure of an X.509 v3 [digital certificate](http://en.wikipedia.org/wiki/Digital_certificate) is as follows:

* Certificate (This section is hashed then encrypted with the subject’s private key)
  + Version
  + Serial Number
  + Algorithm ID
  + Issuer
  + Validity
    - Not Before
    - Not After
  + Subject
  + Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  + Issuer Unique Identifier (optional)
  + Subject Unique Identifier (optional)
  + Extensions (optional)
* Certificate Signature Algorithm
* Certificate Signature

CA private key is used to encrypt hash of certificate, using the CA public key the signature can  
be decrypted to reveal the hash used to verify the certificate.

Ql5. [9 marks] Consider a language that consists only of the following symbols: A, B, C, D and

E. Examining large amounts of text in this language results in the following relative frequencies,

which we can interpret as probabilities:

A: 0.11

B: 0.25

C: 0.2

0: 0.05

E: 0.39

a) [5 marks) What is the Shannon Information per symbol in this language?

Calculate x \* (-log x / log2) for each value, return sum of values

0.11 \* (-log 0.11 / log2) + 0.25 \* (-log 0.25 / log2) + 0.2 \* (-log 0.2 / log2) + 0.05 \* (-log 0.05 / log2) + 0.39 \* (-log 0.39 / log2)

= 2.06

b) [4 marks] The following binary encoding scheme is used for the above language.

A = 11

B = 10

c = 011

D = 010

E=OO

What is the redundancy of this code (in bits per symbol)? Hint: Redundancy is defined as the

average symbol length minus the entropy.

Av = (2 + 2 + 3 +3 +2) / 5 = 2.4  
2.4 - 2.0608 = 0.3392 bits of redundancy