Proseminar Schlüsselaustausch (Diffie - Hellman)

- Schlüsselaustausch
- Mathematische Grundlagen
- Das DH – Protokoll
- Sicherheit
- Anwendung

Schlüsselaustausch

- Warum Schlüsselaustausch?
  - Übertragen eines bestehenden Schlüssels oder Vereinbarung eines neuen Schlüssels (wie bei D-H)
  - Anderes Beispiel : Needham-Schröder-Protokoll zur Schlüsselverteilung und Authentifikation
  - Der Schlüssel kann danach z.B. Grundlage für ein symmetrisches Verschlüsselungsverfahren oder andere Kryptosysteme sein

Schlüsselaustausch

- Was macht Diffie – Hellman ?
  - Erzeugt einen neuen Schlüssel zwischen zwei Kommunikationspartnern über einen unsicheren Kanal
  - Ein Angreifer kann anhand der übertragenen Information nicht effizient den Schlüssel berechnen
  - D-H ist kein asymetrisches Kryptosystem wie z.B. RSA – nur ein geheimer Schlüssel wird vereinbart

Schlüsselaustausch

- Historisches
  - 1976 von Whitfield Diffie und Martin Hellman in Stanford entwickelt, Ralph Merkle zählt auch zu den Erfindern
  - Vor allem für militärische Zwecke war der Schlüsselaustausch von großer Bedeutung, da der Transport von Codebüchern oder Streichlisten ein großes Sicherheitsrisiko darstellte
  - 1997 gab der britische Nachrichtendienst GCHQ bekannt, das bis dato geheim gehaltene Protokoll bereits 1960 parallel entwickelt zu haben

Schlüsselaustausch

- Diffie – Hellman war das erste public – key (asymmetrische) Verfahren

- Kurz darauf folgte RSA, das erste wirkliche Kryptosystem auf asymmetrischer Basis

Zahlentheoretische Grundlagen

- Das Diffie – Hellman Protokoll basiert auf :
  - Endliche zyklische Gruppe
  - Generatorelement a
  - Einwegfunktion mit Falltür, d.h. Umkehrung aufwendig zu berechnen (wie z.B. Primfaktorisierung bei RSA)

Zahlentheoretische Grundlagen

- Die zyklische Gruppe ist Teil des Restklassenkörpers

modulo p : $F_p = \mathbb{Z}/p\mathbb{Z}$

(p prim)

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Trägermenge M = {0,..,6}

- In einem endlichen Körper über einer Primzahl p ist Addition, Subtraktion, Multiplikation und Division wohl definiert.

Zahlentheoretische Grundlagen

- Restklassenkörper → zyklische Gruppe
  - F_p^* beschreibt die zyklische multiplikative Gruppe aus dem Restklassenkörper $F_p \setminus \{0\}$ $M=\{1,...,p-1\}$
  - In dieser Gruppe gibt es mindestens einen Generator a der alle Elemente der Gruppe erzeugt
  - Ein Element $a \in M$ ist Generator (primitive Einheitswurzel) wenn:
    - $\forall m \in \{1,...,p-1\} : \exists\ q \in \{0,...,p-1\}$, so dass :

      $m \equiv a^q \bmod p$

Zahlentheoretische Grundlagen

- Beispiel:

  wir wählen p = 7 ; M = {1,...,6}

  - Ist 2 eine primitive Einheitswurzel (Generator) der Gruppe?

$2^6 = 64 \equiv \mathbf{1} \bmod 7$	$2^1 = 2 \equiv \mathbf{2} \bmod 7$
$2^2 = 4 \equiv \mathbf{4} \bmod 7$	$2^3 = 8 \equiv \mathbf{1} \bmod 7$
$2^4 = 16 \equiv \mathbf{2} \bmod 7$	$2^5 = 32 \equiv \mathbf{4} \bmod 7$

  - Nein, da nicht jedes Element aus {1,..6} erzeugt wird (3,5,6)

Zahlentheoretische Grundlagen

- Beispiel 2:

  wieder p = 7; M = {1,...,6}

  - Ist 3 eine primitive Einheitswurzel?

