DIE KOCH CHIFFRE

VON DIPL. ING. FRANK GERLACH

DER NUTZEN

- Ähnliche **Garantien** wie SSL/TLS:
  - keine Replay-Attacke möglich
  - wiederholter Klartext erzeugt unterschiedlichen Chiffretext
  - Gegenstelle ist stark authentifiziert
  - Klartext ist verdeckt

VORTEILE DER KOCH CHIFFRE IM VERGLEICH ZU SSL/TLS

- Minimaler Umfang (548 Zeilen Sappeur Code)
  - Formal validierbar !
- Halbe Mathematische Angriffsfläche (nur der symmetrische Algorithmus)
- Kein Man-in-The-Middle Angriff machbar
- Schlüsseltausch mittels Bote, Papierbrief, GNUpg oder KVZ

VIELEN DANK

FRANKGERLACH.TAI@GMX.DE