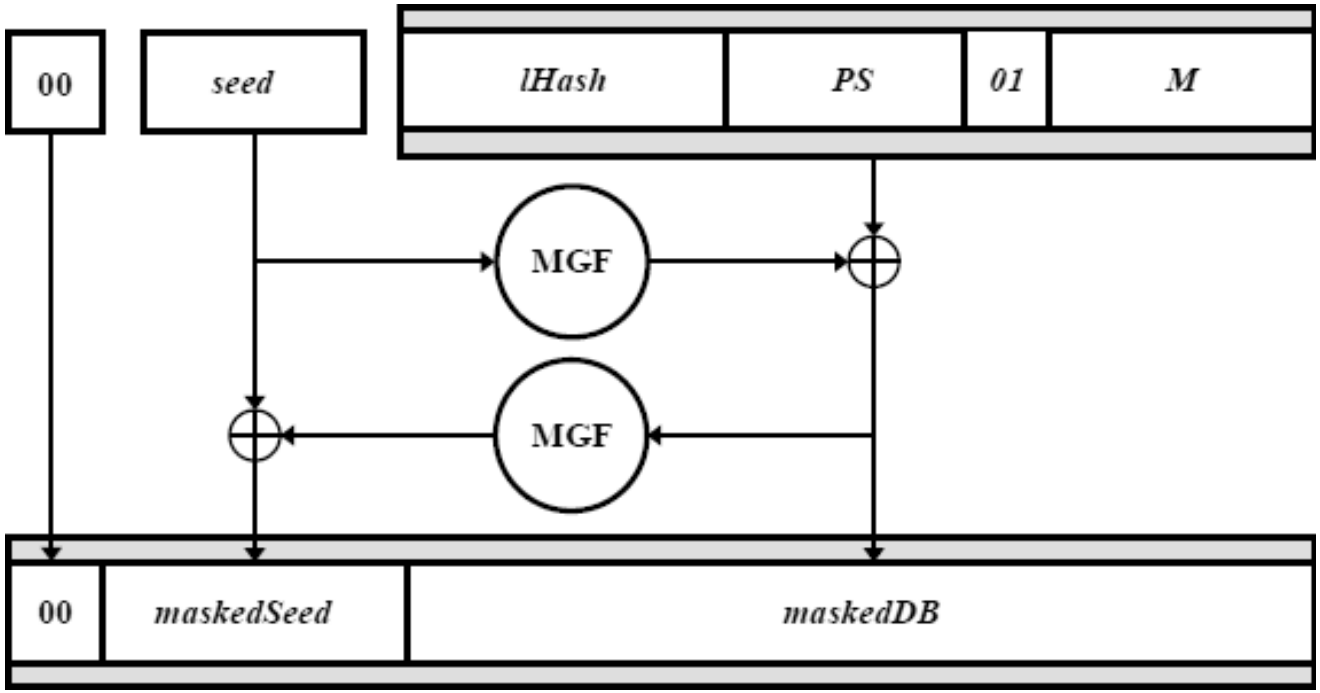
Diffie-Hellman-Schlüsseltausch

Luc Spachmann

FSU Jena

07.01.2022

Nachtrag



- Byte als Zahl interpretiert in 'Big Endian'!

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 $A = g^a \mod p$ bzw $B = g^b \mod p$
- 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

Man-in-the-Middle Angriff

- DH ist nicht authentifiziert
- Eve kann sich als Alice bzw. Bob ausgeben
- Eve erzeugt zwei Schlüssel und 'übersetzt'
- Lösung: Signieren der Nachrichten

Aufgabe

- Implementiert DH-Schlüsseltausch und Parametergenerierung
- (ohne Signatur)