Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

March 19, 2019

Cryptography & Encryption:6G7Z1011 : Introduction

1 Cryptography & Encryption:6G7Z1011 : Introduction

1.0.1 ⇝:

Please complete all lab question before next week. In this first week I need to assess how well you can all code and adjust the depth and number of questions accordingly.
You do not need to know much Java to complete this unit, and I can not suppose you have meet Java at all. The concepts that I will use most frequently are the following:

1. the if statement;
2. the for loop;
3. arrays (and their traversal)
4. methods;
5. functions

You may know Java already but I can not assume this (you have a wide range of academic backgrounds) so I will introduce Java with some simple questions.

1.1 problem:initilization

⌜ Declare and initialize a string an integer and a float. ⌟

1.2 problem:

⌜Write a method that takes two strings and returns the length of the largest string. ⌟

1.3 problem:

⌜Write a method that takes two three strings and returns the length of the largest string. ⌟

1.4 problem:

⌜Write a method that takes two integers and returns true if and only if the first integer divides the second integer. ⌟

1.5 problem:getting used to arrays

⌜ Declare and initialise two arrays of integers a and b of the same size. Populate them with some data:

$$a = \boxed{2}\boxed{3}\boxed{32}\boxed{54}\boxed{32}\boxed{156} \tag{1}$$

$$b = \boxed{12}\boxed{43}\boxed{12}\boxed{15}\boxed{62}\boxed{-6} \tag{2}$$

Write Java code that compares each element of a with its equivalent element in b and prints the value of the largest. For example, the code would print 12 (because $12 > 2$), 43 (because $43 > 3$), 32 (because $32 > 12$) and so on.

⌟

1.6 problem:

⌜Write a Java function that takes as an argument an array of integers and returns the array but in the reverse order. For example if you pass it a in eqn. 1 it will return

$$\boxed{156}\boxed{32}\boxed{54}\boxed{32}\boxed{3}\boxed{2} \tag{3}$$

⌟

1.7 problem:

⌜Write a Java function that takes as an argument an array of integers and returns the largest element of the array.

⌟

1.8 problem:conversion between type

⌜Write Java Code that takes a String, converts it into an array of characters, and then prints out the ASCII value of each character. ⌟

1.8.1 ⇝:

Some cryptography.

1.9 problem:Caesar cipher

⌜Write a Java program Caesar.java that implements the Caesar cipher. Declare two character arrays p for plain text and c for cipher text let the key equal 4 (so we push on by four) then

$$p = \boxed{\text{‘c’}}\boxed{\text{‘a’}}\boxed{\text{‘t’}}\boxed{\text{‘s’}}\boxed{.}\boxed{.} \tag{4}$$

$$c = \boxed{\text{‘g’}}\boxed{\text{‘e’}}\boxed{\text{‘x’}}\boxed{\text{‘w’}}\boxed{.}\boxed{.} \tag{5}$$

⌟

1.10 problem:

⌜The Caesar cipher is not used in real world applications; it is too easy to crack. Write Java code that ‘cracks’ the Caesar cipher (implicit here is that you have no knowledge of the key used to encrypt the data), you crack it by running all possible keys on the encrypted message until you get a message that you can read. ⌟

1.11 problem:counting primes

⌜Write Java code that will print all the prime numbers between 2 and 2000, how many are there? ⌟
Cryptography & Encryption:6G7Z1011 : Simple Ciphers , Statistical Analysis and $\mathbb{Z}(n)$

2 Cryptography & Encryption:6G7Z1011 : Simple Ciphers , Statistical Analysis and $\mathbb{Z}(n)$

2.1 Caesar Cipher, Symmetric Cipher

The Caesar cipher, the affine cipher and the symmetric cipher are all attackable by statistical analysis.

