

Kryptographie II

Asymmetrische Kryptographie

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Sommersemester 2009

Organisatorisches

- Vorlesung: **Mi 08:30-10:00** in NA 01/99 (2+2 SWS, 6 CP)
- Übung: **Mi 12-14** in NA 2/99
- Assistent: **Mathias Herrmann**, Korrektor: **Marc Kleffmann**
- Übungsbetrieb: jeweils abwechselnd alle 2 Wochen
 - ▶ Präsenzübung, Start 22.April
 - ▶ Zentralübung, Start 29.April
- Übungsaufgaben werden korrigiert.
- Gruppenabgaben bis 3 Personen
- Bonussystem:
1/3-Notenstufe für 50%, 2/3-Notenstufe für 75%
Gilt nur, wenn man die Klausur besteht!
- Klausur: Mitte-Ende August

Literatur

Vorlesung richtet sich nach

- Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”, Taylor & Francis, 2008

Weitere Literatur

- S. Goldwasser, M. Bellare, “Lecture Notes on Cryptography”, MIT, online, 1996–2008
- O. Goldreich, “Foundations of Cryptography – Volume 1 (Basic Tools)”, Cambridge University Press, 2001
- O. Goldreich, “Foundations of Cryptography – Volume 2 (Basic Applications)”, Cambridge University Press, 2004s
- A.J. Menezes, P.C. van Oorschot und S.A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996

Erinnerung an Kryptographie I

Symmetrische Kryptographie

- Parteien besitzen gemeinsamen geheimen Schlüssel.
- Erlaubt Verschlüsselung, Authentifikation, Hashen, Pseudozufallspermutationen.
- **Frage:** Wie tauschen die Parteien einen Schlüssel aus?

Nachteile

- 1 U Teilnehmer benötigen $\binom{U}{2} = \Theta(U^2)$ viele Schlüssel.
- 2 Jeder Teilnehmer muss $U - 1$ Schlüssel sicher speichern. Update erforderlich, falls Teilnehmer hinzukommen oder gelöscht werden.
- 3 Schlüsselaustausch funktioniert nicht in offenen Netzen.

Schlüsselverteilungs-Center (KDC)

Partielle Lösung: Verwenden vertrauenswürdige Instanz

- IT-Manager eröffnet Key Distribution Center (KDC).
- Teilnehmer besitzen gemeinsamen, geheimen Schlüssel mit KDC.
- Alice schickt Nachricht "Kommunikation mit Bob" an KDC.
- Alice authentisiert Nachricht mit ihrem geheimen Schlüssel.
- KDC wählt einen *Session-Key* k , d.h. einen neuen Schlüssel.
- KDC schickt Verschlüsselung $E_{Alice}(k)$ an Alice.
- KDC schickt Verschlüsselung $E_{Bob}(k)$ an Bob.

Alternativ im Needham Schröder Protokoll:

KDC schickt $E_{Bob}(k)$ an Alice und diese leitet an Bob weiter.

Vor- und Nachteile von KDCs

Vorteile

- Jeder Teilnehmer muss nur *einen* Schlüssel speichern.
- Hinzufügen/Entfernen eines Teilnehmers erfordert Update *eines* Schlüssels.

Nachteile

- Kompromittierung von KDC gefährdet das gesamte System.
- Falls KDC ausfällt, ist sichere Kommunikation nicht möglich.

Praktischer Einsatz von KDCs

- Kerberos (ab Windows 2000)

Diffie Hellman Gedankenexperiment

Szenario

- Alice will eine Kiste zu Bob schicken.
- Post ist nicht zu trauen, d.h. die Kiste muss verschlossen werden.
- Sowohl Alice als auch Bob besitzen ein Schloss.

Algorithmus 3-Runden Diffie-Hellman Austausch

- 1 Alice sendet die Kiste an Bob, verschlossen mit ihrem Schlüssel.
- 2 Bob sendet die Kiste zurück, verschlossen mit seinem Schlüssel.
- 3 Alice entfernt ihr Schloss und sendet die Kiste an Bob.
- 4 Bob entfernt sein Schloss und öffnet die Kiste.

Beobachtung: Viele Funktionen sind inherent asymmetrisch.