$3^6 = 729 \equiv \mathbf{1} \bmod 7$	$3^2 = 9 \equiv \mathbf{2} \bmod 7$
$3^1 = 3 \equiv \mathbf{3} \bmod 7$	$3^4 = 81 \equiv \mathbf{4} \bmod 7$
$3^5 = 243 \equiv \mathbf{5} \bmod 7$	$3^3 = 27 \equiv \mathbf{6} \bmod 7$

Ja, M\{0} = {1,..,6} wird erzeugt

Zahlentheoretische Grundlagen

- Berechnung der primitiven Einheitswurzel a
  - Fast die Hälfte aller Gruppenelemente sind erzeugende Elemente der Gruppe → gute Chance, mit zufälligem a<p eine Einheitswurzel zu treffen, aufwendig ist die Verifikation

Zahlentheoretische Grundlagen

- Berechnung der primitiven Einheitswurzel a
  - Fast die Hälfte aller Gruppenelemente sind erzeugende Elemente der Gruppe → gute Chance, mit zufälligem a<p eine Einheitswurzel zu treffen, aufwendig ist die Verifikation
  - Indem man p-1 faktorisiert, kann man effizient testen ob :

    Für alle Primfaktoren f : $a^{(p-1)/f} \not\equiv 1 \bmod p$

    → Dann würde es eine Sequenz der Länge (p-1)/f geben und a könnte nicht erzeugend sein

Zahlentheoretische Grundlagen

- Berechnung der primitiven Einheitswurzel a
  - Fast die Hälfte aller Gruppenelemente sind erzeugende Elemente der Gruppe → gute Chance, mit zufälligem a<p eine Einheitswurzel zu treffen, aufwendiger ist die Verifikation
  - Indem man p-1 faktorisiert, kann man effizient testen ob :

    Für alle Primfaktoren f : $a^{(p-1)/f} \neq 1 \bmod p$

    → Dann würde es eine Sequenz der Länge (p-1)/f geben und a könnte nicht erzeugend sein
    - Einfacher Fall : Wenn p-1 = 2r und r ist prim → Dann hat p-1 2 Primfakoren, 2 und r:

      Wenn $a^2 \neq 1 \bmod p$ und $a^r \neq 1 \bmod p$ → a ist primitive Einheitswurzel

Zahlentheoretische Grundlagen

- In der Praxis
  - Je nach Sicherheitsanforderung gibt es feste Primzahlen in der Größe von 1024 bit – 8192 bit (Diffie – Hellman Gruppen)
  - Generator a wird nicht jedesmal berechnet und verifiziert, sondern es ist ein Passender bekannt (meistens a=2, da modulo potenzieren besonders effizient ist)

Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Gemeinsame Basisinformation (nicht geheim):
    - Große Primzahl p und prim. Einheitswurzel a

Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Gemeinsame Basisinformation (nicht geheim):
    - Große Primzahl p und prim. Einheitswurzel a
  - Berechnen der Schlüsselpaare x_i, y_i :

Alice	*Bob*
- wählt x_1 mit $1 \leq x_1 \leq p-1$ zufällig	- wählt x_2 mit $1 \leq x_2 \leq p-1$ zufällig

Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Gemeinsame Basisinformation (nicht geheim):
    - Große Primzahl p und prim. Einheitswurzel a
  - Berechnen der Schlüsselpaare x_i, y_i :

