2011 Paper 6 Question 1

Complexity Theory

The following is a quotation from an Internet forum on cryptography.

> Cracking RSA is NP-complete so nothing better than brute force is possible.

Your task is to evaluate to what extent (if any) this statement is true. For full marks, you will consider the following questions.

- What would it mean, precisely, for "cracking RSA" to be NP-complete? In particular, what is the decision problem involved and what is meant by saying it is NP-complete?
- Is the problem, in fact, NP-complete? Why or why not?
- What is meant, precisely, by the conclusion, "nothing better than brute force is possible"?
- Assuming the premise is correct, i.e. "cracking RSA is NP-complete", does the conclusion follow? Why or why not?
- What is the relationship, more generally, between encryption systems and NP-completeness?

[20 marks]