

## Oral Exam Questions - Paul Rowe (2006)

### Crypto/Security

- 1) What is semantic security?
- 2) Describe the Dolev-Yao model.
- 3) What is a hash function? “What’s all this about hash functions being broken and why is it important?”

### Probability

- 1) Construct a probability space to model fair coin tosses.
- 2) What can you say about the “long term behavior” of this model? (Intentionally vague.)
- 3) What is a “stopping time”?
- 4) Suppose you invest a proportion  $p$  of your money into a stock which yields  $X$  or  $Y$  (gain or loss percentages), each with probability  $1/2$ ; the remaining money is placed, say, under your mattress. Analyze the situation. What value of  $p$  will maximize expected long term gain?