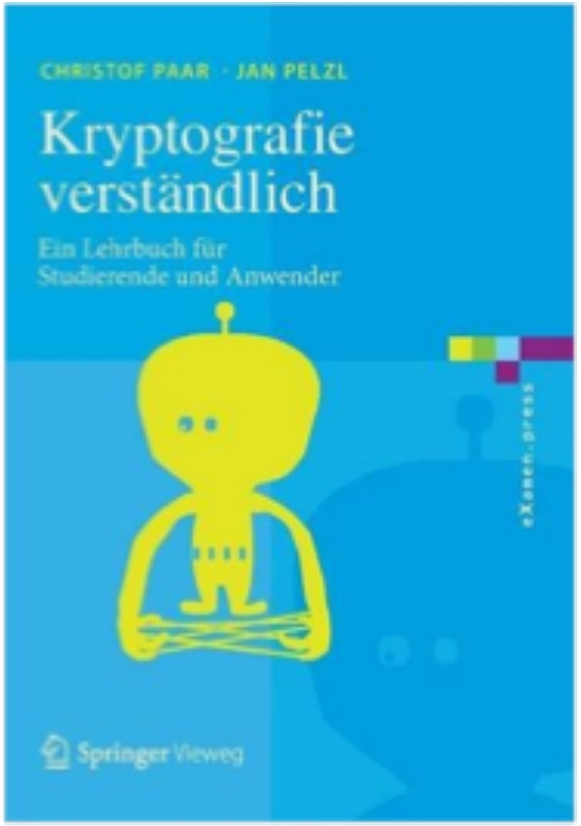
Kryptografie verständlich

Ein Fachbuch für
Studierende und Anwender

von
Christof Paar und Jan Pelzl

www.crypto-textbook.com



Kapitel 8

Asymmetrische Verfahren basierend auf dem diskreten Logarithmusproblem

(Version: 1. Dezember 2016)

Übersicht

- Der Diffie-Hellman Schlüsselaustausch
- Das diskrete Logarithmusproblem
- Sicherheit des Diffie-Hellman Schlüsselaustauschs
- Das Elgamal Verschlüsselungsverfahren

Übersicht

- **Der Diffie-Hellman Schlüsselaustausch**
- Das diskrete Logarithmusproblem
- Sicherheit des Diffie-Hellman Schlüsselaustauschs
- Das Elgamal Verschlüsselungsverfahren

Diffie-Hellman Schlüsselaustausch
Übersicht

- 1976 durch **Whitfield Diffie** und **Martin Hellman** vorgestellt
- **Weit verbreitet**, u.a. in Secure Shell (SSH), Transport Layer Security (TLS) und Internet Protocol Security (IPSec)
- Der Diffie-Hellman Key Exchange (DHKE) ist ein Schlüsselaustausch-Protokoll und **nicht** zur Verschlüsselung geeignet

  (Hierzu gibt es Elgamal, eine Erweiterung auf Basis von DHKE)

Video: DHKE using colors:
https://www.youtube.com/watch?v=YEBfamv-_do

Diffie-Hellman Schlüsselaustausch

Set-Up

1. Wähle große Primzahl *p.*
2. Wähle ganze Zahl $\alpha \in \{2,3, \ldots, p-2\}$.
3. Veröffentliche *p* und α.

Diffie-Hellman Schlüsselaustausch

Protokoll

Alice		Bob
Wähle zufälligen privaten Schlüssel $k_{prA}=a \in \{1,2,\ldots,p-1\}$		Wähle zufälligen privaten Schlüssel $k_{prB}=b \in \{1,2,\ldots,p-1\}$
Berechne zugehörigen öff. Schlüssel $k_{pubA}= A = \alpha^a \bmod p$	$A \rightarrow$	
	$\leftarrow B$	Berechne zugehörigen öff. Schlüssel $k_{pubB}= B = \alpha^b \bmod p$
Berechne gemeinsames Geheimnis $k_{AB} = B^a = (\alpha^a)^b \bmod p$		Berechne gemeinsames Geheimnis $k_{AB} = A^b = (\alpha^b)^a \bmod p$

