ANSWER SHEET (DO NOT write in right hand column)

MODULE CODE:	**ELEC6242**	Student ID:	**31990401**	
Question number:	1a	This is page number:	1	of my answers

First, we need to count the length of the message, where L = 13 (without spaces)

Then we calculate how many times each letter occurs in the cipher text
E = 2
B = 2
O = 4
T = 3
N = 1
R = 1

Now we will apply the index of coincidence formula (Nx*Nx-1)/(L*L-1) + …
So, we have:

$$2\left(\frac{2\cdot 1}{13\cdot 12}\right)+\left(\frac{4\cdot 3}{13\cdot 12}\right)+\left(\frac{3\cdot 2}{13\cdot 12}\right)+2\left(\frac{1\cdot 0}{13\cdot 12}\right)$$

$$=2\left(\frac{2}{156}\right)+\frac{12}{156}+\frac{6}{156}+2\left(\frac{0}{156}\right)$$

$$=\frac{4}{156}+\frac{12}{156}+\frac{6}{156}=\frac{22}{156}=0{,}141$$

Thus, the index of coincidence is 0,141.

MODULE CODE:	**ELEC6242**	Student ID:	**31990401**	
Question number:	1b	This is page number:	2	of my answers

We can use textual steganography and hide our secret message by marking letters in a random text.

Let’s assume that the random text “c” is the following:

Bu**g** **o**n th**a**t **t**ranscript **t**ry **w**arning **o**thers

Our secret message is: Go at two
So, in order to hide this message in the c we just need to mark in each word the letter we want.

Bu**g** **o**n th**a**t **t**ranscript **t**ry **w**arning **o**thers

The c message will be transmitted and when the recipient receives it, he will just read the letters that make the secret message

MODULE CODE:	ELEC6242		Student ID:	31990401	
Question number:	1c	This is page number:		3	of my answers

In order to find the possible key length, we will use the Kasisky Test technique.

We need to find words that have been encrypted in the same way and then ensure that their difference is multiple of their length.

NOLRYPPZDAMLWERLJEGRC**NOL**RYPZZIQMOQKBPLNHAGOWLSRJPOLREGE

We can see NOL exist two times. NOL has a length of 3. The distance between the first NOL and the second one is 18 which is multiple of 3 (3*6 = 18).
Thus, the possible key length is 3.

MODULE CODE:	ELEC6242	Student ID:	31990401	
Question number:	1d	This is page number:	4	of my answers

x= 5/17

$x = \frac{5}{17} = 5 \cdot \frac{1}{17} \rightarrow$ 17 in Z_{23} is 19

So, $5 \cdot \frac{1}{17} = 5 \cdot 19 = 95 \bmod 23 = 3$ in Z_{23}

x = root (2)

$r^2 = x \bmod 23$

$r^2 = 2 \bmod 23$

$r = \sqrt{2} \bmod 23$

$r = 18$ as $r^2 = 18^2 \bmod 23 = 2$

However $-18 \bmod 23 = 5$

Thus there are two solutions $\rightarrow$ 18 and 5

x = 22^8

22 in Z23 is -1

Thus, 22^8 = (-1) ^8 = 1

We will first need to find all the points of the curve where a = 1 and b = 3.

For each x (from 0 to 16 as we are in Z17) we calculate the y^2. Then we convert this in Z17. If the result has a perfect square in Z17 then we take the point.

Thus, all the points of the elliptic curve are the following (they are calculated with the above formula):
(2,9) (2,8) (11,6) (7,8) (16,16) (8,9) (12,3) (3,13) (16,1) (6,2) (7,9) (12,14) (3,4) (11,11) (8,8) (6,15), O

As a result, the order of the curve is p - 1 = 17 – 1 = 16.
Due to the fact that the order is p-1 = 16 then the group is cyclic.
The generator was (12, 3) so if we calculate n * generator (n e (1, 16)) it will produce an all the distinct points of the curve.

MODULE CODE:	ELEC6242	Student ID:	31990401
Question number:	2b	This is page number: 6	of my answers

We need to find an i that if we calculate i * (16, 16) will give 12,4

$$2P = R = (x_R, y_R)$$
$$P = (x_1, y_1) = (16, 16)$$
$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 16^2 + 1}{2 \cdot 16} = \frac{769}{32} = \frac{4}{15}$$
$$\frac{4}{15} = 4 \cdot \frac{1}{15} = 4 \cdot 2 = 8 \mod 17$$
$$x_R = \lambda^2 - 2x_1 = 8^2 - 2 \cdot 16 = 32$$
$$y_R = -y_1 + \lambda(x_1 - x_R) = -16 + 8(16 - 32) = -144$$
$$2P = (15, 9)$$

If we use the same formula, we can calculate the 3P, 4P and by doing that we can find that 5P is the point which gives us (12, 14).