2.2 problem:statistical analysis

⌜ Write a Java program that statistical analyses a long paragraph taken from an online document:

1. Store the paragraph as a Java String.
2. Using the split function place the string into array that contains the words of the string.
3. Split each word into an array of characters.
4. Run through the character array incrementing a counter each time it meets a particular letter.

For example

'code snippet'

```
String sentence="the cat sat on the mat";
int charoccurs[]=new int [26];
// charoccurs[0] = 3
// as 'a' occurs three times in sentence
```

⌟

2.3 problem:affine cipher

⌜We showed that the affine cipher only worked for particular key pairs.

1. Pick a legitimate key pair and let $e(i)$ denote the encryption of i. Print out the encrypted values of $e(0), e(1), \ldots e(25)$. Note there should be 26 different number printed out.
2. Pick an illegitimate key pair and print out the encrypted values of $e(0), e(1), \ldots e(25)$. Note there will be duplications.

⌟

2.4 problem:

⌜ Determine those elements of $\mathbb{Z}(26)$ that have a multiplicative inverse (hint, there are seven) ,and in each case state what the inverse is.
⌟

2.5 problem:

⌜ Write a JAVA program that takes two integers and returns true if and only if they are relatively prime. ⌟

2.6 problem:

⌜ Write a JAVA program that prints out the Euler ϕ function for the first 1000 integers. ⌟

2.7 problem:

⌜This is not an encryption question, it is a utility question (that is it performs a simple task of use to us in this unit).

1. Write a JAVA program that opens a file, say data.txt, and reads it line by line into an array of Strings. That is, array element zero contains the first line of the file, array element one contains the second line of the file, and so on.

2. Close the file.

3. Loop over the array and print out each line.

⌟

2.8 problem:

⌜ Write a JAVA program that prints out a file consisting of two columns. The first column is a list of the integers from 1 to 1000 and the second column is the number of prime numbers found up to that point. For example, consider 10 then 2, 3 5, 7 are the primes less that or equal to 10 so the file entry is

$$\begin{array}{ll} 9 & 4 \\ 10 & 4 \\ 11 & 5 \\ 12 & 5 \\ 13 & 6 \\ 14 & 6 \\ & . \end{array} \tag{6}$$

Using MATLAB (or visualisation software of your choosing) plot column one against

$$\frac{\text{column one}}{\text{column two}} \tag{7}$$

(that is we are plotting the density of the primes).
Any thoughts?
⌟
Cryptography & Encryption:6G7Z1011 : Euclid, and the Fast Powering Algorithm

3 Cryptography & Encryption:6G7Z1011 : Euclid, and the Fast Powering Algorithm

3.0.1 ☞:

Please code the following in JAVA.

a	b	c
d	e	f
g	h	i

first string

j	k	l
m	n	o
p	q	r

second string

Table 1: The encryption involves making the first row the first column, the second row the second column and the third row the third column.

a	d	g
b	e	h
c	f	i

first string encrypted

j	m	p
k	n	q
l	o	r

second string encrypted

Table 2: Encrypting the array strings, the rows become columns.

3.1 problem:Introduction to Blocks

⌜ This problem introduces some of the ideas used in the DES algorithm which we will meet later.

1. Create a string with some plain text in, we will use the plain text 'abcdefghijklmnopqr'
2. Split the string into an array of strings, each string in the array being of size n^2, in our example $n = 3$ so we are slitting on 9.
3. Write each string in the array into a $n \times n$ matrix.
4. Encrypt each matrix as shown in table 2.
5. Write out the encrypted string, in the example this is 'adfbehcfijmpknqlor'.
6. Write the decryption algorithm

For example if the string is 'abcdefghijklmnopqr' and $n = 3$ then the array has two elements:

1. the first is 'abcdefghi'
2. the second is 'jklmnopqr'.

