RSA example

- Select two random prime numbers for p and q.
- Calculate RSA Modulus by multiplying them together
- p=11
- q=5
- n=11
- $\phi(n)=40$
- Next select public value e, condition is e must be smaller than $\phi(n)$ and is coprime to $\phi(n)$.
- 3, 7, 9, 13, 17,…

RSA..

- Suppose we choose *e=7.*
- Calculating d using the following equation:
- deΞ 1 mod ϕ(n)
- de Ξ 1 mod 40
- d(7) Ξ 1 mod 40
- Euclidean Algorithm
- 40=5(7)+5
- 7=1(5)+2
- 5=2(2)+1

- Extended Euclidean Algorithm
- 1=5-2(2)
- 1= 5- 2(7-1(5))
- = 5-2(7)+2(5)=3(5)-2(7)
- =3(40-5(7))-2(7)
- =3(40)-15(7)-2(7)= 3(40)-17(7)
- d=-17 mod 40
- d=23 mod 40
- d=23
- https://www.youtube.com/watch?v=O-4_oS3G7MI