Alice	*Bob*
- wählt x_1 mit $1 \leq x_1 \leq p-1$ zufällig	- wählt x_2 mit $1 \leq x_2 \leq p-1$ zufällig
- berechnet $y_1 = a^{x_1} \bmod p$	- berechnet $y_2 = a^{x_2} \bmod p$

x_i ist jeweils die persönliche, geheime Information

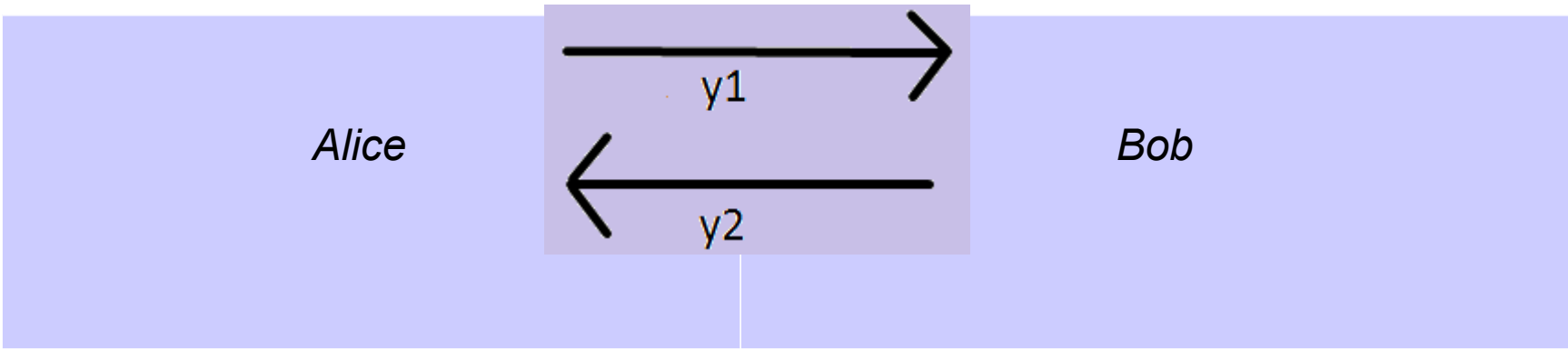
Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Kommunikation:

Alice	*Bob*

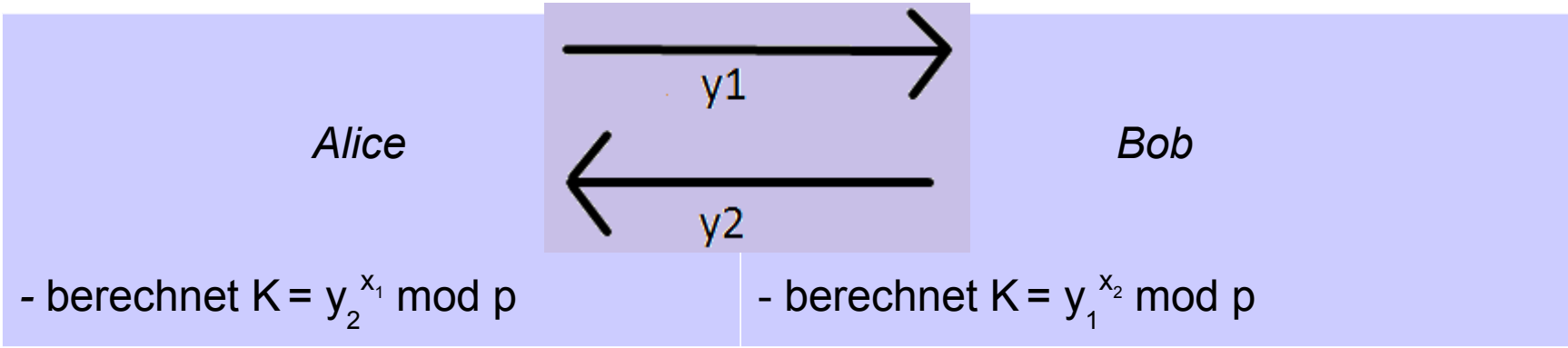
Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Kommunikation:



Diffie – Hellman Verfahren

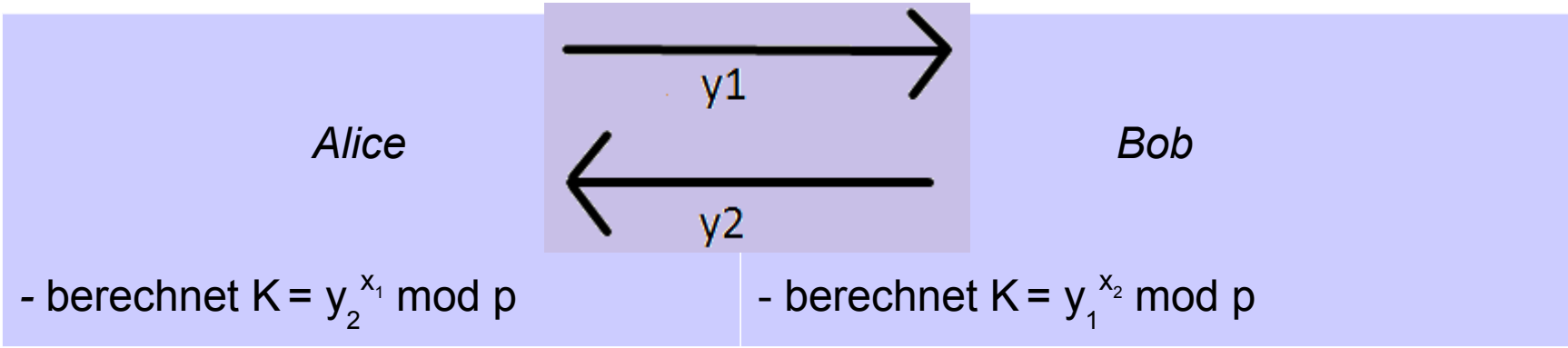
- Schlüsselvereinbarung
  - Kommunikation:



$$K = (a^{x_2})^{x_1} \bmod p = (a^{x_1})^{x_2} \bmod p$$

Diffie – Hellman Verfahren

- Schlüsselvereinbarung
  - Kommunikation:



$$K = (a^{x_2})^{x_1} \bmod p = (a^{x_1})^{x_2} \bmod p$$

K ist somit der gemeinsam vereinbarte, geheime Schlüssel

Diffie – Hellman Verfahren

- Schlüsselvereinbarung – Beispiel
  - Zunächst wird p = 7 und a = 3 vereinbart

Alice	*Bob*
- wählt x_1 = 2 zufällig	- wählt x_2 = 6 zufällig

Diffie – Hellman Verfahren

- Schlüsselvereinbarung – Beispiel
  - Zunächst wird p = 7 und a = 3 vereinbart

Alice	*Bob*
- wählt $x_1 = 2$ zufällig - berechnet $y_1 = 2 \equiv 3^2 \bmod 7$ --> $y_1 = 2$	- wählt $x_2 = 6$ zufällig - berechnet $y_2 = 1 \equiv 3^6 \bmod 7$ <--- $y_2 = 1$

Diffie – Hellman Verfahren

- Schlüsselvereinbarung – Beispiel
  - Zunächst wird p = 7 und a = 3 vereinbart

Alice	*Bob*
- wählt $x_1 = 2$ zufällig - berechnet $y_1 = 2 \equiv 3^2 \bmod 7$ ---> $y_1 = 2$	- wählt $x_2 = 6$ zufällig - berechnet $y_2 = 1 \equiv 3^6 \bmod 7$ <--- $y_2 = 1$
- berechnet $K_{1,2} = y_2^{x_1} \bmod p =$ $1^2 \bmod 7 = 1 \bmod 7 =$ **1**	- berechnet $K_{2,1} = y_1^{x_2} \bmod p =$ $2^6 \bmod 7 = 64 \bmod 7 =$ **1**

