Lecture 9:
Hash House Harriers

CS551: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Menu

- “Quiz” Results
- Hashing

Quiz Results

- Six people got everything right
- Most common mistake:

  $e * d \equiv 1 \bmod n$

  should be:

  $e * d \equiv (\bmod (p-1)(q-1))$

  Why is $e * d \equiv 1 \bmod n$ a bad guess?
- Little correlation between how well you said you understood RSA and correctness of answers