Store each string in the array in a square array of size $n \times n$ so we have the situation in table 1. Encrypting each string gives table 1, and the strings are joined to give the encrypted message 'adfbehcfijmpknqlor'. ⌟

3.2 problem:Euclid

⌜Code Euclid's algorithm in JAVA. Fix a large integer a and let $1 \leq b \leq a$. Plot b against the number of divisions required to evaluate $\gcd(b, a)$, and overlay the function from the notes to see how well they agree. ⌟

3.3 problem:Fast Power

⌜ Evaluate, on paper first if you wish, using the fast powering algorithm

$$x = 3^{123456} \mod 17 \tag{8}$$

⌟

3.4 problem:

⌜Find all the solutions to

$$x^2 + x = 1 \mod 19 \quad \text{and} \quad 11^x = 21 \mod 71. \tag{9}$$

There is no need to construct a fast algorithm, any algorithm that works is fine. ⌟

3.5 problem:

⌜Looking ahead, we need some ideas from the theory of matrices. I am sure you have all meet matrices before, they are simply square arrays of numbers. For now, write code that takes two 3×3 matrices matrices and evaluates their product. ⌟

3.6 problem:

⌜Solve the above problem by creating a function that takes two matrices and returns (if possible) their product. ⌟
Cryptography & Encryption:6G7Z1011 : Mathematical Structures and a First Look at Diffie

4 Cryptography & Encryption:6G7Z1011 : Mathematical Structures and a First Look at Diffie

4.0.1 ☙:

We do some calculations with groups. Recall that the permutation group S_n has $n!$ elements (for example S_{10} has $10 \times 9 \times 8 \cdots \times 1$ elements) then you realise how fast S_n grows as a function of n.

4.1 problem:

⌜This was a homework question, but it is important so we look at it here. Let p denote a $p$lain text message then $A(p)$ is to be read A acts on p, and

$$e = A(p) \tag{10}$$

is the resulting encrypted message. One of the easiest examples of this is letting A be a matrix. If we consider the 2×2 case we have

$$\overbrace{\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}}^{e} = \overbrace{\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}}^{A} \overbrace{\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}}^{p} \tag{11}$$

The important point to note is that if we wish to use A as an encryption technique we need to ensure A^{-1} the inverse of A exists. In the following p and e are real vectors of length 2 and any matrix is 2×2.

1. Write a Java method that takes two arguments: a matrix A and a plain message p, and returns the encrypted message e.

2. Write a Java method that takes one argument: a matrix A and returns, if it exists, A^{-1}.

⌟

4.2 problem:

⌜ Prove directly by hand calculation and by writing Java code that the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{12}$$

form a group of order four. It is abelian. ⌟

4.3 problem:

⌜Prove by writing Java code that S_3 is a group, you need to think how best to represent S_3 in a Java class.

⌟

4.4 problem:

⌜ Prove directly by hand calculation and by writing Java code that the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \tag{13}$$

form a group. Note : $i^2 = -1$, so you need to be able to multiple complex numbers together in your calculation. The matrices form a group of order eight, it is non-abelian. ⌟

4.5 problem:

⌜This is a bit of a challenge, can you describe the multiplication table of the permutation group S_4, note it has 24 elements.

⌟

4.6 problem:

⌜A subset S of a group G is termed a *subgroup* of G is S is itself a subgroup. Find an example of a subgroups in each of the following groups:

1. S_3
2. S_4

⌟

4.7 problem:mod functions

⌜ Consider the function $y = 627^x \mod 941$ on the x range $[0, 941]$. Sketch — if you can — what you think the function looks like. Save the function points to a file and plot it in Excel, Matlab (software of your choice). What do you deduce?

⌟

4.8 problem:groups

⌜Read the definition of a group. Determine if the following are groups; if they are a group state if they are abelian and what the unit element 1 is.

1. The set of real numbers under addition.
2. The set of all natural numbers $\{1, 2, 3 \ldots\}$ under addition.
3. The set of all 2×2 matrices under addition.
4. The set of all 2×2 matrices under multiplication.

