Kryptografie

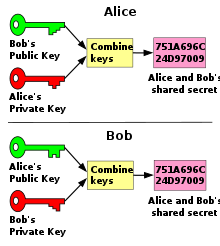
* Symmetrisches (gleicher Schlüssel)
  + AES
  + …
* Asymmetrisches
* RSA
* DH (Diffie Hellman)

Protokolle

* TLS
* SSH

Diffie Hellman Key-exchange

Diffie Hellman Key- exchange ist dafür da, dass man sich den gemeinsamen Schlüssel tauscht

 öffentlicher parameter:

p ... Primzahl

g muss Element von {1,2,....,p-1}

Die eine Person sucht sich einen Schlüssel aus

Eine Zahl aus

a = Kprivate Element {2,3,..., p-2}

A = Kpublic = ga modulo p

KAB = Ba modulo p

Die andere Person

b = Kprivate Element {2,3,…,p-2}

B = Kpublic = gb modulo p

KAB = Ab modulo p

Die beiden tauschen ihren Public Key

Konkreter Beweis:

Ba = (gb)a = ga\*b modulo p

Ab = (ga)b = ga\*b modulo p

p ist ein öffentlicher Parameter, der beiden bekannt ist