- Zudrücken eines Schlosses ist leicht, Öffnen ist schwer.
- Multiplizieren von Zahlen ist leicht, Faktorisieren ist schwer.
- Exponentieren von Zahlen ist leicht, dlog ist (oft) schwer.

Diffie-Hellman Schlüsselaustausch (1976)

Szenario:

- Alice und Bob verwenden öffentlichen Kanal.
- Beide wollen einen zufälligen Bitstring k austauschen.
- **Angreifer ist passiv**, d.h. kann nur lauschen, nicht manipulieren.

Systemparameter:

- Sicherheitsparameter 1^n
- Schlüsselerzeugung $(G, q, g) \leftarrow \mathcal{G}(1^n)$
 - ▶ \mathcal{G} ist probabilistischer polynomial-Zeit (in n) Algorithmus
 - ▶ G ist multiplikative Gruppe mit Ordnung q und Generator g .

Protokoll 2-Runden Diffie-Hellman Schlüsselaustausch

- 1 Alice: Wähle $x \in_R \mathbb{Z}_q$. Sende $h_1 = g^x$ an Bob.
- 2 Bob: Wähle $y \in_R \mathbb{Z}_q$. Sende $h_2 = g^y$ an Alice.
- 3 Alice: Berechne $k_A = h_2^x$.
- 4 Bob: Berechne $k_B = h_1^y$.

Korrektheit und Schlüsselerzeugung

Korrektheit: $k_A = k_B$

- Alice berechnet Schlüssel $k_A = h_2^x = (g^y)^x = g^{xy}$.
- Bob berechnet Schlüssel $k_B = h_1^y = (g^x)^y = g^{xy}$.

Schlüsselerzeugung:

- Gemeinsamer Schlüssel $k_A \in G$ ist Gruppenelement, kein Zufallsstring $k \in \{0, 1\}^m$.
- Konstruktion von Zufallsstring mittels sog. *Zufallsextraktoren*.
- Sei k_A ein zufälliges Gruppenelement aus G .
- Zufallsextraktor liefert bei Eingabe k_A einen Schlüssel $k \in \{0, 1\}^m$, ununterscheidbar von einem Zufallsstring derselben Länge.

Übung: Schlüssel k + sichere symmetrische Verschlüsselung liefert zusammen ein beweisbar sicheres Verfahren.

Spiel zur Unterscheidung des Schlüssels

Spiel Schlüsselaustausch $KE_{\mathcal{A},\Pi}(n)$

Sei Π ein Schlüsselaustausch-Protokoll für Gruppenelemente aus G .
Sei \mathcal{A} ein Angreifer für Π .

- 1 $(k, \text{trans}) \leftarrow \Pi(n)$, wobei k der gemeinsame Schlüssel und trans der Protokollablauf ist.
- 2 Wähle $b \in_R \{0, 1\}$. Falls $b = \begin{cases} 1 & k' = k \\ 0 & k' \in_R G \end{cases}$.
- 3 $b' \leftarrow \mathcal{A}(\text{trans}, k')$. Ausgabe $\begin{cases} 1 & \text{falls } b' = b \\ 0 & \text{sonst} \end{cases}$.

- \mathcal{A} gewinnt, falls $KE_{\mathcal{A},\Pi}(n) = 1$.
- D.h. \mathcal{A} gewinnt, falls er erkennt, welches der korrekte Schlüssel k des Protokolls Π und welches der zufällige Schlüssel $k' \in_R G$ ist.
- \mathcal{A} kann trivialerweise mit Ws $\frac{1}{2}$ gewinnen. (Wie?)

Sicherheit Schlüsselaustausch

Definition negl

Eine Funktion $f : \mathbb{N} \rightarrow \mathbb{R}^+$ heißt *vernachlässigbar*, falls für jedes Polynom $p(n)$ und alle hinreichend großen n gilt $f(n) < \frac{1}{p(n)}$.

Notation: Wir bezeichnen eine bel. vernachlässigbare Fkt mit $\text{negl}(n)$.

Bsp:

- $\frac{1}{2^n}$, $\frac{1}{2^{\sqrt{n}}}$, $\frac{1}{n^{\log \log n}}$ sind vernachlässigbar.
- $\frac{1}{2^{\mathcal{O}(\log n)}}$ ist nicht vernachlässigbar.
- Es gilt $q(n) \cdot \text{negl}(n) = \text{negl}(n)$ für jedes Polynom $q(n)$.