⌟

4.9 problem:finite fields

⌜The condition of being a field is more restrictive than being a group. We will show in a later lecture that for p prime and n a positive integer there is one and only field of size p^n. An example will illustrate, let $p = 3$ and $n = 2$. Recall a field has both addition and multiplication. Let

$$F = \mathbb{Z}(3) \times \mathbb{Z}(3); \tag{14}$$

that is each element (x, y) in F is such that $x, y \in \mathbb{Z}(3)$. Define addition in the obvious way

$$(x_1, y_1) +_F (x_2, y_2) = (x_1 +_{\mathbb{Z}(3)} x_2, y_1 +_{\mathbb{Z}(3)} y_2), \tag{15}$$

and multiplication in the (much less obvious way)

$$(x_1, y_1) \times_F (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \mod 3. \tag{16}$$

Prove this is a field of size nine, do it on paper and as a Java class. ⌟

4.10 problem:Diffie

⌜ We implement Diffie with some real data. We work on the Java Implementation of the Diffie-Hellman protocol. We will use small prime numbers — if a question asks you to verify something you are free to use a brute force attack. And you will need to be able to write a fast-powering algorithm.

1. Let $p = 941$ (prove 941 is prime), we let $g = 237$.
2. Suppose Alice chooses a secret key $a = 347$ what is A?
3. Suppose Bob chooses a secret key $b = 781$ what is B?
4. What is the value of A'?
5. What is the value of B'?

Of course A' and B' should agree, what is their shared value? ⌟
Cryptography & Encryption:6G7Z1011 : Coding Diffie

5 Cryptography & Encryption:6G7Z1011 : Coding Diffie

5.1 problem:Diffie

⌜ We implement Diffie with some real data. We work on the Java Implementation of the Diffie-Hellman protocol. We will use small prime numbers — if a question asks you to verify something you are free to use a brute force attack.

1. Let $p = 941$ (prove 941 is prime), we let $g = 237$.
2. Suppose Alice chooses a secret key $a = 347$ what is A?
3. Suppose Bob chooses a secret key $b = 781$ what is B?
4. What is the value of A'?
5. What is the value of B'?

Of course A' and B' should agree what is their shared value? ⌟

5.2 problem:mod functions

⌜ Consider the function $y = 627^x \mod 941$ on the x range $[0, 941]$. Sketch — if you can — what you think the function looks like. Save the function points to a file and plot it in Excel, Matlab (software of your choice). What do you deduce?
⌟

5.3 problem:

⌜Start your assignment. ⌟
Cryptography & Encryption:6G7Z1011 : The RSA Algorithm

6 Cryptography & Encryption:6G7Z1011 : The RSA Algorithm

We discuss the most widely used public key encryption algorithm

6.1 the RSA algorithm

The usual notation is in place: for example, $K_{B,Pr}$ is a key belonging to Bob and it is private, and $K_{B,Pu}$ is a key belonging to Alice and it is public, and p, q are prime numbers.

1. Bob picks two primes p and q (p, $q > 2^{1000}$) evaluates $N = pq$ and picks an encryption exponent e, where e satisfies
$$\gcd(e, (p-1)(q-1)) = 1. \tag{17}$$
2. Bob's public key is the tuple (that is, it is a pair of numbers) $K_{B,Pu} = (N, e)$
3. Alice has a plaintext message m (m an integer) and evaluates
$$c = m^e \mod N, \tag{18}$$
c is the ciphertext sent to Bob.
4. Bob solves
$$ed = 1 \mod (p-1)(q-1). \tag{19}$$
The only term in eqn. 19 that Bob does not know is d.

5. Bob evaluates
$$m' = c^d \mod N \tag{20}$$
and we find $m = m'$.

7 Problems & Supplementary Material:Problems

7.1 problem:

⌜Consider the field $\mathbb{F}_{17}$ then $\mathbb{F}_{17}^*$ is a group of order 16.