That means that i = 5 and 5*(16, 16) = (12, 14)

MODULE CODE:	ELEC6242		Student ID:	31990401
Question number:	2c	This is page number:	7	of my answers

$2P = 2(16,16)$

$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 16^2 + 1}{2 \cdot 16} = \frac{769}{32} = \frac{13}{8}$

$\frac{13}{8} = 13 \cdot \frac{1}{8} = 13 \cdot 15 = 195 \mod 17$

$x_R = \lambda^2 - 2x_1 = 195^3 - 2 \cdot 16 = 37993$

$y_R = -y_1 + \lambda(x_1 - x_R) = -16 + 195(16 - 37993) = -7405531$

so $2P = (8,2)$

$3P = 2(8,2)$

$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 8^2 + 1}{2 \cdot 2} = \frac{193}{4} = \frac{3}{13}$

$\frac{3}{13} = 3 \cdot \frac{1}{13} = 3 \cdot 4 = 12 \mod 17$

$x_R = \lambda^2 - 2x_1 = 12^2 - 2 \cdot 8 = 144 - 16 = 128$

$y_R = -y_1 + \lambda(x_1 - x_R) = -2 + 12(8 - 128) = -1442$

So $3P = (2,6)$

$4P = 2(2,6)$

$\lambda = \frac{3 \cdot 2^2 + 1}{2 \cdot 6} = \frac{13}{12} = \frac{4}{10}$

$\frac{4}{10} = 4 \cdot \frac{1}{10} = 4 \cdot 12 = 48 \mod 17$

$x_R = 48^2 - 2 \cdot 2 = 2304 - 4 = 2300$

$y_R = -6 + 48(2 - 2300) = -110310$

So $4P = (7,6)$

MODULE CODE:	ELEC6242	Student ID:	31990401
Question number: 2c	This is page number: 8	of my answers	

$5P = 2(7,6)$

$\lambda = \frac{3 \cdot 7^2 + 1}{2 \cdot 6} = \frac{3 \cdot 49 + 1}{12} = \frac{148}{12} = \frac{10}{10}$

$10 \cdot \frac{1}{10} = 10 \cdot 12 = 120 \bmod 17$

$x_R = 120^2 - 2 \cdot 7 = 14400 - 14 = 14386$

$y_R = -6 + 120(7 - 14386) = -1723326$

So $5P = (13, 8)$

$6P = 2(13, 8)$

$\lambda = \frac{3 \cdot 13^2 + 1}{2 \cdot 8} = \frac{508}{16} = \frac{8}{16}$

$\frac{8}{16} = 8 \cdot \frac{1}{16} = 8 \cdot 16 = 128 \bmod 17$

$x_R = 128^2 - 2\,13 = 16384 - 26 = 16358$

$y_R = -8 + 128(13 - 16358) = -2092168$

So $6P = (13, 7)$

The multiplicative inverse of 13 in Z_{17} is 4

Finally $x^{-1} \cdot C_2 = 4^{-1} \cdot 13 = \frac{13}{4}$

MODULE CODE:	ELEC6242		Student ID:		31990401
Question number:	2d	This is page number:		9	of my answers

We are going to use the Hasse's theorem where:

||E(F(q)|-(q+1) |<2root(q) → -2sqrt(q) + q + 1 <= E(fq) <= 2sqrt(q) + q + 1

If we apply the numbers of our curve the minimum number of points, we can find on this curve is:

9,7 <= E(Fq) <= 26

MODULE CODE:	ELEC6242	Student ID:	31990401

Question number:	3a	This is page number:	10	of my answers

This is a columnar transposition cipher.

The cipher length is 20 so the key length could be a divisor of 20 (1, 2, 4, 5).

We will try to produce tables according to the possible key lengths.
So, the first table will have 1 column and 20 rows the second one 2 columns and 10 rows, the third one 4 columns and 5 rows and so on.

If we use the key length 5, we can see that we have the following table (5 columns and 4 rows):

1	2	3	4	5
A	Y	H	O	U
N	V	I	E	F
M	A	Y	L	L
T	A	I	D	E

If we rearrange the columns as 2, 4, 5, 3, 1

2	4	5	3	1
Y	O	U	H	A
V	E	F	I	N
A	L	L	Y	M
A	D	E	I	T

and read the table horizontally we can see that we can deduce the plaintext which is “YOU HAVE FINALLY MADE IT”. Thus, the key length is 5 and the key is “BDECA”

MODULE CODE:	ELEC6242	Student ID:	31990401

Question number:	3b	This is page number:	11	of my answers

The system that is described is the AES ECBC. This encryption technique is not semantically secure because ECB-encrypted ciphertext can leak information about the plaintext (even beyond its length, which all encryption schemes accepting arbitrarily long plaintexts will lead to some extent).

The problem with ECB mode is that encrypting the same block of 128 bytes of plaintext using ECB mode always yields the same block of ciphertext.
This can allow an attacker to detect whether two ECB-encrypted messages are identical, or to detect whether two ECB-encrypted messages share a common prefix or to detect whether two ECB-encrypted messages share other common substrings, as long as those substrings are aligned at block boundaries or to detect whether a single ECB-encrypted message contains repetitive data

MODULE CODE:	ELEC6242	Student ID:	31990401

Question number:	3c	This is page number:	12	of my answers

1. Correct
2. Wrong (AES128 will not be secure as 128bits will become 64, but AES256 will be as 256 bits will become 128)
3. Wrong (there are cbc attacks where we can find the cipher text and the key can be the same)
4. Wrong (Elgamal uses discrete logarithm, it is not a trap door function)
5. Correct (cpm perfect secrecy explains how good an algorithm is. However, if the cryptosystem is bad, we can perform timing attack)
6. Wrong (we can have more points in the curve)
7. Wrong (We can find all the bits. It's difficult but not impossible)
8. Correct (it is easier to find collisions)
9. Wrong (the probability must be >= 50…so it can be 70 or 65…not exactly 80. Could also be more than 80)