Diffie – Hellman Verfahren

- Zusammenfassung
  - Wählen einer großen Primzahl und passender Einheitswurzel und Übertragung über unsicheren Kanal
  - Alice und Bob berechnen jeweils eine Zufallszahl $X_A < p$ (~private key) und berechnen $Y_A = a^{x_A} \bmod p$ (~public Key)
  - Alice und Bob berechnen geheimen Schlüssel parallel

    → Schlüsselvereinbarung kann vollständig über unsicheren Kanal stattfinden

    → Authentifizierung muss jedoch getrennt davon stattfinden

Sicherheit

- Das Diffie – Hellman – Problem
  - Für einen potenziellen Angreifer sind Primzahl p, prim. Einheitswurzel a sowie die öffentlichen Schlüssel y_i bekannt
  - Die Sicherheit beruht auf einer „Einwegfunktion mit Falltür“, man nimmt an, dass die Berechnung des diskreten Logarithmus exponentiell zum Aufwand der Exponentiation steigt

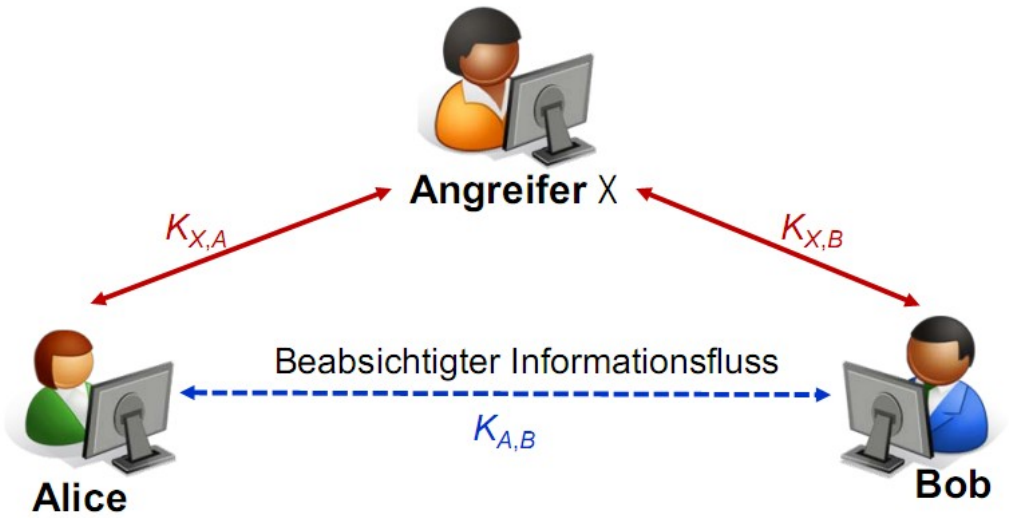
Sicherheit

- DH – Problem Teil 2
  - Wenn keine weiteren Informationen bekannt sind, muss der Angreifer das diskrete Logarithmusproblem

    $X_i = \log_a Y_i \bmod p$ lösen, um den Schlüssel zu berechnen
  - Beispiel : $p < 200$
    - Für K werden max. 400 Multiplikationen benötigt (jeweils max. 200 Operationen für a^{x_i} und $y_i^{x_i}$)(x_i<p)
    - Die Berechnung des Logarithmus erfordert $2^{400/2}=10^{30}$ Operationen

Sicherheit

- Andere Angriffsmöglichkeiten
  - Man in the Middle – Angriff



  - Da D.-H. keine Authentifizierung bereitstellt, muss sie anders stattfinden, z.B. über Station-to-Station Protokolle
  - Timing Attacks sind u.A. ebenfalls möglich

Anwendungen von Diffie Hellman

- Oft wird DH zur Vereinbarung von Schlüssel für symmetrische Kryptosysteme genutzt
- Elgamal ist ein auf DH basierendes asymetrisches Kryptosystem
- In VPN wird oft Diffie – Hellman genutzt