Diffie Hellman

Sicherheit:

Anfällig gegen ‚Man-in-the-middle‘-Angriff. Dieser ‚Man‘ kann die Schlüssel austauschen und die Nachrichten verfälschen.

* + Alice ----- Man-in-the-Middle ----- Bob
  + Situation: Alice und Bob wollen ihre Schlüssel austauschen und eine Person hat sich dazwischen geschaltet

Nähere Erklärung zu:

* Schlüssel ersetzen
  + Person empfängt die beiden Schlüssel, verändert (zweimal Diffie-Hellman-Schlüsselaustausch ausführen) diese und sendet sie weiter an Bob und Alice
* Nachricht verfälschen
  + Person empfängt die Nachrichten liest, verhindert oder verändert diese sogar und sendet sie eventuell an den jeweiligen Empfänger weiter

RSA

Anwendung

* Pretty Good Privacy (PGP)
  + BekanntesVerschlüsselungsprogramm
  + Benutzt RSA-Algorithmus
  + Ist so siehcre, dass es verboten war das Programm von Amerika nach Europa zu exportieren, da es unter das militärische Gesetzt zur Spionageabwehr fiel
* Chipkarten
  + Spezielle RSA-Chipkarten, die beispielsweise einen PIN mit dem RSA-Algorithmus verschlüsseln
* Bankenwesen
  + Z.B. Verschlüsselung von Geheimzahlen
* Verschleierung von Pay-TV-Programmen
* Verschlüsselung von Mobilfunknetzen
* Verschlüsselung bei Geheimdiensten