

CS 465 HW 7

RSA

Benjamin Bergeson

$$p=7 \quad q=13 \quad 0 < e < 7 \quad e=5$$

$$n = p \cdot q = 91$$

$$\phi(n) = (p-1) \cdot (q-1) = (7-1)(13-1) = (6)(12) = 72$$

$$\text{Public Key} = (e, n) = (5, 91)$$

$$d = \text{GCD}(\phi(n), e) = \text{GCD}(72, 5)$$

$$\text{GCD}(72, 5)$$

$$72 / 5 = 14 \text{ r } 2$$

$$5 / 2 = 2 \text{ r } 1$$

$$2 / 1 = 2 \text{ r } 0$$

$$1 / 0$$

$$\Rightarrow 2 = 72(1) + 5(-14)$$

$$\Rightarrow 1 = 5(1) + 2(-2)$$

$$\Rightarrow 0 = 2(1) + 1(-2)$$

$$5 = 72(1) + 5(-14)$$

$$1 = 5(1) + [72(1) + 5(-14)](-2)$$

$$= 5(1) + 72(-2) + 5(28)$$

$$= 72(-2) + 5(29)$$

$$1 = 72(-2) + 5(29)$$

$$d = 29 \quad k = -2$$

$$\text{Private Key} = (d, n) = (29, 91)$$

3-0235 — 50 SHEETS — 5 SQUARES
 3-0236 — 100 SHEETS — 5 SQUARES
 3-0237 — 200 SHEETS — 5 SQUARES
 3-0137 — 200 SHEETS — FILLER

COMET