# **COMS3000: 2015 exam answers**

**Q1) [2 marks] You are given a binary ciphertext message C = 11001100 which has been encrypted with a one-time pad using the key K = 10101010. What is the corresponding plaintext message M?**

11001100  
Xor

10101010  
-------------

01100110

M= 01100110

**Q2) [2 marks] Assuming we are working on a Linux system, and based on the information provided below, what are the access rights to the file ‘config’ for each of the following three users: ‘ben’, ‘alice’, and ‘bob’. The user ‘alice’ is a member of the group ‘finance’, but ‘bob’ is not.**

-rwsr-xr-- ben finance config

ben has read write execute

alice has read execute

bob has read.

wouldn’t bob also have write? since permission is elevated to owner? and noone can execute because small s?

^ SUID is set so the program will be run on ben’s permission (Small s means the execute is allowed). (verified for capital and lowercase s, lowercase grants execute to owner)

However this doesn’t change the the access rights of ben alice and bob, it just means that alice and bob will get ben’s access rights as well as their GID and UID access rights when running it ?

The set bit does not change the ‘subject’ / user permissions, correct.

**Q3) [3 marks] Discuss if and how cryptography can help achieve each of the 5 main aims of Information Security.**

The 5 main aims of Information security are:

* Confidentiality
* Integrity
* Availability
* Authenticity
* Non-repudiation

Cryptography helps achieving **confidentiality** by creating a ciphertext from a plain message, ensuring that only the sender & receiver know its content.

**Integrity & authenticity** can also be verified using public key encryption (e.g RSA), Alice calculates the hash of the file to send, then “signs” it by encrypting the hash with his private key, then sends both the file and the “signature” to Bob. Bob then proceeds to calculate the hash for the file and decrypt the signature with Alice’s public key. If the decrypted hash and calculated hash are the same then Bob can confirm that Alice sent the file and that it hasn’t been changed.

By extension if both Alice and Bob are sure that their private key is unique and secret then through the use of Trust certificates (e.g with the use of RSA) **Non-repudiation** is also ensured.

Cryptography can also be indirectly linked with **Availability** with the use of TKIP and CCMP in RSN making DoS harder to perform.

**Q4) [2 marks] Assume an attacker has intercepted a 1000 bit ciphertext message encrypted with a one-time pad. Also assume that the attacker has a very special computer that can do 2^1000 bitwise XOR operations per second. Can the attacker recover the plaintext message using brute force in less than one day? Explain your answer.**

Possible keys combinations = 2^1000

The computer can do 2^1000 bitwise XOR combinations in a second therefore it should take about a second to break the cypher.

Technically, you can recover all the possible plaintext within a day, however you don’t actually know which one is the one you’re looking for.

^ agreed. The question asks if the attacker can recover the plaintext message, which he can he just won't know which one is the correct one..

Given a pre-determined key K1 used to generate ciphertext C1, I’d say that ‘recovering’ the message means producing an M such that K1 xor M = C1, the attacker cannot do this, as they would not be able to give a single M to the person who knows K1 that would satisfy this. So I’d say they haven’t recovered the mes0 sage as such.

**Q5) [2 marks] What is the Entropy (Shannon Information) of a 4 digit decimal ATM PIN? You can assume all numbers are equally likely.**

Possible messages : 10^4

H(x) = -

H(x)

H(x) = log(10^4)/log2 = 13.28771238 ← Yes!

(hint: if your calculator does not have a log2 function, use the relationship: log2 x = log x/log2)

**Q6) [2 marks] Explain the goal and key idea of multi-factor authentication. Use a practical example.**

Authentication is the process of confirming someone's Identity, there are several method of authentication:

* Something you know (password,PIN)
* Something you have(smart card, door key)
* Something you are or do(Biometrics).

The idea of multi-factor authentication is that using a single of these methods can be easily tricked into authenticating an intruder (e.g Someone cracks your password or steals your key).   
Instead of using a single method of authentication, two or more are required to be granted access, allowing for reinforced security.

A common multi-factor authentication is using a password(something you know) and pseudo-random string generator key(something you have). To be able to access the system both must be correct.

**Q7) [2 marks] Assume you have a Feistel cipher with a 128**

**bit key. With the computing power available to an attacker, it takes on average 4 weeks to break the cipher via brute force. What is the minimum key size which increases the expected time to brute force the cipher to no less than 400 years?**

Number of possible Keys = 2^128  
Takes 1/12 of a year( on average) to break through 2^128 keys

we need 400/(1/12) = 4800 times the number of keys  
2^wanted number of bits= 2^128\*4800

wanted number of bits= log2(2^128\*4800) =140.22.. (can’t have 0.22.. of a key so round up)

We need at least 141 bits .