1. Using JAVA determine the subgroups generated by each single element of $\mathbb{F}_{17}^*$ and in each case verify that the order of the group generated by the element divides 16.
2. Recall those elements of $\mathbb{F}_{17}^*$ that generate the entire group are termed primitive; what are the primitive elements of $\mathbb{F}_{17}^*$. Hint : 2 is not a primitive root, but 3 is a primitive root.

⌟

7.2 problem:

⌜Write Java code that implements the RSA algorithm, check it works by running it with the following data.

1. Let Bob pick two primes $p = 1223$ and $q = 1987$, what is the value of $N = pq$. [Answer: $pq = 2430101$.]
2. Bob picks an exponent $e = 948047$, check that $\gcd(e, (p-1)(q-1)) = 1$ and his public key is the tuple $K_{B,Pu} = (N, e)$
3. Alice's plaintext message is $m = 1070777$
4. Alice encrpyts m to
$$c = m^e \mod N; \tag{21}$$
c is sent to Bob.
5. Bob solves for d in
$$ed = 1 \mod (p-1)(q-1) \tag{22}$$
6. Bob evaluates
$$m'c^d \mod N \tag{23}$$
and,if it has all worked, $m = m'$

⌟

7.3 problem:Lagrange

⌜ Let S_3 denote the permutation group on three objects, and let $H = \langle (1,2,3) \rangle$ denote the subgroup generated by the permutation $(1,2,3)$. Find a decomposition of S_3 into cosets of the form $G = \sqcup_{a \in G'} Ha$ where G' is some subset of G.
⌟

7.4 problem:Properties of ϕ

To get you thinking.

1. What is $\phi(p)$ for p prime?
2. Prove $\phi(p^i) = p^{i-1}(p-1)$
3. Verify directly $\phi(15) = \phi(3)\phi(5)$

7.5 problem:

⌜Consider $\mathbb{F}_2 = \{0, 1\}$ and let $GL(2, \mathbb{F}_2)$ denote the set of invertible matrices of size 2×2 with entries from $\mathbb{F}_2$. Show that $GL(2, \mathbb{F}_2)$ is a group. $GL(2, \mathbb{F}_2)$ is isomorphic to a group we have meet before —which one?
⌟

7.6 problem:primes

⌜ The RSA algorithm depends on certain properties of the primes. Answer the following questions:

1. Are there an infinite number of primes? If you think there are can you prove it?
2. A prime of the form $2^n - 1$ is called a *Mersenne prime*, for $1 \leq n \leq 10$ determine if $2^n - 1$ is prime.
3. Are there an infinite number of Mersenne primes?
4. If n is even and $n > 2$ prove $2^n - 1$ is not prime.
5. If $3 \mid n$ and $n > 3$ then prove $2^n - 1$ is not prime.

⌟

7.7 problem:

⌜Continue with your assignment. ⌟
Cryptography & Encryption:6G7Z1011 : Digital Signatures, and Introduction to Collision Algorithms

8 Cryptography & Encryption:6G7Z1011 : Digital Signatures, and Introduction to Collision Algorithms

9 Problems & Supplementary Material:Problems

9.1 problem:iterative solution

⌜We present an iterative way of solving (certain types of equations). Suppose we wished to solve $x^3 - x - 1 = 0$ on $[1, 2]$. The fixed point iteration requires

$$f : [1, 2] \to [1, 2], x \mapsto f(x) = (1 + x)^{1/3} \tag{24}$$

The idea being if $x = f(x)$ we have a fixed point. Write a Java method that takes a starting point x_1 and finds the solution to $x^3 - x - 1 = 0$ to four decimal places. To commence let $x_1 = 1.1$
⌟

9.2 problem:Digital Signatures

⌜Code the RSA Digital Signature algorithm in JAVA.

