Lecture 11: Birthday Paradoxes

CS588: Security and Privacy
University of Virginia
Computer Science

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

Quiz Results

1. How well do you feel you understand RSA?

a. Broke it yesterday 0

b. Well enough to implement 2 (1 has done it)

c. Almost everything in RSA paper 4 (but 2 revealed otherwise in their answers)

d. Sort of 19 (6 answered all questions well)

e/f. Not really, No Clue 11

8 got all blanks right

8 got all blanks right except $ed \equiv 1 \bmod \underline{(p-1)(q-1)}$

Quiz Results

Lectures

way too fast:	3
too fast:	23
write in “little too fast”	3
write in “just right”	2
too slow:	2

(with comments: a little, but really think they’re fine)

way too slow:	0