Definition Sicherheit Schlüsselaustausch

Ein Schlüsselaustausch Protokoll Π ist sicher gegen passive Angriffe, falls für alle probabilistischen Polynomialzeit (ppT) Angreifer gilt $\text{Ws}[KE_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$.

Der Wsraum ist definiert über die zufälligen Münzwürfe von \mathcal{A} und Π .

dlog Problem

Definition Diskrete Logarithmus (dlog) Annahme

Das *Diskrete Logarithmus Problem* ist hart bezüglich \mathcal{G} , falls für alle ppt Algorithmen \mathcal{A} gilt

$$|\text{Ws}[\mathcal{A}(G, g, q, g^x) = x]| \leq \text{negl.}$$

Der Wsraum ist definiert bezüglich der zufälligen Wahl von $x \in \mathbb{Z}_q$ und der internen Münzwürfe von \mathcal{A} und \mathcal{G} .

dlog Annahme: Das dlog Problem ist hart bezüglich \mathcal{G} .

- Unter der dlog Annahme können die geheimen Schlüssel x, y bei Diffie-Hellman nur mit vernachlässigbarer Ws berechnet werden.
- D.h. die dlog Annahme ist eine notwendige Sicherheitsannahme.

CDH Problem

Definition Computational Diffie-Hellman (CDH) Annahme

Das *Computational Diffie-Hellman Problem* ist hart bezüglich \mathcal{G} , falls für alle pp-Algorithmen \mathcal{A} gilt $\text{Ws}[A(G, g, q, g^x, g^y) = g^{xy}] \leq \text{negl}$.

Wsraum: zufällige Wahl von $x, y \in \mathbb{Z}_q$, interne Münzwürfe von \mathcal{A} , \mathcal{G} .

CDH Annahme: Das CDH Problem ist hart bezüglich \mathcal{G} .

- Unter der CDH-Annahme kann ein DH-Angreifer Eve den Schlüssel $k_A = g^{xy}$ nur mit vernachlässigbarer Ws berechnen.

Problem:

- Sei CDH schwer, so dass Angreifer Eve k_A nicht berechnen kann.
- Benötigen aber, dass k_A ein zufälliges Gruppenelement in G ist.
- Unterscheiden von g^{xy} und g^z , $z \in_R \mathbb{Z}_q$ könnte einfach sein.

DDH Problem

Definition Decisional Diffie-Hellman (DDH) Annahme

Das *Decisional Diffie-Hellman Problem* ist hart bezüglich \mathcal{G} , falls für alle pp-Algorithmen \mathcal{A} gilt

$$|\text{Ws}[\mathcal{A}(G, q, g, g^x, g^y, g^{xy})] - \text{Ws}[\mathcal{A}(G, q, g, g^x, g^y, g^z)]| \leq \text{negl.}$$

Wsraum: zufällige Wahl von $x, y, z \in \mathbb{Z}_q$, interne Münzwürfe von \mathcal{A} , \mathcal{G} .

DDH Annahme: Das DDH Problem ist hart bezüglich \mathcal{G} .

- Unter der DDH-Annahme kann Eve den DH-Schlüssel g^{xy} nicht von einem zufälligen Gruppenelement unterscheiden.

Sicherheitsbeweis des DH-Protokolls

Satz Sicherheit des Diffie-Hellman Protokolls

Unter der DDH-Annahme ist das DH-Protokoll Π sicher gegen passive Angreifer \mathcal{A} .

Beweis: Es gilt $\text{Ws}[KE_{\mathcal{A},\Pi}(n) = 1]$

$$\begin{aligned} &= \frac{1}{2} \cdot \text{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] + \frac{1}{2} \cdot \text{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] \\ &= \frac{1}{2} \cdot \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] + \frac{1}{2} \cdot \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 0] \\ &= \frac{1}{2} \cdot \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] + \frac{1}{2} \cdot (1 - \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]) \\ &= \frac{1}{2} + \frac{1}{2} \cdot (\text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] - \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]) \\ &\leq \frac{1}{2} + \frac{1}{2} \cdot |\text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] - \text{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]| \\ &\leq \frac{1}{2} + \frac{1}{2} \cdot \text{negl} \quad \text{nach DDH-Annahme.} \end{aligned}$$