1. Sam picks two primes $p = 1223$ and $q = 1987$; check they are prime. Evaluate

$$N = p.q = 1223.1987 = 2430101. \tag{25}$$

2. Sam picks a verification exponent $v = 948047$ check

$$\gcd(v, (p-1)(q-1)) = 1 \tag{26}$$

3. Sam's signing key is the s that solves

$$sv = 1 \mod (p-1)(q-1); \tag{27}$$

find s (you should get $s = 1051235$.)

4. Suppose the document is $D = 1070777$ then the signed document is

$$S = D^s \tag{28}$$

Sam makes S (the signed document), D (the actual document) and v (the verification exponent) and N available.

5. Victor has access to N, v, S and D, Sam evaluates

$$S^v \mod N, \tag{29}$$

and it should equal D.

⌟

9.3 problem:Probability and Combinatorics

⌜

1. How many different seven letter words can be formed from the symbols A, B and C?
2. Using the seven letters A, A, A, A, B, B, B how many different words of length seven can be formed?
3. A fair coin is flipped six times, find the probability that:
   1. The result is six heads.
   2. Exactly one head occurs.
   3. There are the same number of heads as there are tails.
   4. A *n-sequence* is when the same result (head or tail) turns up n-times so HHHTHT contains a 3-sequence of heads. What is the probabilty that no sequence of length 2 or greater occurs in the six flips?

⌟

9.4 problem:

⌜Continue with your assignment. ⌟
Cryptography & Encryption:6G7Z1011 : Elliptic Cryptography & Quantum Encryption

10 Cryptography & Encryption:6G7Z1011 : Elliptic Cryptography & Quantum Encryption

11 Problems & Supplementary Material:Elliptic Curves

11.1 problem:

⌜ Write a java method that finds the solutions of

$$ax^2 + bx + c = 0; \tag{30}$$

the method should take three arguments a, b and c. ⌟

11.2 problem:

⌜ Write a java method that finds the solutions of

$$ax^3 + bx^2 + cx + d = 0; \tag{31}$$

the method should take four arguments a, b, c and d. Hint
`https://en.wikipedia.org/wiki/Cubic_function#General_formula`.
⌟

11.3 problem:

⌜Find all the solutions to

$$y^2 = x^3 + 3x + 8 \mod \mathbb{F}_{13} \tag{32}$$

That is each (x, y) solution is an element of $\mathbb{F}_{13} \times \mathbb{F}_{13}$ and it satisfies eqn. 32, for example $(2, 3)$ is a solution. You should find eight answers, see §11.4 ⌟

11.4 problem:

⌜The eight solutions from §11.3 are shown in table 3, if we append an identity element 0 the nine elements can be given an abelian group structure. Formally you are creating

$$\text{Ellip}(y^2 = x^3 + 3x + 8, \mathbb{F}_{13}); \tag{33}$$

the abelian group associated with $y^2 = x^3 + 3x + 8$ and the field $\mathbb{F}_{13}$. Using the algorithm in the notes evaluate the group table.
⌟

11.5 problem:$\mathbb{F}_{3^2}$

⌜Construct the field $\mathbb{F}_{3^2}$ The following matrices are a field of cardinality nine over $\mathbb{Z}(3)$

$$\begin{aligned}
a &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}, \\
d &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}, \\
g &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad h = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}, \quad i = \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}.
\end{aligned} \tag{34}$$

⌟

11.6 problem:

⌜Continue with your assignment. ⌟

	0	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
0									
$(1,5)$									
$(1,8)$									
$(2,3)$									
$(2,10)$									
$(9,6)$									
$(9,7)$									
$(12,2)$									
$(12,11)$									

Table 3: The points all lie on $y^2 = x^3 + 3x + 8$ over the field $\mathbb{F}_{13}$. Using the ideas of the lecture can you complete the table to create an abelian group of order 9?

$\times$	b	c	d	e	f	g	h	i
b								
c								
d								
e								
f								
g								
h								
i								