Von nun an können wir den gemeinsamen Schlüssel k_{AB} zur Verschlüsselung z.B. mit AES nutzen

$y = AES_{kAB}(x)$ $\quad y \rightarrow \quad$ $x = AES^{-1}_{kAB}(y)$

Diffie-Hellman Schlüsselaustausch

Beispiel mit kleinen Zahlen

Domänenparameter p=29, α=2

Alice		Bob
Wähle zufälligen privaten Schlüssel $k_{prA} = a = 5$		Wähle zufälligen privaten Schlüssel $k_{prB} = b = 12$
Berechne zugehörigen öff. Schlüssel $k_{pubA} = A = 2^5 = 3 \bmod 29$	A →	
	← B	Berechne zugehörigen öff. Schlüssel $k_{pubB} = B = 2^{12} = 7 \bmod 29$
Berechne gemeinsames Geheimnis $k_{AB} = B^a = 7^5 = 16 \bmod 29$		Berechne gemeinsames Geheimnis $k_{AB} = A^b = 3^{12} = 16 \bmod 29$

Korrektheitsbeweis:

Alice berechnet: $B^a = (\alpha^b)^a \bmod p$
Bob berechnet: $A^b = (\alpha^a)^b \bmod p$

d.h., Alice und Bob haben den gleichen Schlüssel k_{AB} *berechnet!*

Übersicht

- Der Diffie-Hellman Schlüsselaustausch
- **Das diskrete Logarithmusproblem**
- Sicherheit des Diffie-Hellman Schlüsselaustauschs
- Das Elgamal Verschlüsselungsverfahren

Diffie-Hellman Schlüsselaustausch

Das diskrete Logarithmusproblem

Das diskrete Logarithmusproblem (DLP) in Z_p^*

- Gegeben: endliche zyklische Gruppe Z_p^* der Ordnung $p-1$ primitives Element $\alpha \in Z_p^*$ und Element $\beta \in Z_p^*$
- Das DLP ist die ganzzahlige Lösung $1 \leq x \leq p-1$ mit $\alpha^x \equiv \beta \bmod p$
- Diese Berechnung nennt man **diskretes Logarithmusproblem (DLP)**

$$x = log_\alpha \beta \bmod p$$

- Beispiel: Berechne x mit $5^x \equiv 41 \bmod 47$

Diffie-Hellman Schlüsselaustausch

Das verallgemeinerte diskrete Logarithmusproblem

- Gegeben: endliche zyklische Gruppe G mit Gruppenoperation $\circ$ und Kardinalität n
- Wir betrachten die Element $\alpha, \beta \in G$
- Das diskrete Logarithmusproblem ist die ganzzahlige Lösung x mit $1 \leq x \leq n$, so dass gilt

$$\beta = \underbrace{\alpha \circ \alpha \circ \alpha \circ \ldots \circ \alpha}_{x\text{-mal}} = \alpha^x$$

Diffie-Hellman Schlüsselaustausch

Das verallgemeinerte diskrete Logarithmusproblem

Über folgende Gruppen werden diskrete Logarithmusprobleme in der Kryptografie verwendet:

1. Die multiplikative Gruppe im Primzahlkörper Z_p oder einer Untergruppe daraus. Der klassische DHKE verwendet z.B. diese Gruppe, aber auch Elgamal Verschlüsselung oder der digital Signatur Algorithmus (DSA).
2. Die zyklische Gruppe von Punkten auf elliptischen Kurven
3. Die multiplikative Gruppe im endlichen Körper $GF(2^m)$ oder einer Untergruppe daraus. Verfahren wie der DHKE kann damit realisiert werden.
4. Hyperelliptische Kurven oder algebraische Varietäten, welche als Verallgemeinerung von elliptischen Kurven angesehen werden können.

Anmerkung: Die Gruppen 1. und 2. werden in der Praxis am meisten verwendet.

