# **COMS3000 2015 Final Exam Answers**

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

## **Get more out of your study time. ~~Join UQAttic's revision chat.~~ UQCS’s Slack.**

#### [**Other exam papers**](https://docs.google.com/folder/d/0B6_D4T6LJ-uwYzY1YWMzNjYtMzUyZC00OTEyLWJlMjktOGExYWUwOTc4NDE3/edit)

### 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.

### To get editing permissions, simply go to the [chatroom](http://uqattic.net) and provide us with your Google Account address.

### **Style.**

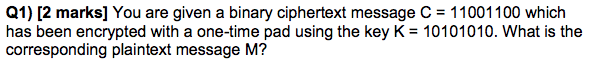
### Type answers in blue beneath each question.

### 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.

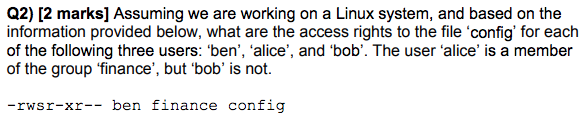
### If you want some extra explanation from someone else on their answer, highlight the other person's answer and repeat the procedure above.

### **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 prep tips. If you have your own IRC client, point it to irc.uqattic.net, port 6667, channel #attic.



0110 0110

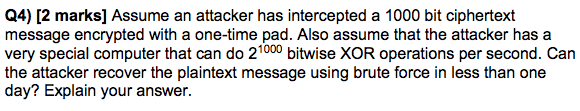


Ben: read, write, execute

Alice: read, execute as ben (SUID)

Bob: read





No. In fact, it is mathematically impossible to ever decrypt a one-time pad encryption in a finite amount of time using brute-force. I mean, you can't ever decrypt it with an infinite of time either. If my ciphertext was 3 characters long, I could have a pad that makes the message "yes" and a different pad that makes the message "nay".

A one-time pad cannot be decrypted. An attacker has an identical chance of randomly guessing the message than brute-forcing it. In mathematical terms, the amount of information the attacker gains by observing the ciphertext is 0 bits. You’re legit better off guessing what the target will say.

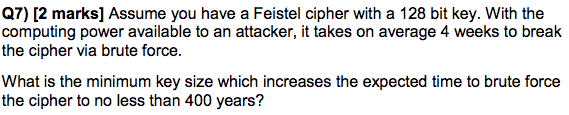
I will add that you will also see all intelligible English (if language used) as you guess the plaintext.



H(X) = - SUM Pi \* log2pi = -(1/10000 \* log21/10000) \* 10000

= 13.2877





You can calculate this directly by taking the log:

4 weeks is 0.07671 of a year (28 days / 365)

0.07671 \* 2x = 400

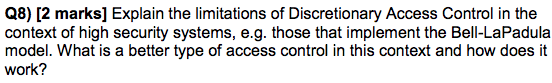
2x = 400 / 0.07671

log2 (400 / 0.07671) = x

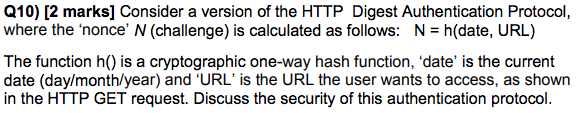
x = 12.3447

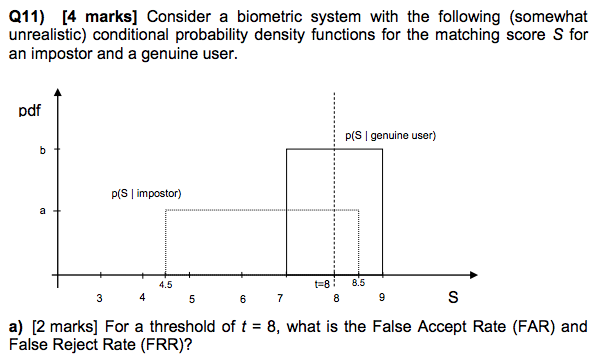
We round up, so x = 13 bits

Total key length = 128 bits + 13 new bits = 141 bits









You can calculate a and b using area under curve = 1 (total probability = 1)

a \* (8.5 - 4.5) = 1 / b \* (9 - 7) = 1

a = ¼ = 0.25 / b = 1/2

FAR = 0.5 \* a = 0.5 \* 0.25

= 0.125 (12.5%)

FRR = 1 \* b = 1 \* 0.5

= 0.5 (50%)



Equal Error Rate (EER) aka Crossover Error Rate / Crossover Accuracy

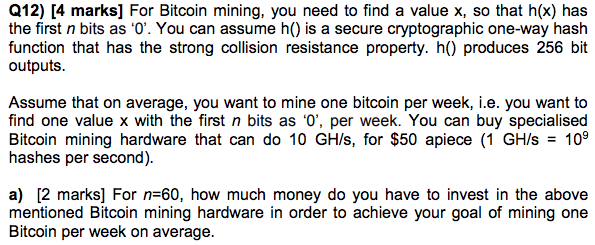
Error rate where FAR = FRR

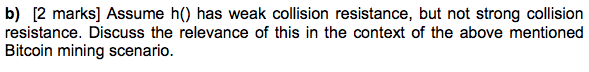
FAR = (8.5 - t) \* a = (8.5 - t) \* 0.25

FRR = (t - 7) \* b = (t - 7) \* 0.5

(t - 7) \* 0.5 = (8.5 - t) \* 0.25 (Solve for t)

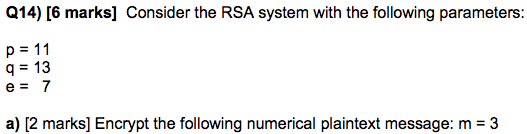
Threshold required for EER: t = 7.5 (25% FAR and FRR)







76 mod 11 = 4



C = m^e mod n  
C = 3^7 mod (p \* q)

C = 2187 mod (143)

C = 42



e \* d mod z = 1

Z = (p - 1) (q-1) = 120

7 \* d mod 120 = 1,

121 mod 120 is 1 so 121/7 = d

d has to be an integer

d = 103

7 \* 103 mod 120 = 721 mod 120 = 1



gcd(e, (p - 1) \* (q - 1)) must be 1

You could just punch a few numbers into your calculator, or bring in a factor table of the first couple hundred integers.

One possible solution is e = 13 -> gcd(13, 120) = 1







Revoke them by adding the certificate ID to the certificate revocation list of the issuing certificate authority.





(764 \* 74) mod 11 i think is what we want  
764 mod 11= (716  \* 74) mod 11  
(716) mod 11 = (78 \* 72) mod 11 = (9 \* 5) mod 11 = 1

764 mod 11 = (1 \* 3) mod 11 = 3

(764 \* 74) mod 11 = (3 \* 3) mod 11 = 9