**Q8) [2 marks] Explain the limitations of Discretionary Access Control in the context of high security systems, e.g. those that implement the Bell-LaPadula model. What is a better type of access control in this context and how does it work?**

Discretionary Access Control (DAC) lets the owner decide access rights.  
It uses Unix criteria: Owner, group and other with read, write and execute privilege for each.   
This means that the principle of least privilege is not necessarily respected and it cannot prevent users from involuntarily or voluntarily share sensitive information.  
If Trudy is trying to gain access to a file F only Bob has access to she can write a programme to execute the following commands:   
- Create new file F1  
- Grant Bob write access to F1

-Grant trudy read access to F1

- Copy F into F1

then send the programme to Bob and tell him to execute it, once Bob executes the program she has access to the content of F.

In a system that implements the Bell-LaPadula model this would break the **no read up** and the **no write down** rule.

A better type of access control in this case would be Mandatory Access Control (MAC), where a system wide policy defines access to objects.  
Each file has a classification indicating its level of sensitivity and each user has a clearance level indicating which file he is allowed to access.

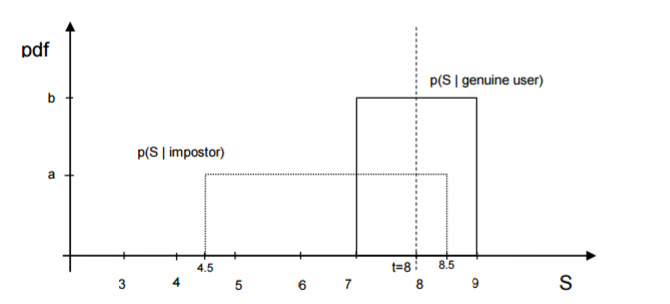
Moreover users and files have compartments to ensure that information is distributed on a “need to know” basis.

**Q9) [2 marks] Discuss the relative advantages and disadvantages of public key cryptography and secret key cryptography.**

Public key cryptography greatly simplifies the key distribution process (by directly publishing public keys) as well as allows for integrity authenticity and non-repudiation to be implemented directly into cryptography.  
 However it is computationally much more expensive to use Public key rather than private keys especially with large files.   
Private key cryptography makes the encryption process faster and easier however it relies entirely on the secrecy of the key, if the key becomes known the encryption is compromised.

**Q10) [2 marks] Consider a version of the HTTP Digest Authentication Protocol, where the ‘nonce’ N (challenge) is calculated as follows: N = h(date, URL) The function h() is a cryptographic one-way hash function, ‘date’ is the current date (day/month/year) and ‘URL’ is the URL the user wants to access, as shown in the HTTP GET request. Discuss the security of this authentication protocol.**

HTTP digest authentication protocol will be more secure than the basic authentication protocol which sends the id and password of the user in clear text.  
However this particular form of the HTTP digest authentication isn’t very secure, as the Nonce could be precalculated for a specific site on a specific day and would not actually be NONCE if two users where to access the same site on the same day (high probability of it happening).   
Therefore this system would be vulnerable to replay attacks and once the attacker (Trudy) figures out that the NONCE is only changing daily for every website she would be able to break the pre-image resistance of the hash function.

**Q11) [4 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] For a threshold of t = 8, what is the False Accept Rate (FAR) and False Reject Rate (FRR)?**

FRR =FNMR=(t-7) / (9-7) =½= 50%

FAR =FMR= 8.5-t / 8.5-4.5 = ⅛ = 0.125

**b) [2 marks] For what threshold t do we have the same probability of an impostor being accepted, as a genuine user being rejected? What is this probability called?**

The probability is called Equal Error Rate (EER) / Crossover Error Rate  
(t-7)/(9-7) = (8.5-t)/8.5-4.5

⇔ 2(t-7)=8.5-t

⇔ 2t -14 = 8.5-t

⇔ 3t = 22.5 ⇔ t = 7.5

**Q12) [4 marks] For Bitcoin mining, you need to find a value x, so that h(x) has the first n bits as ‘0’. You can assume h() is a secure cryptographic one-way hash function that has the strong collision resistance property. h() produces 256 bit outputs. Assume that on average, you want to mine one bitcoin per week, i.e. you want to find one value x with the first n bits as ‘0’, per week. You can buy specialised Bitcoin mining hardware a) [2 marks] For n=60, how much money do you have to invest in the above mentioned Bitcoin mining hardware in order to achieve your goal of mining one Bitcoin per week on average.**

Question is copy pasted wrongly (1 GH/s is actually = **10^9 not 109**)  
I recalculated with the correct value and result in 191 devices = 9550$ spent. Can anyone check? **yep**

Average hashes required = 2^n = 2^60

Average hashes per second = 1010

Time per collision = 2^60 / 10^10

Hardware required 60\*60\*24\*7 = 2^60 / (n \* 10^10)

n = 2^60 / (60\*60\*24\*7 \* 10^10) = 191

Total cost = 191 \* 50 = $9550 **YeP**

**b) [2 marks] Assume h() has weak collision resistance, but not strong collision resistance. Discuss the relevance of this in the context of the above mentioned Bitcoin mining scenario.**

Weak collision resistance is what we are trying to break, we know the format that h(x) must have and we are trying to find any possible x to match it.   
Strong collision resistance protects two distinct inputs from having the same hash value, if strong collision resistance is not maintained by h() then we can “cheat” to finding new bitcoins values with this hash function.  
Once we have found one bitcoin value we use the fact that h() does not have strong collision resistance to find the rest (computationally easier than breaking weak collision resistance again).

