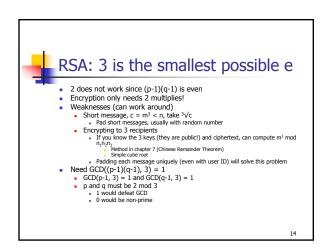


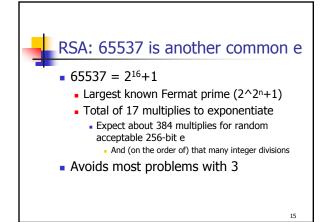
12

RSA: Choosing d and e

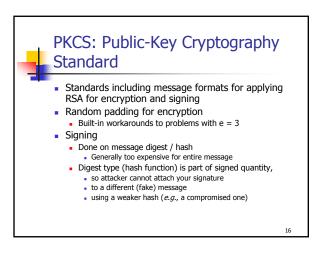
- GCD((p-1)(q-1), e) = 1
- Select e at random and test for relative primarily
- Or, Choose e and then select p and q for relative primality
 - Certain choices of e will make public key computations easier without sacrificing security

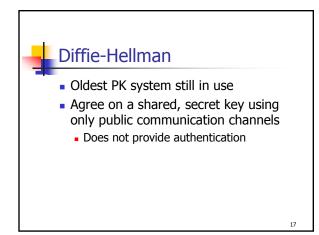
13

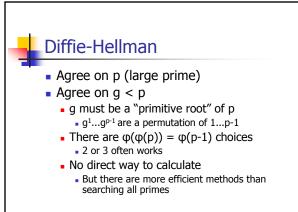




© Eric A. Durant, PhD







18

