Asymmetrische Kryptographie in Java
Handout

A. H. W. Lindemann, N. Vetter

10. Januar 2014

1 Asymmetrische Kryptographie

1.1 Kerckhoffs Prinzip

„Sicherheit ist allein vom Schlüssel und nicht vom Verfahren abhängig.“

1.2 Theorie

⇒ Einwegfunktionen mit Falltür.

- injektive Funktion $f : X \to Y$
- $\forall x \in X$ ist f(x) effizient zu berechnen
- aus Bild y = f(x) darf Urbild x nur „effizient“ berechnet werden können, wenn Zusatzinformationen verfügbar sind.
- Bsp.: h-te Potenz mod(n), Zusammengesetzter mod(n)

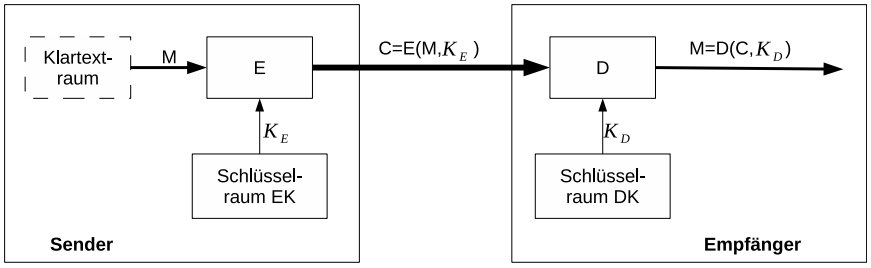

Abbildung 1: Asymmetrische Kryptographie (nach [Eckert, 2013])

- Tupel = (M, C, EK, DK, E, D)
- 2 endliche Alphabete (A_1, A_2)
- Klartext $(M \subseteq A_1^* \backslash \emptyset)$
- Kryptotext $(C \subseteq A_2^* \backslash \emptyset)$
- Verschlüsselungsschlüsselraum $(EK \backslash \emptyset)$
- Entschlüsselungsschlüsselraum $(DK/\emptyset \; mit \; f : EK \to DK \; und \; f(K_E) = K_D)$
- Verschlüsselungsverfahren $(E : \; MxEK \to C)$
- Entschlüsselungsverfahren $(D : \; CxDK \to M)$
- Es gilt: $\forall M : D(E(M, K_E), K_D) = M$

1.3 Vertreter

- RSA, DSA, Diffie-Hellman, ElGamal

1.4 Anwendungen

- PGP, SSL / TLS

2 Hybride Kryptographie

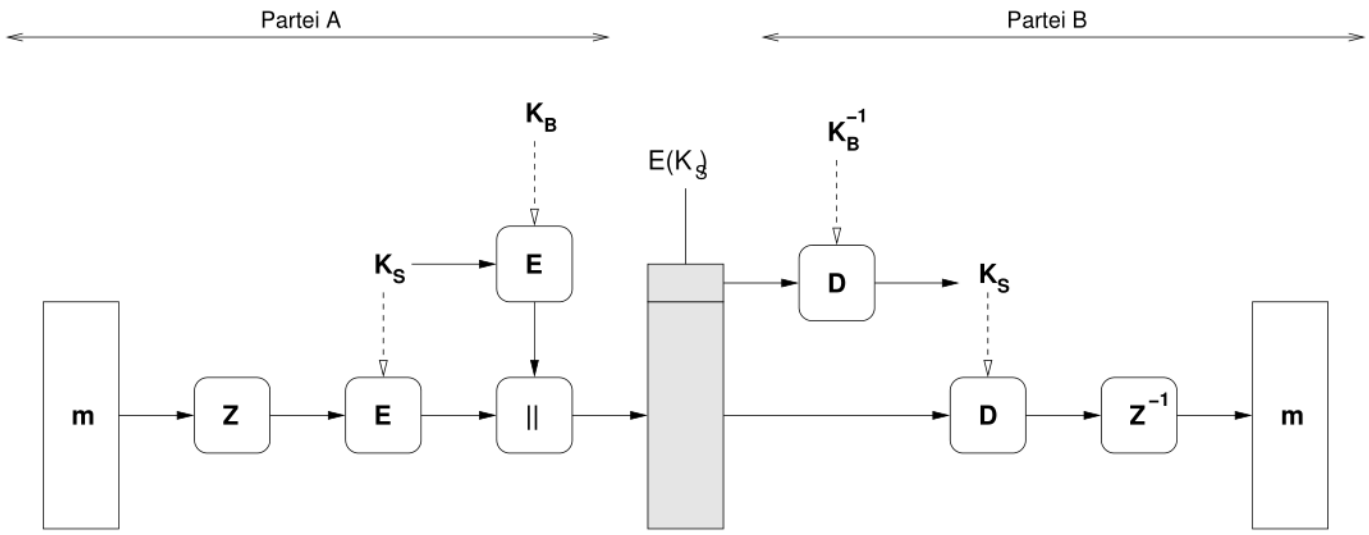

Abbildung 2: Hybride Kryptographie (Alice → Bob, aus VL „Sicherheit in Rechnernetzen“)

- Nachricht = m
- Komprimierung = Z
- Verchlüsselung = E
- symmetrischer Schlüssel = K_S
- öffentlicher Schlüssel (Bob) = K_B
- Konkatenation = $||$
- verschlüsselter symmetrischer Schlüssel = $E(K_S)$
- Entschlüsselung = D
- privater Schlüssel (Bob) = K_B^{-1}
- Dekomprimierung = Z^{-1}

3 Java-Implementierung

3.1 JCA vs JCE

Abspaltung aufgrund von Exportbeschränkungen der USA:

- **J**ava **C**ryptography **A**rchitecture - Hashfunktionen, Schlüsselgeneratoren,...
- **J**ava **C**ryptography **E**xtension - Verschlüsselungsfunktionen

3.2 Kryptoprovider

Interne Provider
Beispiel „The SunJCE Provider“

- AES, DES, ...
- RSA
- Diffie-Hellman

Externe Provider
Beispiel „Bouncy Castle“

- AES, DES, ...
- RSA, ElGamal, NTRU
- Diffie-Hellman (verschiendene Varianten)

4 Literaturliste

Literatur

[Eckert, 2013] Eckert, C. (2013). *IT-Sicherheit : Konzepte - Verfahren - Protokolle*. Oldenburg.

[Engelbrecht, 2004] Engelbrecht, M. (2004). *Entwicklung sicherer Software - Modellierung und Implementierung mit Java*. Spektrum.