

Diffie-Hellman-Schlüsseltausch

Luc Spachmann

FSU Jena

18.01.2024

- Abgabe der Programme am 15. März
- Bevorzugt als Git-Repository, sonst auch als Archiv
- Programme grob kommentiert (was macht diese Funktion, nicht: was macht diese Zeile)
- README:
 - Welche Programme gibt es?
 - Wie sind diese auszuführen?

Diffie-Hellman Schlüsseltausch

- Benötigt Primzahl p und Generator g von \mathbb{Z}_p^* (global bekannt)
- Geheime Zahlen a und b zwischen 2 und $p - 1$
- Beide berechnen $A = g^a \bmod p$ bzw $B = g^b \bmod p$
- A und B werden ausgetauscht
- Berechne geteiltes Geheimnis $S = B^a$ bzw $S = A^b$
- Kann als Schlüssel für z.B. AES verwendet werden

Generierung der Parameter

- Problem: Generator g ist schwer zu berechnen (Faktorisierung von $p - 1$)
- Sucht Primzahl q , sodass $p = 2q + 1$ prim
- Jedes $1 < g < p - 1$ geeignet (nicht zwangsweise Generator!)
- Praxis: Meist 2, 3, ...
- Größe von g nicht sicherheitsrelevant
- Oft auch standardisierte p, q verwendet
- Geheime Zahlen a, b ausreichend groß

- Implementiert DH-Schlüsseltausch und Parametergenerierung
- Einziger Inputparameter: Bitlänge der Primzahl (Als Zahl, ungefähr)
- Ausgabe in Standardoutput:
 - Erste Zeile: Primzahl p
 - Zweite Zeile: Generator g
 - Dritte Zeile: Alice' Berechnung A
 - Vierte Zeile: Bobs Berechnung B
 - Fünfte Zeile: Berechnetes Geheimnis S