15

- Either explicitly or via transfer of trust

- Sara trusts she want to “talk” to Chuck

- Open system
  - Multiple entity trust model
  - No single control of who “talks” to whom


e : N

- Chuck trusts [redacted] belongs to Sara

$e : N$ d

- Given [redacted] it is difficult* to determine

- represents a binding relationship through

$$e = 17,\ d = 33,\ N = 55$$

$$\left(e \cdot d\right) \% \varphi(N) = 1$$

Structure

Structure

- $e = 17,\ d = 33,\ N = 55$ represents a binding relationship through

$$(e \cdot d)\ \%\ \varphi(N) = 1$$

- Given $e : N$ it is difficult* to determine d
- Chuck trusts $e : N$ belongs to Sara
  - Either explicitly or via transfer of trust
- Sara trusts she want to “talk” to Chuck
- Open system
  - Multiple entity trust model
  - No single control of who “talks” to whom

* The RSA problem is linked to the integer factorization problem

Man-in-the-Middle