Övning 8

1,

n = 55

e = 7

a = 2 kryptera

b = 2 dekryptera

Element 2 krypteras till 2

Dekryptera 2

Om n = 55 så måste p och q vara 5 respektive 11.

m = 4\*10 = 40

gcd(40,7) = 1

40 = 7 \* 5 + 5

7 = 5\*1 + 2

5 = 2 \* 2 + 1

Extended

1 = 5 – 2\*2

= 5 – 2(7 – 5)

= 2\*5 – 2\*7

= 2(40 – 7\*5) – 2\*7

= 2\*40

5,

a, Det finns 11 kolonner och 4 rader. 11 – 7 = 7

27 = 128 ord

b,