Diffie-Hellman Schlüsselaustausch

Angriffe auf das diskrete Logarithmusproblem

Sicherheit asymmetrischer Verfahren beruht oft auf der Schwierigkeit, den DLP in zyklischen Gruppen zu berechnen, d.h. Berechne x für ein gegebenes α und β so dass

$$\beta = \alpha \circ \alpha \circ \alpha \circ . \; . \; . \circ \alpha = \alpha^x$$

Diffie-Hellman Schlüsselaustausch

Angriffe auf das diskrete Logarithmusproblem

Es gibt folgende Algorithmen zur Berechnung diskreter Logarithmen:

- Generische Algorithmen (funktionieren in allen Gruppen)
  - Brute-Force-Suche
  - Shanks‘ Baby-Step-Giant-Step Methode
  - Pollard‘s Rho Methode
  - Pohlig-Hellman Methode
- Nicht-generische Algorithmen (funktionieren nur in bestimmten Gruppen, insbesondere in Z_p)
  - Index Calculus Methode

Anmerkung: Elliptische Kurven können nur mit den (schwächeren) generischen Methoden angegriffen werden und kommen daher auch mit geringerer Schlüssellänge als z.B. das DLP in Primzahlkörpern Z_p aus.

Diffie-Hellman Schlüsselaustausch

Angriffe auf das diskrete Logarithmusproblem

Bisherige Rekorde für DLP-Berechnungen in Z_p^*

Dezimalstellen	Bitlänge	Datum
58	193	1991
68	216	1996
85	282	1998
100	332	1999
120	399	2001
135	448	2006
160	532	2007

Um Angriffe, welche das DLP lösen, zu vermeiden, werden Primzahlen von mindestens 1024 Bit Länge für Verfahren wie Diffie-Hellman in Z_p^* empfohlen.

Übersicht

- Der Diffie-Hellman Schlüsselaustausch
- Das diskrete Logarithmusproblem
- **Sicherheit des Diffie-Hellman Schlüsselaustauschs**
- Das Elgamal Verschlüsselungsverfahren

Diffie-Hellman Schlüsselaustausch

Sicherheit des klassischen DHKE

- Welche Informationen hat Oskar?
  - α, p
  - $k_{pubA} = A = \alpha^a \bmod p$
  - $k_{pubB} = B = \alpha^b \bmod p$
- Welche Informationen möchte Oskar haben?
  - $k_{AB} = \alpha^{ba} = \alpha^{ab} = \bmod p$
    (auch bekannt als das Diffie-Hellman Problem (DHP))
- Einzig bekannter Weg zur Lösung des DHP ist die Lösung des DLP, d.h.:
  - Berechne $a = log_\alpha A \bmod p$
  - Berechne $k_{AB} = B^a = \alpha^{ba} = \bmod p$
  - Es wird angenommen, dass das Lösen des DHP und DLP äquivalent ist
- Um praktische Angriffe auf das DLP zu verhindern, wähle $p > 2^{1024}$

Übersicht

- Der Diffie-Hellman Schlüsselaustausch
- Das diskrete Logarithmusproblem
- Sicherheit des Diffie-Hellman Schlüsselaustauschs
- **Das Elgamal Verschlüsselungsverfahren**

Diffie-Hellman Schlüsselaustausch

Das Elgamal-Verschlüsselungsverfahren

- Von Taher Elgamal in 1985 vorgeschlagen
- Kann als Erweiterung des DHKE Protokolls gesehen werden
- Basiert auf der Schwierigkeit, das DLP und das DHP zu lösen

