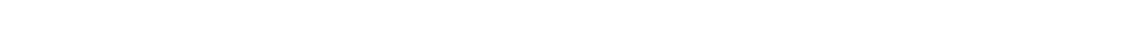




 Chuck and Sara only trust each other • Each holds a participating piece of the binding relationship Closed system Single entity trust model Explicit control over who "talks" to whom



Given



%

x = 5, v = 6, g = 2, N = 13

Structure

Structure

• x = 5, v = 6, g = 2, N = 13 represents a binding relationship through

$$v = g^x \% N$$

- Given v:g:N it is difficult* to determine x
- Chuck and Sara only trust each other
 - Each holds a participating piece of the binding relationship
- Closed system
 - Single entity trust model
 - Explicit control over who "talks" to whom

^{*} The SRP problem is linked to the Diffie-Hellman problem which is linked to the discrete logarithm problem

SRP & ALS