Also birthday paradox? 2^(n/2)?

As per the birthday paradox, the work factor is now 2^(n/2), so would only take (2^30/10^10) seconds, or under one second to mine one coin.

**Q 13) [2 marks] Compute the discrete logarithm of 4 to the base 7, if we are calculating modulo 11, i.e. log7 4 mod 11 =**

7^x mod 11 = 4

7^2 mod 11 = ~~3~~ 5

7^3 mod 11 = 2

7^4 mod 11 = 3

7^5 mod 11 = 10

7^6 mod 11 = 4 -> therefore log\_7 4 mod 11 = 6

**Q14) [6 marks] Consider the RSA system with the following parameters: p = 11 q = 13 e = 7**

**a) [2 marks] Encrypt the following numerical plaintext message: m = 3**

Encryption c= m^e mod n

n =p\*q = 143

c = (3^7)mod 143=42

**b) [2 marks] Find the corresponding decryption (private) key d.**

Decryption key = (n,d)

e\*d mod z =1

z = 10\*12 =120

7\*d mod 120 = 1 ⇔ d=103 (use your calculator to find the first multiple of 120 (+1)that can be divided by 7 (in this case 721%7 = 103))

Decryption key = (143,103)

**c) [2 marks] For the given values of p and q, find two additional valid encryption keys e.**

z = 120

e = 13 or e = 11

gcd(120,13) = 1, gcd (120, 11) = 1

**Q15) [3 marks] Explain how Public Key certificates are used in TLS/SSL. Explain their purpose**.

During The TLS handshake Public Key certificates are used to establish trust between the client and the server.

The server sends its public key and certificate chain to the client to prove that he is indeed the correct server.  
The public key certificates links the public key with an identity and ensures that both the parties are who they say they are.

The certificate should come as a certificate chains which starts with the server certificate at bottom of the chain and goes all the way up to a trusted third party, Certification Authority (CA), self signed root certificate ensuring that the party is trusted by the CA.

**Q16) [3 marks] Explain how cryptographic hash functions can be used to provide authentication and integrity for messages. Give an example where this is used.**

Authentication and integrity can be ensured by cryptographic hash functions can be used to provide authentication and integrity through the RSA protocol for instance.   
When sending a File to Alice, Bob first calculates the hash of the file then “signs” it by encrypting it. He then sends the file and the signature over to Alice.   
Alice Decrypts the signature and calculates the hash of the file, if the calculated hash and the decrypted signature are the same. then she knows for sure that bob sent the file and that it hasn’t been modified after he sent it.

**Q17) [2 marks] In a Public Key Infrastructure, how can you deal with the problem of leaked private keys?**

The Certificate Authority should be holding a Certificate Revocation List(CRL), when a private key is compromised, the public key is put on the CRL, When using a public key encryption it is the duty of the users to check the CRL to make sure the keys can be trusted.

**Q18) [3 marks] Discuss the differences between the Diffie-Hellman protocol and RSA.**

Diffie-Hellman protocol and RSA are fairly similar yet differ on different aspects,   
Diffie-Hellman is a method of sharing a private key securely within a public space, for later use in a symmetric encryption process.   
Whereas RSA generates a pair of public/private keys for use in asymmetric encryption

Also, Diffie-Hellman is vulnerable to MITM attack as it does not provide authentication.

Diffie-Hellman relies on a one way function, and cannot be used to directly secure data transmission, instead only serving the purpose of ensuring the secure (but vulnerable to MITM) generation of a shared secret. RSA relies on a trapdoor one way function, and can be used to directly secure data for transmission in addition to key exchange.

**Q19) [2 marks] Calculate (7^68) mod 11 = ?**

**How does this top one get to 9 when** 7^68 mod 11 =(7^32mod 11 \* 7^32 mod 11) mod 11 = 3? 7^68 = 7^(64+4) so 7^68 mod 11 = (7^64 mod 11\*7^4 mod 11) mod 11 = (3\*3) mod 11 = 9

68 = 1000100 = (2^2 + 2^6) = 4 + 64

7^68 mod 11 = 7^(4+64) mod 11

7^68 mod 11 = (7^2 + 7^6) mod 11

7^2 mod 11 = 5

7^6 mod 11 = 4

hence 7^64 mod 11 = (7^2 mod 11 \* 7^6 mod 11) mod 11 = 20 mod 11 = 9

wolframalpha checks out I agree with this solution

The relation they appear to have used in initial steps (verified independently as working):

Or

(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