1. [12%] What will be shown in the “Message Box” on the screen after the following Visual Basic (VB) code segment executes? Please explain briefly.

```vbnet
Sub Main()
    MsgBox(myfun(21, 6))
End Sub

Function myfun(ByVal a As Short, ByVal b As Short)
    If a = b Then
        myfun = b
    Else
        myfun = myfun(a Mod b, b / 2)
    End If
End Function
```

Answer: 3

Explanation: Call # 1 has arguments 21, 6; a is not equal to b so the function gets called with arguments 21 mod 6 = 3 and 6/3 = 3. Returns on the next call as a is now = b

2. [10%] What is the message on the screen after the following VB code segment executes? Please explain briefly.

```vbnet
Public Class Obj
    Public v As Integer
    Public before As Obj
    Public after As Obj
End Class

Sub Main()
    Dim a As New Obj() : Dim b As New Obj()
    Dim c As New Obj()
    a.v = 3 : b.v = 5 : c.v = 7
    a.before = b : a.after = a.before
    MsgBox(a.after.v)
```
Answer: 5

Explanation: a after becomes the object b; b.v is the number 5.

3. [10%] What will be the result of the following Matlab (ML) commands:

```matlab
>> A=[linspace(-1,7,5); 2:6];
>> (A>3).*A
```

```
ans =
   0     0     5     7
   0     0     4     5     6
```

Explanation: A is initially
```
-1     1     3     5     7
2     3     4     5     6
```
The second command selects only elements > 3, sets the rest to 0

4. [12%] Given the ML function file “test.m” that contains:

```matlab
function [a]=test(b,c)
a=b^c;
b=b+2;
```

What is the result of the following ML commands? Please explain your answer briefly.

```matlab
>> b=4; c=2; a=1;
>> test(b,c)+ b + a
```

```
ans =
   21
```

Explanation: Within function, a is \(4^2 = 16\); once we return to calling program, the values of a, b and c in the function are irrelevant; the answer is

\[16 + 4 + 1 = 21\]
5. [12%] What is the result of the following ML commands? Please explain your answer briefly.

```
>> j = 3 > 2;
>> for i = 1:6
    j = j-1;
end
>> j
```

```
ans = -5
```

Explanation: Since $3 > 2$ the initial value of $j$ is 1; the loop is executed 5 times, resulting in a net value for $j$ of -5.

6. [10%] What is the result of the following ML commands? Please explain your answer briefly.

```
>> syms x t
>> diff(limit(x^2+t*x+1,t,0))
```

```
an = 2*x
```

Explanation: Taking symbolic limit of $x^2 + tx + 1$ as $t \to 0$ we get $x^2+1$.
Differentiating we get the symbolic expression “$2x$”.

7. [9%] Explain briefly (in 2-3 sentences) what an "NP-complete" problem is and give one example of such a problem.

Class of problems that are not mathematically proven to be "bad" (intractable), but for which the best known algorithms are in exponential time. Nondeterministic Polynomial time problems can be solved in polynomial time with the help of "magic coin" to guide solution.

Classic NP-complete problems: TSP, Timetable, Bin-packing

4/13 lecture, slides 8, 11
8. [5%] Is factoring large integers an NP-complete problem?

No; it is hard but not NP-complete (4/13 lecture, slide 21)

9. [15%] Explain as best as you can how RSA “public key” cryptography works:

Choose two prime numbers $p \neq q$ randomly and independently of each other. Compute $N = p \cdot q$
Choose an integer $1 < e < N$ which is relatively prime to $(p-1) \cdot (q-1)$.
Compute $d$ such that $\text{mod}(d \cdot e, (p-1) \cdot (q-1)) = 1$
Destroy all records of $p$ and $q$.

Encode using $C = \text{mod}(M^e, N)$

Decode using $M = \text{mod}(C^d, N)$

In decoding, one avoids exponentiation by taking successive “mod” operations

(4/22 Lecture)

10. [5%] Describe the main elements of a Turing machine:

The machine has a number of possible internal “states” and reads from a “tape” one character at a time. Depending on the internal state and the character read, it may (a) write back a character, (b) change state and then one of:

- moves to the left
- moves to the right
- halts (stops)

(4/13 Lecture)