Diffie-Hellman Schlüsselaustausch

Das Elgamal-Verschlüsselungsverfahren

Alice		Bob
	β ←	Wähle $d = k_{prB} \in \{2,\ldots,p\text{-}2\}$ Berechne $\beta = k_{pubB} = \alpha^d \bmod p$
Wähle i = $k_{prA} \in \{2,\ldots,p\text{-}2\}$ Berechne temporären Schlüssel $k_E = k_{pubA} = \alpha^i \bmod p$	k_E →	
		Berechne $k_M = k_E^d \bmod p$
Berechne $k_M = \beta^i \bmod p$ Verschlüssele Nachricht $x \in Z_p^*$: $y = x \cdot k_M \bmod p$	y →	
		Entschlüssele $x = y \cdot k_M^{-1} \bmod p$

Ähnlichkeit mit dem DHKE: Das Elgamal Protokoll führt die Berechnungen in einer anderen Reihenfolge durch, um eine Nachricht zu sparen (sh. nächste Folie)

Diffie-Hellman Schlüsselaustausch

Das Elgamal-Verschlüsselungsverfahren

Alice

Bob

Wähle große Primzahl p

Wähle primitives Element $\alpha \in Z_p^*$ oder aus einer Untergruppe Z_p^*

$k_{pubB} = (p, \alpha, \beta)$ ←

Wähle $d = k_{prB} \in \{2,\ldots,p\text{-}2\}$

Berechne $\beta = k_{pubB} = \alpha^d \bmod p$

Wähle i = $k_{prA} \in \{2,\ldots,p\text{-}2\}$

Berechne $k_E = k_{pubA} = \alpha^i \bmod p$

Berechne Maskierungsschlüssel $k_M = \beta^i \bmod p$

Verschlüssele Nachricht $x \in Z_p^*$:
$y = x \cdot k_M \bmod p$

→ (k_E, y)

Berechne Maskierungsschlüssel $k_M = k_E^d \bmod p$

Entschlüssele $x = y \cdot k_M^{-1} \bmod p$

Diffie-Hellman Schlüsselaustausch

Elgamal: Rechentechnische Aspekte

- Schlüsselerzeugung
  - Erzeugung einer Primzahl p
  - Die Größe von p muss mindestens1024 Bit betragen
- Verschlüsselung
  - Benötigt zwei modulare Exponentiationen und eine modulare Multiplikation
  - Alle Operanden haben eine Bitlänge von $\log_2 p$
  - Effiziente Durchführung benötigt Methoden wie den Square-and-Multiply Algorithmus
- Entschlüsselung
  - Benötigt eine modulare Exponentiation und eine modulare Inversion

Diffie-Hellman Schlüsselaustausch
Elgamal: Sicherheit

- Passive Angriffe
  - Angreifer fängt p, α, $\beta = \alpha^d$, $k_E = \alpha^i$, $y = x \cdot \beta^i$ ab und möchte x berechnen
  - Problem basiert auf dem DLP

- Aktive Angriffe
  - Ist der öffentliche Schlüssel nicht authentisch, kann ein Angreifer einen falschen öffentlichen Schlüssel einführen
  - Wird der Exponent i mehrfach verwendet, ist ebenfalls ein Angriff möglich

Lessons Learned

- Das Diffie-Hellman Protokoll ist ein weitverbreitetes Verfahren zum Schlüsselaustausch und basiert auf zyklischen Gruppen.
- Das diskrete Logarithmus Problem ist eine der wichtigsten Einwegfunktionen in der asymmetrischen Kryptografie, worauf viele Algorithmen basieren.
- Für das Diffie-Hellman Protokoll in Z_p^* sollte die Primzahl p mindestens eine Länge von 1024 Bit haben, um eine vergleichbare Sicherheit wie ein 80-Bit symmetrisches Verfahren zu haben.
- Für eine bessere Langzeitsicherheit sollte die Primzahl eine Länge von 2048 Bit oder mehr aufweisen.
- Das Elgamal Verfahren ist eine Erweiterung des DHKE, wobei der hergeleitete Sitzungsschlüssel als multiplikativer Maskierungsschlüssel zur Verschlüsselung der Nachricht dient.
- Elgamal ist ein probabilistisches Verschlüsselungsverfahren, d.h. zwei identische Klartexte ergeben unterschiedliche Chiffrate.