1 Economics of Security

a. Describe the “market for lemons” and how it parallels to the anti-virus software industry.

b. The deployment of IPv6 and DNSSEC has been slow with each of their own problems. Describe possible corporations’ reasons for not deploying these technologies as soon as possible and what can be done to speed up the worldwide deployment process?

2 De-anonymising Alice

Describe how you would de-anonymise Alice in the second last page of Dr Steven Murdoch’s Anonymity & Censorship lecture? Can you improve it with more time or other resources?

3 Anonymous Communications (2009 Paper 8 Question 11)

a. Give four uses of anonymous communication other than censorship resistance.

b. Explain the role of privacy in anonymous communications. What limits or costs does low latency impose?

c. Imagine you are a government censor, trying to identify which of your citizens are viewing forbidden websites through Tor. (i) If you are able to wiretap the Internet connections of any 1% of the population, what effective capability does this give against Tor users? (ii) If there are currently 1000 active Tor nodes, what extra capability would you acquire if you added a further 100 nodes under your control? Explain any assumptions you make.

d. If you are using Tor to escape censorship, how often should you change the circuit path you use? Explain your answer.
4 Anonymous Communication-Proxies

Consider two designs for an anonymizing proxy which seeks to avoid timing analysis of individual packets

- **Stop and Go** The proxy will wait until it receives $k$ packets, then send the $k$ packets out in a random order.

- **Pooling** The proxy will keep a pool of between $k$ and $2k$ packets at all times. When the pool gets to size $2k$, it will randomly select $k$ packets to send from its pool, then wait for $k$ more packets to arrive.

We will compare the properties of these two designs.

a. What are the performance implications of the two designs? How does their throughput compare? How does their latency, specifically how much longer do we expect a packet to wait in a Pooling proxy compared to a Stop and Go proxy?

b. How large is the anonymity set for each packet sent out from a Stop and Go proxy? How large is it for a Pooling proxy?

c. Is the absolute size of the anonymity set a “fair” comparison between the two designs? What might be a better way to compare the anonymity provided by the Pooling proxy?

5 Zero-knowledge Proofs

Peggy has a private key ($K_p$) and she wants to proof her identity (i.e. possession of $K_p$) to Victor.

a. Describe a zero-knowledge proof protocol (based on knowledge of $K_p$) that Peggy can use to prove her identity to Victor.

b. How could this protocol be exploited by a pair of impostors that want to impersonate Peggy in front of Victor?